COBIT® 2019

Marco de Referencia

Introducción y metodología

ISACA®

Acerca de ISACA

Con casi 50 años de vida, ISACA® (isaca.org) es una organización global que ayuda tanto a individuos como a empresas a alcanzar el potencial positivo de la tecnología. La tecnología impulsa el mundo de hoy e ISACA proporciona a los profesionales con el conocimiento, las credenciales, la educación y la comunidad para avanzar en sus carreras profesionales y transformar sus organizaciones. ISACA aprovecha la experiencia de su medio millón de dedicados profesionales en información y ciberseguridad, gobierno, aseguramiento, riesgo e innovación, así como su filial de desempeño empresarial, el instituto CMMI®, para contribuir a una mayor innovación a través de la tecnología. ISACA está presente en más de 188 países, incluyendo más de 217 capítulos y oficinas, tanto en Estados Unidos como en China.

Descargo de responsabilidad

ISACA ha diseñado y creado el *Marco de referencia COBIT® 2019: Introducción y metodología* (el «Trabajo») fundamentalmente como un recurso educativo para los profesionales del gobierno empresarial de tecnologías de la información (GETI), aseguramiento, riesgo y seguridad. ISACA no asume ninguna responsabilidad acerca de que el uso de cualquier parte del Trabajo garantice un resultado exitoso. No debe considerarse que el Trabajo incluye toda la información, procedimientos y pruebas correctas, ni que excluye otra información, procedimientos y pruebas que estén orientadas razonablemente hacia la obtención de los mismos resultados. Para determinar la propiedad de cualquier información, procedimiento o prueba específicos, los profesionales del gobierno empresarial de tecnologías de la información (GETI), aseguramiento, riesgo y seguridad deberían aplicar su propio criterio profesional a las circunstancias específicas de los sistemas o entorno de tecnología de la información particular.

Copyright

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: https://support.isaca.org
Website: www.isaca.org

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAHQ
Instagram: www.instagram.com/isacanews/

Marco de referencia COBIT® 2019: Introducción y metodología
ISBN 978-1-60420-788-0

En memoria: John Lainhart (1946-2018)

Dedicado a John Lainhart, Presidente del Consejo de Administración de ISACA, 1984-1985. John fue una figura clave en la creación del marco COBIT® y en los últimos años ejerció como presidente del grupo de trabajo de COBIT® 2019, que culminó con la creación de este trabajo. Durante sus cuatro décadas en ISACA, John participó en distintos aspectos de la organización, además de contar con las certificaciones CISA, CRISC, CISM y CGEIT de ISACA. John deja un increíble legado personal y profesional, y su trabajo ha tenido un gran impacto en ISACA.

Página intencionalmente en blanco

Agradecimientos

ISACA desea agradecer a:

COBIT Working Group (2017-2018)

John Lainhart, Presidente, CISA, CRISC, CISM, CGEIT, CIPP/G, CIPP/US, Grant Thornton, EE. UU.
Matt Conboy, Cigna, EE. UU.
Ron Saull, CGEIT, CSP, Great-West Lifeco & IGM Financial (jubilado), Canadá

Equipo de desarrollo

Steven De Haes, Ph.D., Antwerp Management School, University of Antwerp, Bélgica
Matthias Goorden, PwC, Bélgica
Stefanie Grijp, PwC, Bélgica
Bart Peeters, PwC, Belgium
Geert Poels, Ph.D., Ghent University, Bélgica
Dirk Steuperaert, CISA, CRISC, CGEIT, IT In Balance, Bélgica

Revisores expertos

Sarah Ahmad Abedin, CISA, CRISC, CGEIT, Grant Thornton LLP, EE. UU.
Floris Ampe, CISA, CRISC, CGEIT, CIA, ISO27000, PRINCE2, TOGAF, PwC, Bélgica
Elisabeth Antonssen, Nordea Bank, Suecia
Krzystof Baczkiewicz, CHAMP, CITAM, CSAM, Transpectit, Polonia
Christopher M. Ballister, CRISC, CISM, CGEIT, Grant Thornton, EE. UU.
Gary Bannister, CGEIT, CGMA, FCMA, Austria
Graciela Braga, CGEIT, Auditor and Advisor, Argentina
Ricardo Bria, CISA, CRISC, CGEIT, COTO CICSA, Argentina
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapur
Peter T. Davis, CISA, CISM, CGEIT, COBIT 5 Assessor, CISSP, CMA, CPA, PMI-RMP, PMP, Peter Davis+Associates, Canadá
James Doss, CISM, CGEIT, EMCCA, PMP, SSGB, TOGAF 9, ITvalueQuickStart.com, EE. UU.
Yalcin Gerek, CISA, CRISC, CGEIT, ITIL Expert, Prince2, ISO 20000LI, ISO27001LA, TAC AS., Turquía
James L. Golden, Golden Consulting Associates, EE. UU.
J. Winston Hayden, CISA, CISM, CRISC, CGEIT, Sudáfrica
Jimmy Heschl, CISA, CISM, CGEIT, Red Bull, Austria
Jorge Hidalgo, CISA, CISM, CGEIT, Chile
John Jasinski, CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CSM, CSPO, IT4IT-F, ITIL Expert, Lean IT-F, MOF, SSBB, TOGAF-F, EE. UU.
Joanna Karczewska, CISA, Polonia
Glenn Keaveny, CEH, CISSP, Grant Thornton, EE. UU.
Eddy Khoo S. K., CGEIT, Kuala Lumpur, Malasia
Joao Souza Neto, CRISC, CGEIT, Universidade Católica de Brasília, Brasil
Tracey O'Brien, CISA, CISM, CGEIT, IBM Corp (jubilada), EE. UU.
Zachy Olorunojowon, CISA, CGEIT, PMP, BC Ministry of Health, Victoria, BC Canadá
Opeyemi Onifade, CISA, CISM, CGEIT, BRMP, CISSP, ISO 27001LA, M.IoD, Afenoid Enterprise Limited, Nigeria
Abdul Rafeq, CISA, CGEIT, FCA, Managing Director, Wincer Infotech Limited, India
Dirk Reimers, Entco Deutschland GmbH, A Micro Focus Company
Steve Reznik, CISA, CRISC, ADP, LLC., EE. UU.
Bruno Horta Soares, CISA, CRISC, CGEIT, PMP, GOVaaS - Governance Advisors, as-a-Service, Portugal

Agradecimientos *(cont.)*

Revisores expertos (cont.)

Dr. Katalin Szenes, Ph.D., CISA, CISM, CGEIT, CISSP, John von Neumann Faculty of Informatics, Obuda University, Hungría
Peter Tessin, CISA, CRISC, CISM, CGEIT, Discover, USA
Mark Thomas, CRISC, CGEIT, Escoute, EE. UU.
John Thorp, CMC, ISP, ITCP, The Thorp Network, Canadá
Greet Volders, CGEIT, COBIT Assessor, Voquals N.V., Bélgica
Markus Walter, CISA, CISM, CISSP, ITIL, PMP, TOGAF, PwC Singapur/Suiza
David M. Williams, CISA, CAMS, Westpac, Nueva Zelanda
Greg Witte, CISM, G2 Inc., EE. UU.

Consejo de dirección de ISACA

Rob Clyde, CISM, Clyde Consulting LLC, EE. UU., Presidente
Brennan Baybeck, CISA, CRISC, CISM, CISSP, Oracle Corporation, EE. UU., Vicepresidente
Tracey Dedrick, Ex Director de Riesgo con Hudson City Bancorp, EE. UU.
Leonard Ong, CISA, CRISC, CISM, CGEIT, COBIT 5 Implementador y Asesor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP, Merck & Co., Inc., Singapur
R.V. Raghu, CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India
Gabriela Reynaga, CISA, CRISC, COBIT 5 Foundation, GRCP, Holistics GRC, México
Gregory Touhill, CISM, CISSP, Cyxtera Federal Group, EE. UU.
Ted Wolff, CISA, Vanguard, Inc., EE. UU.
Tichaona Zororo, CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA, EGIT | Enterprise Governance of IT (Pty) Ltd, Sudáfrica
Theresa Grafenstine, CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA, Deloitte & Touche LLP, EE. UU., Presidenta del Consejo de Administración de ISACA, 2017-2018
Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, INTRALOT, Grecia, Presidente del Consejo de Administración de ISACA, 2015-2017
Matt Loeb, CGEIT, CAE, FASAE, Director Ejecutivo, ISACA, EE. UU.
Robert E Stroud (1965-2018), CRISC, CGEIT, XebiaLabs, Inc., EE. UU, Presidente del Consejo de Administración de ISACA, 2014-2015

ISACA lamenta profundamente el fallecimiento de Robert E Stroud en septiembre de 2018.

ÍNDICE

Lista de figuras 9

Capítulo 1. Introducción 11
1.1 Gobierno empresarial de la Información y Tecnología 11
1.2 Beneficios del gobierno de tecnologías de la información 11
1.3 COBIT como marco de gobierno de I&T 12
1.3.1 ¿Qué es COBIT y qué no es? 13
1.4 Estructura de esta publicación 14

Capítulo 2. Público objetivo 15
2.1 Partes interesadas en el gobierno 15

Capítulo 3. Principios de COBIT 17
3.1 Introducción 17
3.2 Seis principios para un sistema de gobierno 17
3.3 Tres principios para un Marco de Gobierno 18
3.4 COBIT® 2019 19

Capítulo 4. Conceptos básicos: Sistema de Gobierno y Componentes 21
4.1 Generalidades de COBIT 21
4.2 Objetivos de gobierno y gestión 22
4.3 Componentes del sistema de gobierno 23
4.4 Áreas prioritarias 24
4.5 Factores de diseño 25
4.6 Cascada de metas 30
4.6.1 Metas empresariales 31
4.6.2 Metas de alineamiento 33

Capítulo 5. Objetivos de gobierno y gestión de COBIT 35
5.1 Propósito 35

Capítulo 6. Gestión del Desempeño en COBIT 39
6.1 Definición 39
6.2 Principios de gestión del desempeño de COBIT 39
6.3 Visión general de la gestión del Desempeño de COBIT 39
6.4 Gestión del desempeño de los procesos 40
6.4.1 Niveles de capacidad del proceso 40
6.4.2 Calificar las actividades del proceso 41
6.4.3 Niveles de madurez del área prioritaria 41
6.5 Gestión del desempeño de otros componentes del sistema de gobierno 42
6.5.1 Gestión del desempeño de las estructuras organizativas 42
6.5.2 Gestión de desempeño de elementos de información 43
6.5.3 Gestión del desempeño de la cultura y el comportamiento 45

Capítulo 7. Diseño de un sistema de gobierno personalizado 47
7.1 Impacto de factores de diseño 47
7.2 Fases y pasos del proceso de diseño 49

Capítulo 8. Implementar el gobierno de TI de la empresa 51
8.1 Propósito de la guía de implementación COBIT 51
8.2 Método de Implementación de COBIT 51

8.2.1 Fase 1: ¿Cuáles son los impulsores? 52
8.2.2 Fase 2: ¿Dónde estamos ahora? 52
8.2.3 Fase 3: ¿Dónde queremos estar? 53
8.2.4 Fase 4: ¿Qué debe hacerse? 53
8.2.5 Fase 5: ¿Cómo llegamos ahí? 53
8.2.6 Fase 6: ¿Lo logramos? 53
8.2.7 Fase 7: ¿Cómo mantenemos el impulso? 53
8.3 Relación entre la Guía de diseño COBIT® 2019 y la Guía de implementación COBIT® 2019 54

Capítulo 9. Comience con COBIT: Construyendo el Caso 55
9.1 Caso de negocio 55
9.2 Resumen ejecutivo 55
9.3 Antecedentes 56
9.4 Desafíos del negocio 57
9.4.1 Análisis de brechas y meta 57
9.4.2 Alternativas consideradas 58
9.5 Solución propuesta 58
9.5.1 Fase 1. Pre-planificación 58
9.5.2 Fase 2. Implementación del programa 59
9.5.3 Alcance del programa 59
9.5.4 Metodología del programa y alineamiento 60
9.5.5 Entregables del programa 60
9.5.6 Riesgo del programa 61
9.5.7 Partes interesadas 61
9.5.8 Análisis de coste-beneficio 61
9.5.9 Desafíos y factores de éxito 62

Capítulo 10. COBIT y otros estándares 65
10.1 Reglas/Guia Principal 65
10.2 Lista de estándares referenciados 65

LISTA DE FIGURAS

Capítulo 1. Introducción

Figura 1.1—El contexto del gobierno empresarial de la Información y Tecnología 11

Capítulo 2. Público objetivo

Figura 2.1—Partes interesadas de COBIT 15

Capítulo 3. Principios de COBIT

Figura 3.1—Principios del Sistema de Gobierno....18
Figura 3.2—Principios del Marco de Gobierno....18

Capítulo 4. Conceptos básicos: Sistema de Gobierno y Componentes

Figura 4.1—COBIT Generalidades....21
Figura 4.2—Modelo Core de COBIT....23
Figura 4.3—Componentes COBIT de un sistema de gobierno 24
Figura 4.4—Factores de diseño COBIT 25
Figura 4.5—Factor de diseño de estrategia de la empresa 25
Figura 4.6—Factor de diseño de metas empresariales 26
Figura 4.7—Factores de diseño del perfil de riesgo (Categorías de riesgo de TI)....26
Figura 4.8—Factor de diseño de problemas relacionados con I&T 27
Figura 4.9—Factor de diseño del panorama de amenazas....28
Figura 4.10—Factor de diseño de los requerimientos de cumplimiento 28
Figura 4.11—Factor de Diseño del rol de TI....28
Figura 4.12—Factor de diseño del modelo de sourcing para TI 29
Figura 4.13—Factor de diseño de los métodos de implementación de TI 29
Figura 4.14—Factor de diseño de la estrategia de adopción de tecnología....29
Figura 4.15—Factor de diseño del tamaño de la empresa....30
Figura 4.16—Cascada de metas de COBIT 30
Figura 4.17—Cascada de metas: Metas y métricas empresariales....31
Figura 4.18—Cascada de metas: Metas y métricas de alineamiento....33

Capítulo 5. Objetivos de gobierno y gestión de COBIT

Figura 5.1—Modelo Core de COBIT: Objetivos y propósito de gobierno y gestión 35

Capítulo 6. Gestión del Desempeño en COBIT

Figura 6.1—Niveles de capacidad....40
Figura 6.2—Niveles de capacidad para los procesos....41
Figura 6.3—Niveles de madurez para áreas prioritarias 42
Figura 6.4—Modelo de referencia de la información Criterio de calidad para la información 44

Capítulo 7. Diseño de un sistema de gobierno personalizado

Figura 7.1—Impacto de los factores de diseño en un sistema de gobierno y gestión 47
Figura 7.2—Flujo de trabajo del diseño del sistema de gobierno....49

Capítulo 8. Implementar el gobierno de TI de la empresa

Figura 8.1—Hoja de ruta de implementación COBIT....52
Figura 8.2—Puntos de conexión entre la Guía de diseño COBIT y la Guía de implementación COBIT 54

Capítulo 9. Comience con COBIT: Construyendo el Caso

Figura 9.1—Desafíos y medidas planificadas de Acme Corporation 62

Página intencionalmente en blanco

Capítulo 1
Introducción

1.1 Gobierno empresarial de la Información y Tecnología

A la luz de la transformación digital, la información y la tecnología (I&T) se han convertido en algo fundamental para el soporte, la sostenibilidad y el crecimiento de las empresas. Anteriormente, los consejos de gobierno (comités de dirección) y la alta gerencia podían delegar, ignorar o evitar las decisiones relacionadas con las I&T. En la mayoría de sectores e industrias, estas actitudes ahora no son aconsejables . La creación de valor para los grupos de interés (por ejemplo, la generación de beneficios con un costo óptimo de recursos y un riesgo optimizado) suele venir de la mano de un alto nivel de digitalización en nuevos modelos de negocio, procesos eficientes, una exitosa innovación, etc. Las empresas digitales dependen cada vez más de la I&T para su supervivencia y crecimiento.

Dada la importancia de la I&T para la gestión del riesgo empresarial y la generación de valor, en las últimas tres décadas se ha prestado una atención especial al gobierno empresarial de tecnologías de la información (GETI). La GETI es una parte fundamental del gobierno corporativo. Esta la ejerce el consejo de administración, que supervisa la definición e implementación de procesos, estructuras y mecanismos relacionados en la organización para permitir a la empresa y al personal de TI desempeñar sus responsabilidades de soporte al negocio/alineamiento de TI y la creación de valor de negocio derivado de las inversiones empresariales posibles gracias a la I&T (**figura 1.1**).

Figura 1.1—El contexto del gobierno empresarial de la Información y Tecnología

Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value, Presentando COBIT 5*, Springer International Publishing, Switzerland, 2.ª ed. 2015, *https://www.springer.com/us/book/9783319145464*

El gobierno empresarial de informacion y tecnología es complejo y multifacético. No existe una fórmula milagrosa (ni modo ideal) para diseñar, implementar y mantener una GETI eficaz dentro de una organización. Así, los miembros de los consejos directivos y la alta gerencia se ven abocados a adaptar e implementar sus medidas GETI conforme a su contexto y necesidades específicas. Además, deben estar dispuestos a aceptar una mayor responsabilidad en cuanto a las I&T y crear una mentalidad y cultura distintas para generar valor a partir de la I&T.

1.2 Beneficios del gobierno de tecnologías de la información

Fundamentalmente, la GETI se preocupa de la creación de valor a partir de la transformación digital y la mitigación del riesgo de negocio derivado de dicha transformación. Más concretamente, tras la adopción satisfactoria de la GETI cabe esperar tres resultados principales:

- **Obtención de beneficios**—Consiste en crear valor para la empresa a través de I&T, con el mantenimiento y el incremento del valor derivado de las inversiones actuales en I&T[1] y eliminando las iniciativas de TI y los activos que no están creando suficiente valor. El principio básico del valor de la I&T consiste en ofrecer servicios y soluciones adecuados, a tiempo y dentro del presupuesto, que generen los beneficios financieros y no financieros

1 A lo largo de este texto, TI se usa para referirse al departamento de la organización cuya principal responsabilidad es la tecnología. I&T se usa en este documento para referirse a toda la información que la empresa genera, procesa y usa para alcanzar sus objetivos, así como la tecnología que lo hace posible en toda la empresa.

esperados. El valor que la I&T ofrecen debería estar directamente alineado con los valores en los que se centra el negocio. El valor de las TI también debería medirse de forma que muestre el impacto y las contribuciones de las inversiones posibles gracias a las TI en el proceso de creación de valor de la empresa.

- **Optimización de riesgos**—Esto implica tener en cuenta el riesgo empresarial asociado al uso, propiedad, operación, involucramiento, influencia y adopción de I&T dentro de una empresa. El riesgo empresarial asociado a la información y la tecnología consiste en eventos relacionados con I&T que podrían llegar a tener un impacto en el negocio. Mientras que aportar valor se centra en la *creación* de valor, la gestión de riesgos se centra en la *preservación* del valor. La gestión de riesgos relacionados con la I&T debería integrarse en la estrategia de gestión de riesgos de la empresa para garantizar que se enfoca en las TI para la empresa. También debería medirse de forma que muestre el impacto y la contribución derivados de la optimización de riesgos empresariales relacionados con la I&T a la hora de preservar el valor.
- **Optimización de recursos**—Esto asegura que se cuente con las capacidades adecuadas para ejecutar el plan estratégico y que se proporcionen recursos suficientes, adecuados y eficaces. La optimización de recursos asegura la dotación de una integrada, económica infraestructura de TI , la introducción de nueva tecnología conforme lo requiera el negocio y la actualización o sustitución de sistemas obsoletos. Porque reconoce la importancia de las personas, además del hardware y software, se centra en proporcionar formación, fomentar la retención y garantizar la competencia del personal clave de TI. Recursos importantes son los datos y la información, y su explotación para obtener un valor óptimo es otro elemento esencial de la optimización de recursos.

El alineamiento estratégico y la medición del desempeño revisten una importancia primordial y afectan a la totalidad de actividades para garantizar que los objetivos relacionados con I&T estén alineados con los objetivos de la empresa.

En un amplio estudio de caso de una compañía aérea internacional, se demostró que los beneficios de la GETI incluían: costos inferiores de continuidad relacionados con las TI, mayor capacidad innovadora gracias a las TI, mayor alineamiento entre la inversión digital y los objetivos y estrategia empresariales, mayor confianza entre el negocio y las TI, y un cambio hacia una «mentalidad de valor» en torno a los activos digitales. [2]

Los estudios muestran que las empresas con estrategias de GETI mal diseñadas o adoptadas tienen un peor alineamiento del negocio y las estrategias y procesos de I&T. Como resultado, estas empresas tienen menor probabilidad de cumplir con sus estrategias de negocio previstas y lograr el valor de negocio que esperan a partir de la transformación digital.[3]

A partir de esto, es obvio que el gobierno debe entenderse e implementarse mucho más allá de la interpretación (limitada) que solemos encontrarnos y que viene sugerida por el acrónimo de gobierno, riesgo y cumplimiento (GRC). El acrónimo GRC sugiere de forma implícita que el cumplimiento y el riesgo relacionado representan el espectro de gobierno.

1.3 COBIT como marco de gobierno de I&T

Con el paso de los años, se han desarrollado y promocionado marcos de mejores prácticas para contribuir al proceso de conocimiento, diseño e implementación de la GETI. COBIT® 2019 integra y se basa en más de 25 años de desarrollo en este campo, no solo mediante la incorporación de los nuevos conocimientos de la ciencia, sino también con la aplicación de estos conocimientos en la práctica.

Desde su nacimiento en la comunidad de las auditorías de TI, COBIT® ha pasado a ser un marco de gobierno y gestión de I&T más amplio y exhaustivo y sigue estableciéndose como un marco generalmente aceptado para el gobierno de I&T.

2 De Haes, S.; W. van Grembergen; *Enterprise Governance of IT: Achieving Alignment and Value, Featuring COBIT 5, Springer International Publishing, Switzerland, 2.ª ed. 2015, https://www.springer.com/us/book/9783319145464*

3 De Haes, Steven; A. Joshi; W. van Grembergen; "State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study", *ISACA® Journal, vol. 4, 2015, https://www.isaca.org/Journal/archives/2015/Volume-4/Pages/state-and-impact-of-governance-of-enterprise-it-in-organizations.aspx. Ver también op cit De Haes y van Grembergen.*

1.3.1 ¿Qué es COBIT y qué no es?

Antes de describir el marco COBIT actualizado, es importante explicar qué es COBIT y qué no es:

COBIT es un marco para el gobierno y la gestión de las tecnologías de la información de la empresa,[4] dirigido a toda la empresa. La I&T empresarial significa toda la tecnología y procesamiento de la información que la empresa utiliza para lograr sus objetivos, independientemente de dónde ocurra dentro de la empresa. En otras palabras, la I&T empresarial no se limita al departamento de TI de una organización, aunque este está indudablemente incluido.

El marco de referencia COBIT hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos.

- **El gobierno** asegura que:
  - Las necesidades, condiciones y opciones de las partes interesadas se evalúan para determinar objetivos empresariales equilibrados y acordados.
  - La dirección se establece a través de la priorización y la toma de decisiones.
  - El desempeño y el cumplimiento se monitorean en relación con la dirección y los objetivos acordados.

En la mayoría de las empresas, el gobierno en general es responsabilidad del consejo de dirección bajo el liderazgo del presidente. Responsabilidades específicas de gobierno se pueden delegar a estructuras organizativas especiales a un nivel adecuado, en particular, en empresas más grandes y complejas.

- **La gerencia** planifica, construye, ejecuta y monitorea actividades en línea con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa.

En la mayoría de las empresas, la gerencia es responsabilidad de la dirección ejecutiva bajo el liderazgo del director general ejecutivo (CEO).

COBIT define los componentes para crear y sostener un sistema de gobierno: procesos, estructuras organizativas, políticas y procedimientos, flujos de información, cultura y comportamientos, habilidades e infraestructura.[5]

COBIT define los factores de diseño que deberían ser considerados por la empresa para crear un sistema de gobierno más adecuado.

COBIT trata asuntos de gobierno mediante la agrupación de componentes de gobierno relevantes dentro de objetivos de gobierno y gestión que pueden gestionarse según los niveles de capacidad requeridos.

Debemos disipar algunos conceptos erróneos acerca de COBIT:

- COBIT no es una descripción completa de todo el entorno de TI de una empresa.
- COBIT no es un marco para organizar procesos de negocio.
- COBIT no es un marco técnico (de TI) para gestionar toda la tecnología.
- COBIT no toma ni prescribe ninguna decisión relacionada con la TI. No decidirá cuál es la mejor estrategia de TI, cuál es la mejor arquitectura, o cuánto puede o debería costar la TI. Por el contrario, COBIT define todos los componentes que describen qué decisiones deberían tomarse, cómo deberían tomarse y quién debería tomarlas.

4 A lo largo de esta publicación, las referencias al «marco para el gobierno de TI» implican la totalidad de esta descripción.

5 Estos componentes se calificaron como habilitadores en COBIT® 5.

1.4 Estructura de esta publicación

El resto de esta publicación contiene los capítulos siguientes:

- El capítulo 2 analiza el público objetivo de COBIT.
- El capítulo 3 explica los principios de los sistemas de gobierno para I&T, y los principios de los marcos de buen gobierno.
- El capítulo 4 explica los conceptos básicos y la terminología de COBIT® 2019, incluido el modelo central de COBIT actualizado con sus 40 objetivos de gobierno y gestión.
- El capítulo 5 profundiza en los 40 objetivos de gobierno y gestión.
- El capítulo 6 explica cómo se concibe la monitorización del desempeño en COBIT® 2019 y, en particular, cómo se introducen los niveles de capacidad inspirados en el Modelo Integrado de Madurez de la Capacidad (CMMI®).
- El capítulo 7 contiene una breve introducción y una descripción general del flujo de trabajo de la *Guía de diseño COBIT® 2019*.
- El capítulo 8 contiene una breve introducción y una visión general de la *Guía de implementación de COBIT® 2019*.
- El capítulo 9 contiene un ejemplo detallado para ilustrar cómo se hace el caso para la adopción e implementación de COBIT en una empresa.
- El capítulo 10 enumera los estándares, marcos y regulaciones que se han usado durante el desarrollo de COBIT® 2019.

Capítulo 2
Público objetivo

2.1 Partes interesadas en el gobierno

El público objetivo de COBIT son las partes interesadas en la GETI y, por extensión, las partes interesadas en el gobierno corporativo. Estas partes interesadas y los beneficios que pueden obtener de COBIT se muestran en la **figura 2.1**.

Figura 2.1—Partes interesadas de COBIT

Parte interesada	Beneficio de COBIT
Juntas de	
Partes interesadas internas	Proporciona información sobre cómo obtener valor del uso de la I&T y explica las responsabilidades relevantes del consejo
Dirección ejecutiva	Proporciona las directrices acerca de cómo organizar y monitorear el desempeño de las I&T en el conjunto de la empresa
Gerentes de negocio	Ayuda a entender cómo obtener las soluciones de I&T que las empresas requieren y la mejor manera de explotar las nuevas tecnologías para acceder a nuevas oportunidades estratégicas
Gerentes de TI	Proporciona las directrices sobre la mejor manera de crear y estructurar el departamento de TI, gestionar el desempeño de TI, poner en funcionamiento una operación de TI eficiente y eficaz, controlar los costos de TI, alinear la estrategia de TI con las prioridades del negocio, etc.
Proveedores de aseguramiento	Ayuda a gestionar la dependencia de proveedores externos de servicio , proveer aseguramiento sobre las TI y asegurar la existencia de un sistema de controles internos eficaz y eficiente
Gestión de riesgos	Ayuda a asegurar la identificación y gestión de todos los riesgo relacionados con las TI
Partes interesadas externas	
Entidades reguladoras	Ayuda a asegurar que la empresa cumpla con toda la normativa y regulaciones aplicables y cuente con el sistema de gobierno adecuado para gestionar y mantener el cumplimiento
Socios de negocios	Ayuda a garantizar que las operaciones de un socio empresarial sean seguras, confiables y cumplan con toda la normativa y regulaciones aplicables
Proveedores de TI	Ayuda a asegurar que las operaciones de un proveedor de TI sean seguras, confiables y cumplan con toda la normativa y regulaciones aplicables

Se requiere un cierto nivel de experiencia y un conocimiento profundo de la empresa para beneficiarse del marco de referencia COBIT. Dicha experiencia y conocimiento permite a los usuarios personalizar las directrices principales de COBIT (cuya naturaleza es genérica) en directrices personalizadas y centradas en la empresa, mediante la consideración del contexto de la empresa.

El público objetivo incluye a aquellos responsables durante todo el ciclo de vida de la solución de gobierno, desde el diseño a la ejecución y al aseguramiento. De hecho, los proveedores de aseguramiento pueden aplicar la lógica y el flujo de trabajo desarrollado en esta publicación para crear un programa de aseguramiento bien documentado para la empresa.

Página intencionalmente en blanco

Capítulo 3
Principios de COBIT

3.1 Introducción

COBIT 2019 se desarrolló en base a dos series de principios:

- Principios que describen los requisitos fundamentales de un **sistema de gobierno** para la Información y la Tecnología de la empresa
- Principios para un **marco de gobierno** que pueda usarse para crear un sistema de gobierno para la empresa

3.2 Seis principios para un sistema de gobierno

Los seis principios para un sistema de gobierno son (**figura 3.1**):

1. Cada empresa necesita un sistema de gobierno para satisfacer las necesidades de las partes interesadas y generar valor del uso de la I&T. El valor refleja un equilibrio entre el beneficio, el riesgo y los recursos, y las empresas necesitan una estrategia y un sistema de gobierno práctico para materializar este valor.
2. Un sistema de gobierno para la I&T de la empresa se crea a partir de una serie de componentes que pueden ser de distinto tipo y que funcionan conjuntamente de forma holística.
3. Un sistema de gobierno debería ser dinámico. Esto significa que cada vez que se cambian uno o más factores del diseño (p. ej. un cambio de estrategia o tecnología), debe considerarse el impacto de estos cambios en el sistema GETI. Una visión dinámica de la GETI llevará a un sistema de GETI preparado para el futuro.
4. Un sistema de gobierno debería distinguir claramente entre actividades de gobierno y gestión, y estructuras.
5. Un sistema de gobierno debería personalizarse de acuerdo con las necesidades de la empresa, utilizando una serie de factores de diseño como parámetros para personalizar y priorizar los componentes del sistema de gobierno.
6. Un sistema de gobierno debería cubrir la empresa de principio a fin, centrándose no solo en la función de TI, sino en todo el procesamiento de tecnología e información que la empresa pone en funcionamiento para lograr sus objetivos, independientemente de dónde se realice el procesamiento en la empresa.[6]

Figura 3.1—Principios del Sistema de Gobierno

6 Huygh, T.; S. De Haes; "Using the Viable System Model to Study IT Governance Dynamics: Evidence from a Single Case Study", *Actas de la 51.ª Conferencia Internacional de Hawái sobre Ciencias de Sistemas, 2018, https://scholarspace.manoa.hawaii.edu/bitstream/10125/50501/1/paper0614.pdf*

3.3 Tres principios para un Marco de Gobierno

Los tres principios para un marco de gobierno son (**figura 3.2**):

1. Un marco de gobierno se debería basar en un modelo conceptual que identifique los componentes principales y las relaciones entre componentes para maximizar la uniformidad y permitir la automatización.
2. Un marco de gobierno debería ser abierto y flexible. Debería permitir la incorporación de nuevo contenido y la capacidad para abordar nuevos asuntos de la forma más flexible, mientras mantiene la integridad y uniformidad.
3. Un marco de gobierno debería alinearse con los principales estándares, marcos y regulaciones relacionados.

Figura 3.2—Principios del Marco de Gobierno

3.4 COBIT® 2019

COBIT® 2019 mejora las anteriores versiones de COBIT en las áreas siguientes:

- **Flexibilidad y apertura**—La definición y uso de los factores de diseño permiten la personalización de COBIT para un mayor alineamiento con el contexto específico de un usuario. La arquitectura abierta de COBIT permite incorporar nuevas áreas prioritarias (ver sección 4.4) o modificar las actuales, sin implicaciones directas para la estructura y el contenido del modelo escencial de COBIT.
- **Actualidad y relevancia**—El modelo COBIT apoya las referencias y alineamiento con conceptos que surgen de otras fuentes (p. ej. los últimos estándares y regulaciones de cumplimiento de TI).
- **Aplicación prescriptiva**—Los modelos como COBIT pueden ser descriptivos y prescriptivos. El modelo conceptual COBIT se crea y presenta de tal modo que su ejemplificación (es decir, la aplicación de los componentes de gobierno personalizados de COBIT) se percibe como una prescripción de un sistema de gobierno de TI personalizado.
- **Gestión del desempeño de TI**—La estructura del modelo de gestión de desempeño de COBIT está integrada en el modelo conceptual. Los conceptos de madurez y capacidad se introducen para lograr un mayor alineamiento con CMMI.

La guía de COBIT usa los términos gobierno de información y tecnología - de la empresa, gobierno empresarial de información y tecnología y gobierno de TI y gobernanza de TI de forma indistinta.

Capítulo 4
Conceptos básicos: Sistema de Gobierno y Componentes

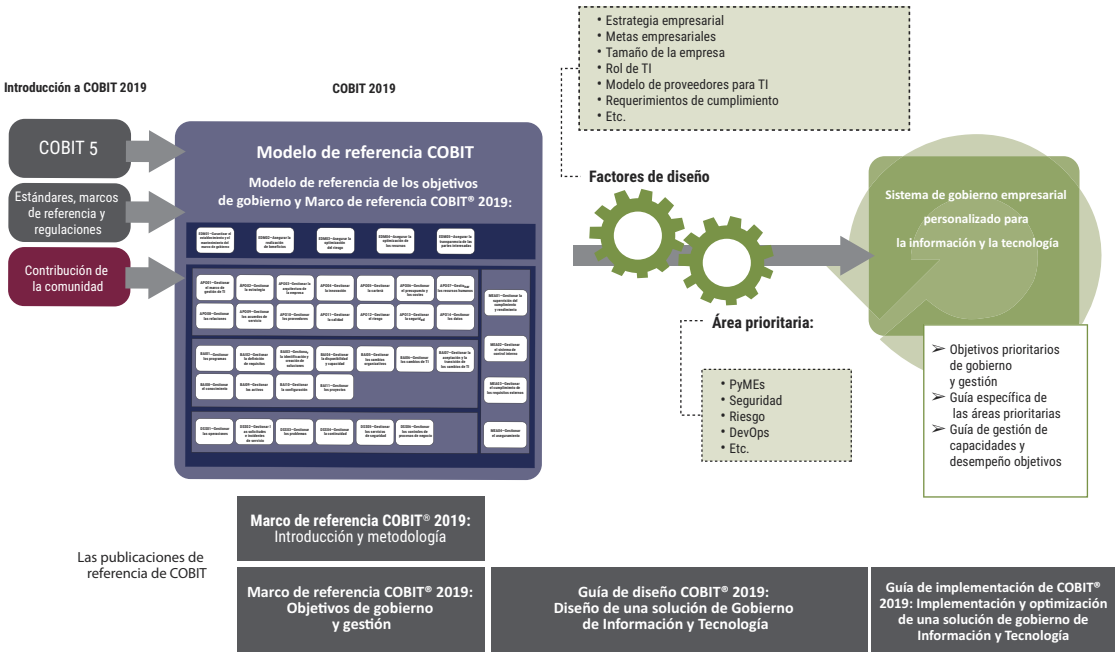
4.1 Generalidades de COBIT

La familia de productos COBIT® 2019 es abierta y se ha diseñado para la personalización. En la actualidad, están disponibles las publicaciones siguientes:[7]

- ***El Marco de referencia COBIT® 2019: Introducción y metodología,*** presenta los conceptos clave de COBIT® 2019.
- ***El Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión*** describe de forma exhaustiva los 40 objetivos principales del gobierno y la gestión, los procesos incluidos en ellos y otros componentes relacionados. Esta guía también hace referencia a otros estándares y marcos.
- ***La Guía de diseño COBIT® 2019 Diseño de una solución de Gobierno de Información y Tecnología*** explora los factores de diseño que pueden influir en el gobierno e incluye un flujo de trabajo para la planificación de un sistema de gobierno personalizado para la empresa.
- ***La Guía de implementación de COBIT® 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología*** representa una evolución de la *Guía de implementación COBIT® 5* y desarrolla una hoja de ruta para la mejora continua del gobierno. Puede usarse en combinación con la *Guía de diseño COBIT® 2019.*

La figura 4.1 muestra una visión general de COBIT® 2019 e ilustra cómo las distintas publicaciones de la serie cubren distintos aspectos.

Figura 4.1—COBIT Generalidades



7 En el momento de la publicación de este título, *Marco de referencia COBIT® 2019: Introducción y metodología, están previstos títulos adicionales de la familia de productos COBIT® 2019, aunque aún no se han publicado.*

El contenido identificado como áreas prioritarias en **la figura 4.1** incluirá una guía más detallada sobre determinados aspectos.[8]

COBIT® 2019 está basado en COBIT® 5 y otras fuentes fidedignas. COBIT está alineado con una serie de estándares y marcos relacionados. La lista de estos estándares se incluye en el capítulo 10. El análisis de estándares relacionados y el alineamiento de COBIT con estos sustentan la posición consolidada de ser la sombrilla del marco de gobierno de la Información y la Tecnología.

En el futuro, COBIT acudirá a su comunidad de usuario para que proponga actualizaciones de contenido, que serán aplicadas como contribuciones controladas de forma continua, para que COBIT esté al día con las últimas percepciones y evoluciones.

Las secciones siguientes explican los conceptos y términos clave que se usan en COBIT® 2019.

4.2 Objetivos de gobierno y gestión

Para que la información y la tecnologìa contribuyan a los objetivos de la empresa, deberían alcanzarse una serie de objetivos de gobierno y gestión. Los conceptos básicos relacionados con los objetivos de gobierno y gestión son:

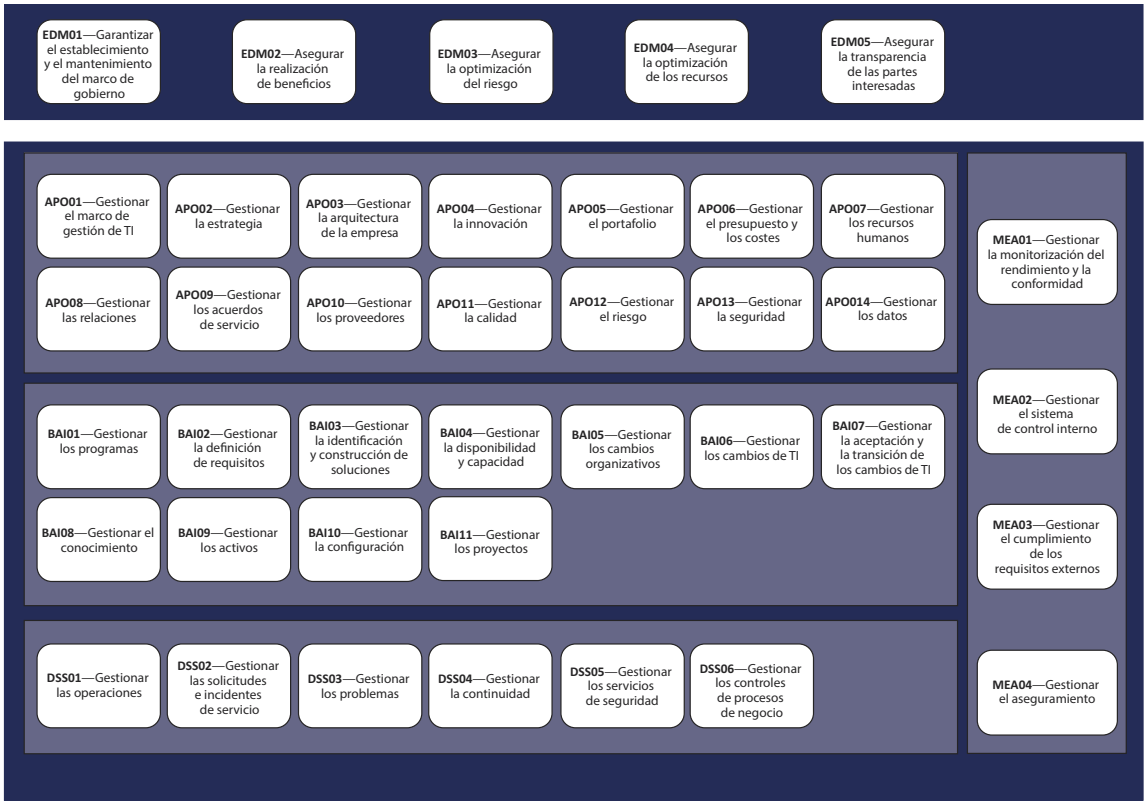
- Un objetivo de gobierno o gestión **siempre está relacionado con un proceso** (con un nombre idéntico o similar) y una serie de componentes relacionados de otros tipos para contribuir a lograr el objetivo.
- Un objetivo de gobierno está relacionado con un proceso de gobierno (mostrado en el fondo azul oscuro de **la figura 4.2**), mientras que un objetivo de gestión está relacionado con un proceso de gestión (mostrado en el fondo azul claro de **la figura 4.2**). Los consejos de administración y la dirección ejecutiva suelen ser responsables de los procesos de gobierno, mientras que los procesos de gestión pertenecen al dominio de la alta y media gerencia.

Los objetivos de gobierno y gestión de COBIT se agrupan en cinco dominios. Los dominios se nombran mediante verbos que expresan el propósito clave y las áreas de actividad del objetivo que tienen:

- Los objetivos de gobierno se agrupan en el dominio **Evaluar, Dirigir y Monitorizar** (EDM). En este dominio, el organismo de gobierno evalúa las opciones estratégicas, direcciona a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza la consecución de la estrategia.
- Los objetivos de gestión se agrupan en cuatro dominios:
  - **Alinear, Planificar y Organizar** (APO) aborda la organización general, estrategia y actividades de apoyo para las I&T.
  - **Construir, Adquirir e Implementar** (BAI) se encarga de la definición, adquisición e implementación de soluciones de I&T y su integración en los procesos de negocio.
  - **Entregar, Dar Servicio y Soporte** (DSS) aborda la ejecución operativa y el soporte de los servicios de I&T, incluida la seguridad.
  - **Monitorizar, Evaluar y Valorar** (MEA) aborda la monitorización y la conformidad de I&T con los objetivos de desempeño interno, los objetivos de control interno y los requerimientos externos.

8 Algunas de estas guías de contenido de áreas ya están preparándose; y otras están previstas. Esta serie de guías de áreas prioritarias es abierta y seguirá evolucionando. Para obtener la información más reciente sobre las publicaciones actualmente disponibles y planificadasasì como otroscontenidos, por favor visite *www.isaca.org/cobit.*

Figura 4.2—Modelo Core de COBIT



4.3 Componentes del sistema de gobierno

Con el objetivo de cumplir con los objetivos de gobierno y gestión, cada empresa debe establecer, personalizar y sostener un sistema de gobierno creado a partir de una serie de componentes.

- Estos componentes son factores que, de forma individual y colectiva, contribuyen al buen funcionamiento del sistema de gobierno de la empresa en cuanto a I&T.
- Los componentes interactúan entre sí, lo que da lugar a un sistema holístico de gobierno de I&T.
- Los componentes pueden ser de diversos tipos. Los más comunes son procesos. Sin embargo, los componentes de un sistema de gobierno incluyen también estructuras organizativas; políticas y procedimientos; elementos de información; cultura y comportamiento; habilidades y competencias; y servicios, infraestructura y aplicaciones (**figura 4.3**).
  - **Los procesos** describen una serie de prácticas y actividades organizadas para lograr determinados objetivos y producir una serie de resultados que contribuyan a la consecución de la totalidad de los objetivos relacionados con las TI.
  - **Las estructuras organizativas** son las entidades clave de toma de decisiones en una empresa.
  - **Los principios, las políticas y los marcos** convierten el comportamiento deseado en orientación práctica para la gestión del día a día.
  - **La información** es generalizada a lo largo de cualquier organización e incluye toda la información producida y utilizada por la empresa. COBIT se centra en la información requerida para el funcionamiento eficaz del sistema de gobierno de la empresa.

- **La cultura, la ética y el comportamiento** de los individuos y de la empresa son, a menudo, subestimados como un factor de éxito de las actividades de gobierno y gestión.
- **Las personas, las habilidades y las competencias** son necesarias para tomar buenas decisiones, ejecutar acciones correctivas y completar satisfactoriamente todas las actividades.
- **Los servicios, la infraestructura y las aplicaciones** incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la empresa un sistema de gobierno para el procesamiento de I&T.

Figura 4.3—Componentes COBIT de un sistema de gobierno

Los componentes de cualquier tipo pueden ser genéricos o variantes de los componentes genéricos:

- **Los componentes** genéricos se describen en el modelo core de COBIT (ver **la figura 4.2**) y se aplican, en principio, a cualquier situación. Sin embargo, su naturaleza es genérica y suelen requerir una adaptación antes de que se puedan implementar en la práctica.
- **Las alternativas** se basan en componentes genéricos, pero se adaptan para un propósito o contexto específico dentro de un área prioritaria (p. ej.: para seguridad de la información, DevOps, una regulación específica).

4.4 Áreas prioritarias

Un **área prioritaria** describe un tópico, dominio o asunto de gobierno que puede abordarse por una serie de objetivos de gobierno y gestión y sus componentes. Algunos de los ejemplos de áreas prioritarias son: pequeñas y medianas empresas, ciberseguridad, transformación digital, computación en la nube, privacidad, y DevOps.[9] Las áreas prioritarias pueden incluir una combinación de componentes de gobierno genéricos y variantes.

[9] DevOps es un ejemplo tanto de una variante de componente como de un área prioritaria. ¿Por qué? DevOPs es un tema de actualidad en el mercado y requiere indudablemente unas directrices específicas, lo que lo convierte en un área prioritaria. DevOps incluye una serie de objetivos de gobierno y gestión genéricos del modelo core de COBIT, junto con una serie de variantes de procesos y estructuras organizativas relativas al desarrollo, la operación y la monitorización.

La cantidad de áreas prioritarias es prácticamente ilimitada. Esto hace que COBIT sea abierto. Se pueden añadir nuevas áreas prioritarias conforme sea necesario o conforme los expertos y especialistas en la materia contribuyan al modelo COBIT abierto.

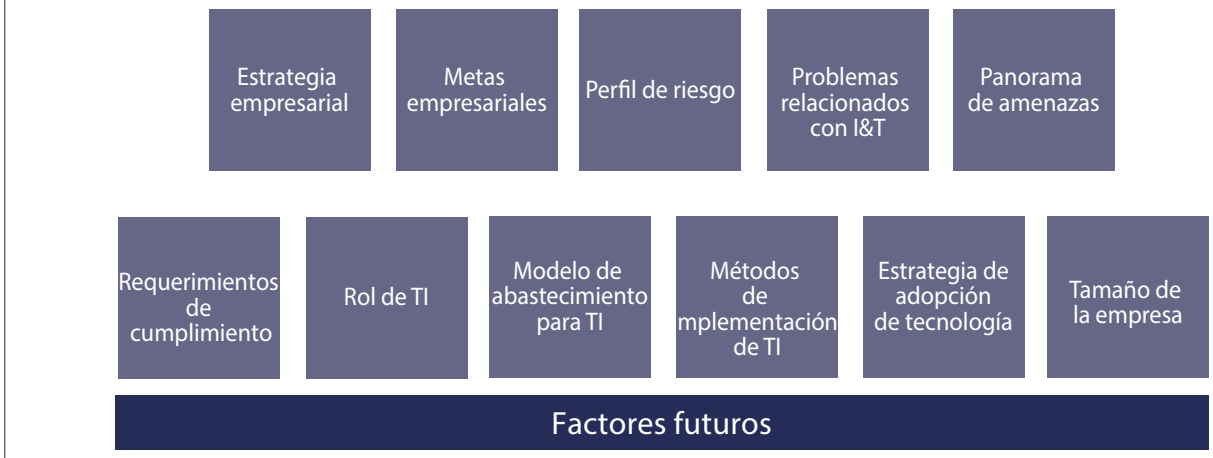
4.5 Factores de diseño

Los factores de diseño son factores que pueden influir en el diseño del sistema de gobierno de una empresa y posicionarla para que tenga éxito al usar la I&T.

Los posibles impactos que pueden tener los factores de diseño en el sistema de gobierno se señalan en la sección 7.1. Puede encontrar más información y una guía detallada acerca de cómo usar los factores de diseño al diseñar un sistema de gobierno en la *Guía de diseño COBIT® 2019*.

Los factores de diseño incluyen cualquier combinación de lo siguiente (**figura 4.4**):

Figura 4.4—Factores de diseño COBIT



1. **Estrategia de la empresa**—Las empresas pueden contar con distintas estrategias, que pueden expresarse como uno o más de los arquetipos que se muestran en **la figura 4.5**. Las organizaciones suelen contar con una estrategia principal y, como mucho, una estrategia secundaria.

Figura 4.5—Factor de diseño de estrategia de la empresa

Arquetipo de la estrategia	Explicación
Crecimiento/Adquisición	La empresa se centra en el crecimiento (ingresos).[10]
Innovación/Diferenciación	La empresa debe centrarse en ofrecer productos y servicios diferentes y/o innovadores a sus clientes.[11]
Liderazgo en costos	La empresa debe centrarse en la minimización de costes a corto plazo.[12]
Servicio al cliente/Estabilidad	La empresa se centra en proporcionar un servicio estable y orientado al cliente.[13]

10 Se corresponde con el prospector de la tipología Miles-Snow. Ver "Miles and Snow's Typology of Defender, Prospector, Analyzer, and Reactor," Elibrary, *https://ebrary.net/3737/management/miles_snows_typology_defender_prospector_analyzer_reactor.*

11 Ver Reeves, Martin; Claire Love, Philipp Tillmanns, "Your Strategy Needs a Strategy," *Harvard Business Review, septiembre 2012, https://hbr.org/2012/09/your-strategy-needs-a-strategy, especialmente relacionado con la visión y el modelado.*

12 Corresponde al liderazgo en costes; ver University of Cambridge, "Porter's Generic Competitive Strategies (ways of competing)," Institute for Manufacturing (IfM) Management Technology Policy, *https://www.ifm.eng.cam.ac.uk/research/dstools/porters-generic-competitive-strategies/. También corresponde a la excelencia operativa; ver Treacy, Michael; Fred Wiersema, "Customer Intimacy and Other Value Disciplines," Harvard Business Review, enero/febrero 1993, https://hbr.org/1993/01/customer-intimacy-and-other-value-disciplines*

13 Corresponde a los defensores de la tipología Miles-Snow. Ver *op cit "Miles and Snow's Typology of Defender, Prospector, Analyzer, and Reactor."*

2. **Objetivos empresariales** que soporten la estrategia empresarial—La estrategia empresarial se logra mediante la consecución de (una serie de) metas empresariales. Estos objetivos se definen en el marco de referencia COBIT, se estructuran en torno a las dimensiones del cuadro de mando integral (balanced scorecard), e incluyen los elementos que se muestran en **la figura 4.6.**

Figura 4.6—Factor de diseño de metas empresariales

Referencia	Dimensión del cuadro de mando integrado (Balanced Scorecard, BSC)	Meta empresarial
EG01	Financiera	Portafolio de productos y servicios competitivos
EG02	Financiera	Gestión de riesgo de negocio
EG3	Financiera	Cumplimiento de leyes y regulaciones externas
EG4	Financiera	Calidad de la información financiera
EG5	Cliente	Cultura de servicio orientada al cliente
EG6	Cliente	Continuidad y disponibilidad del servicio del negocio
EG7	Cliente	Calidad de la información de gestión
EG8	Interna	Optimización de la funcionalidad de los procesos internos del negocio
EG9	Interna	Optimización de costes de los procesos del negocio
EG10	Interna	Habilidades, motivación y productividad del personal
EG11	Interna	Cumplimiento de las políticas internas
EG12	Crecimiento	Gestión de programas de transformación digital
EG13	Crecimiento	Innovación de productos y negocios

La sección 4.6 incluye más información de la cascada de metas de COBIT, que es la elaboración detallada de este factor de diseño.

3. **El perfil de riesgo** de la empresa y los problemas actuales relacionados con la I&T—El perfil de riesgo identifica los tipos de riesgos relacionados con I&T a los que está expuesta la empresa en la actualidad e indica qué áreas de riesgo exceden el apetito al riesgo. Las categorías de riesgo[14] enumeradas en **la figura 4.7** merecen consideración.

Figura 4.7—Factores de diseño del perfil de riesgo (Categorías de riesgo de TI)

Referencia	Categoría de riesgo
1	Toma de decisiones sobre inversiones en TI, definición y mantenimiento del portafolio
2	Gestión del ciclo de vida de programas y proyectos
3	Coste y supervisión de TI
4	Experiencia, habilidades y comportamientos de TI
5	Arquitectura de la empresa/TI
6	Incidentes de infraestructura operativa de TI
7	Acciones no autorizadas
8	Adopción de software/problemas de uso
9	Incidentes de hardware
10	Fallos de software
11	Ataques lógicos (hacking, malware)
12	Incidentes de terceros/proveedores externos
13	Incumplimiento
14	Problemas geopolíticos
15	Acción sindical
16	Desastres naturales
17	Innovación tecnológica
18	Medio ambiente
19	Gestión de información y datos

14 Modificado por ISACA: *La Guía del profesional de Riesgos de TI, EE. UU., 2009*

4. **Problemas relacionados con I&T**—Un método asociado para una valoración de riesgos de I&T de la empresa consiste en considerar a qué problemas relacionados con I&T se enfrenta o, dicho de otro modo, qué riesgo relacionado con I&T se ha materializado. El problema más común de todos[15] Se incluyen en **la figura 4.8**.

Figura 4.8—Factor de diseño de problemas relacionados con I&T

Referencia	Descripción
A	Frustración entre distintas unidades de TI a través de la organización debido a una percepción de baja contribución al valor del negocio
B	Frustración entre distintos departamentos de la empresa (por ej. el cliente de TI) y el departamento de TI debido a iniciativas fallidas o una percepción de baja contribución al valor del negocio
C	Incidentes significativos relacionados con TI, como pérdida de datos, brechas de seguridad, fracaso de proyectos y errores de aplicaciones, relacionados con TI
D	Problemas de entrega del servicio por parte de los terceros de TI
E	Incumplimiento de los requerimientos regulatorios o contractuales relacionados con TI
F	Hallazgos habituales de auditoría u otros informes de evaluación sobre un pobre desempeño de TI o notificación de problemas en la calidad del servicio de TI
G	Importantes gastos ocultos y fraudulentos en TI, es decir, gasto en TI por departamentos de usuarios fuera del control de los mecanismos normales de decisión de inversión y los presupuestos aprobados de TI
H	Duplicidades o solapamientos entre varias iniciativas u otras formas de desperdicio de recursos
I	Recursos de TI insuficientes, personal con habilidades inadecuadas o personal agotado/insatisfecho
J	Cambios o proyectos habilitados por TI no satisfacen a menudo las necesidades del negocio y que se ejecutan tarde o por encima del presupuesto
K	Resistencia de los miembros del consejo de administración, ejecutivos o alta gerencia a involucrarse en las TI o una falta de patrocinio empresarial comprometido con TI
L	Modelo operativo de TI complejo y/o mecanismos de decisión confusos para las decisiones relacionadas con TI
M	Coste de TI excesivamente alto
N	Implementación obstaculizada o fallida de nuevas iniciativas o innovaciones causada por la arquitectura y sistemas de TI actuales
O	Brecha entre conocimiento tecnológico y empresarial, lo que lleva a que los usuarios del negocio y los especialistas en TI hablen lenguajes distintos
P	Problemas habituales con la calidad de los datos y la integración de datos de distintas fuentes
Q	Nivel elevado de informática de usuario final, lo que genera (entre otros problemas) una falta de supervisión y control de calidad sobre las aplicaciones que se están desarrollado y colocando en operación
R	Los departamentos del negocio implementan sus propias soluciones de información con poco o ningún involucramiento del departamento de TI de la empresa.[16]
S	Ignorancia y/o incumplimiento de las regulaciones de privacidad
T	Incapacidad para explotar nuevas tecnologías o innovar utilizando I&T

5. **Panorama de amenazas**—El panorama de amenazas bajo el cual opera la empresa puede clasificarse tal como se muestra en **la figura 4.9**.

Figura 4.9—Factor de diseño del panorama de amenazas

Panorama de amenazas	Explicación
Normal	La empresa funciona bajo lo que se consideran niveles de amenaza normales.
Alto	Debido a su situación geopolítica, sector industrial o perfil específico, la empresa funciona en un entorno de amenazas elevadas.

15 ISACA, *Ver también la Sección 3.3.1 Puntos críticos típicos, en la Guía de implementación de COBIT® 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología, EE.UU., 2019*

16 Este problema está relacionado con la informática de usuario final, que suele surgir de la insatisfacción con respecto a las soluciones y servicios de TI.

6. **Requerimientos de cumplimiento**—Los requerimientos de cumplimiento a los que la empresa está sujeta pueden clasificarse conforme a las categorías enumeradas en **la figura 4.10**.

Figura 4.10—Factor de diseño de los requerimientos de cumplimiento	
Entornos regulatorios	**Explicación**
Requerimientos de cumplimiento bajos	La empresa está sujeta a un conjunto de requerimientos de cumplimiento mínimos que son inferiores a la media.
Requerimientos de cumplimiento normales	La empresa está sujeta a un conjunto de requerimientos de cumplimiento comunes a las distintas industrias.
Requerimientos de cumplimiento altos	La empresa está sujeta a requerimientos de cumplimiento más elevados de lo normal, en la mayoría de los casos relacionados con el sector industrial y las condiciones geopolíticas.

7. **Rol de TI**—-El rol de TI para la empresa puede clasificarse tal como se muestra en **la figura 4.11**.

Figura 4.11—Factor de Diseño del rol de TI	
Rol de TI[17]	**Explicación**
Soporte	TI no es crucial para el funcionamiento y la continuidad de los procesos y servicios del negocio ni para su innovación.
Fábrica	Cuando las TI fallan, hay un impacto inmediato en el funcionamiento y continuidad de los procesos y servicios del negocio. Sin embargo, las TI no se consideran un factor impulsor de la innovación de procesos y servicios del negocio.
Cambio	Las TI se consideran un factor impulsor de la innovación de procesos y servicios del negocio. En este momento, sin embargo, no hay una dependencia crítica en TI para el funcionamiento y la continuidad actual de los procesos y servicios del negocio.
Estratégico	Las TI son críticas para el funcionamiento e innovación de los procesos y servicios del negocio de la organización.

8. **Modelo de abastecimiento para TI**—El modelo de abastecimiento que la empresa adopta puede clasificarse tal como se muestra en **la figura 4.12**.

Figura 4.12—Factor de diseño del modelo de abastecimiento para TI	
Modelo de abastecimiento	**Explicación**
Externalización / Tercerización (outsourcing)	La empresa requiere los servicios de un tercero para proporcionar servicios de TI.
Nube	La empresa maximiza el uso de la nube para proporcionar servicios de TI a sus usuarios.
Internalizado (insourced)	La empresa aporta su propio personal y servicios de TI.
Híbrido	Se aplica un modelo híbrido que combina los otros tres modelos en distintos grados.

17 Los roles incluidos en esta tabla se han extraido de McFarlan, F. Warren; James L. McKenney; Philip Pyburn; "The Information Archipelago—Plotting a Course," *Harvard Business Review, enero 1993, https://hbr.org/1983/01/the-information-archipelago-plotting-a-course.*

9. **Métodos de implementación de TI**—Los métodos que la empresa adopta pueden clasificarse tal como se muestra en **la figura 4.13**.

Figura 4.13—Factor de diseño de los métodos de implementación de TI	
Método de implementación de TI	**Explicación**
Agil	La empresa utiliza los métodos de desarrollo de trabajo Agil para su desarrollo de software.
DevOPs	La empresa usa los métodos de trabajo DevOps para la creación, despliegue y operaciones de software.
Tradicional	La empresa usa un método más clásico para el desarrollo de software (cascada) y separa el desarrollo de software de las operaciones.
Híbrido	La empresa usa una mezcla de implementación de TI tradicional y TI moderna, a la que solemos referirnos como «TI bimodal».

10. **Estrategia de adopción de tecnología**—La estrategia de adopción de tecnología puede clasificarse tal como se muestra en **la figura 4.14**.

Figura 4.14—Factor de diseño de la estrategia de adopción de tecnología	
Estrategia de adopción de tecnología	**Explicación**
El que primero se mueve (First mover)	La empresa suele adoptar nuevas tecnologías lo antes posible e intenta lograr la «ventaja del que primero se mueve».
Seguidor (Follower)	La empresa suele esperar a que las nuevas tecnologías se generalicen y pongan a prueba antes de adoptarlas.
Adoptadores lentos (Slow adopter)	La empresa tarda mucho en adoptar las nuevas tecnologías.

11. **Tamaño de la empresa**—Se identifican dos categorías, tal como se muestra en **la figura 4.15**, para el diseño de un sistema de gobierno de la empresa.[18]

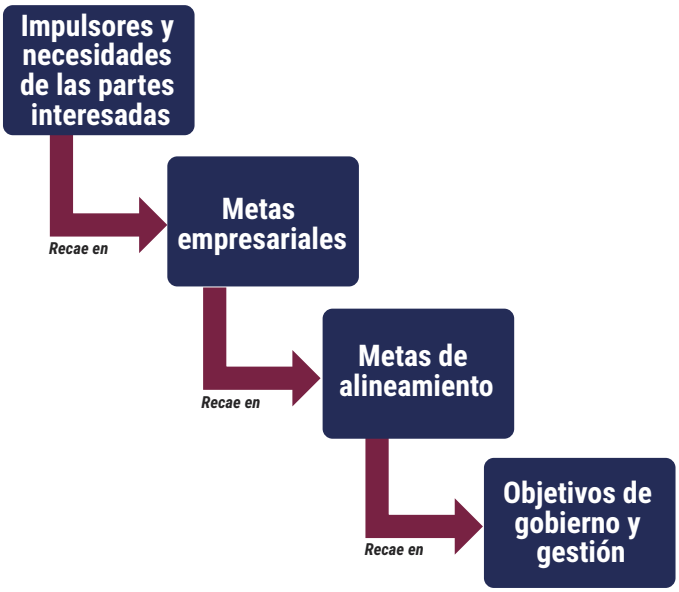
Figura 4.15—Factor de diseño del tamaño de la empresa	
Tamaño de la empresa	**Explicación**
Empresa grande (predeterminada)	Empresa con más de 250 empleados que laboran tiempo completo (FTE)
Pequeñas y medianas empresas	Empresa con entre 50 y 250 empleados que laboran tiempo completo (FTE)

18 En esta publicación no se han considerado las microempresas, es decir, empresas con menos de 50 empleados.

4.6 Cascada de metas

Las necesidades de las partes interesadas tienen que transformase en una estrategia factible para la empresa. La cascada de metas (**figura 4.16**) soporta las metas empresariales, que es uno de los factores de diseño clave para un sistema de gobierno. Apoya la priorización de los objetivos de la dirección basada en la priorización de las metas empresariales.

Figura 4.16—Cascada de metas de COBIT



La cascada de metas soporta además la conversión de las metas empresariales en prioridades para metas de alineamiento. La cascada de metas se ha actualizado de forma exhaustiva en COBIT® 2019:

- las metas empresariales se han consolidado, reducido, actualizado y aclarado.
- Las metas de alineamiento subrayan el alineamiento de todos los esfuerzos de TI con los objetivos del negocio.[19] Este término actualizado también pretende evitar la equivocación frecuente de que estas metas indican exclusivamente metas internas del departamento de TI dentro de una empresa Al igual que las metas empresariales, las metas de alineamiento se han consolidado, reducido, actualizado y aclarado cuando ha sido necesario.

19 Las metas de alineamiento se denominaban metas relacionadas con TI en COBIT 5.

4.6.1 Metas empresariales

Las necesidades de las partes interesadas tienen un efecto en las metas empresariales. **La figura 4.17** muestra el conjunto de 13 metas empresariales junto con una serie de métricas asociadas de ejemplo.

Figura 4.17—Cascada de metas: Metas y métricas empresariales

Referencia	Dimensión del BSC	Meta empresarial	Métricas de ejemplo
EG01	Financiera	Portafolio de productos y servicios competitivos	• Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado • Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente • Porcentaje de productos y servicios que proporcionan una ventaja competitiva • Plazo de comercialización para nuevos productos y servicios
EG02	Financiera	Gestión de riesgo de negocio	• Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos • Tasa (ratio) de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes • Frecuencia adecuada de la actualización del perfil de riesgo
EG03	Financiera	Cumplimiento de leyes y regulaciones externas	• Coste de incumplimiento regulatorio, incluyendo liquidacionesy multas • Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa • Número de problemas de incumplimiento señalados por los reguladores o autoridades supervisoras • Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios empresariales
EG04	Financiera	Calidad de la información financiera	• Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa • Coste de incumplimiento regulatorio con respecto a regulaciones financieras
EG05	Cliente	Cultura de servicio orientada al cliente	• Número de interrupciones del servicio al cliente • Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios al cliente cumpla con los niveles de servicio acordados • Número de quejas de los clientes • Tendencia de los resultados de la encuesta de satisfacción al cliente
EG06	Cliente	Continuidad y disponibilidad del servicio del negocio	• Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos • Coste empresarial causado por los incidentes • Número de horas de procesamiento perdidas por el negocio debido a interrupciones inesperadas del servicio • Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados
EG07	Cliente	Calidad de la información de gestión	• Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones • Número de incidentes causados por decisiones erróneas de negocio basadas en información incorrecta • Tiempo que se tarda en proporcionar la información de soporte para permitir la toma de decisiones empresariales eficaces • Puntualidad en la entrega de la información de gestión

Figura 4.17—Cascada de metas: Metas y métricas empresariales *(cont.)*			
Referencia	**Dimensión del BSC**	**Meta empresarial**	**Métricas de ejemplo**
EG08	Interna	Optimización de la funcionalidad de procesos internos del negocio	• Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso del negocio • Niveles de satisfacción de los clientes con las capacidades de prestación de servicios • Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro
EG09	Interna	Optimización de costes de los procesos del negocio	• Relación entre el coste y los niveles de servicio conseguidos • Niveles de satisfacción del consejo de administración y la dirección ejecutiva con los costes de proceso del negocio
EG10	Interna	Habilidades, motivación y productividad del personal	• Productividad del personal comparada con benchmarks • Nivel de satisfacción de las partes interesadas con los niveles de experiencia y habilidades del personal • Porcentaje de personal cuyas habilidades son insuficientes con respecto a la competencia requerida para sus funciones • Porcentaje de personal satisfecho
EG11	Interna	Cumplimiento con las políticas internas	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de las partes interesadas que entienden las políticas • Porcentaje de políticas respaldadas por estándares y prácticas de trabajo eficaces
EG12	Crecimiento	Gestión de programas de transformación digital	• Número de programas ejecutados a tiempo y dentro del presupuesto • Porcentaje de partes interesadas satisfechas con la ejecución del programa • Porcentaje de programas de transformación del negocio suspendidos • Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas periódicamente
EG13	Crecimiento	Innovación de producto y negocio	• Nivel de conciencia y comprensión de las oportunidades de innovación del negocio • Satisfacción de las partes interesadas con los niveles de experiencia e ideas sobre innovación y productos • Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras

4.6.2 Metas de alineamiento

Las metas empresariales tienen un efecto en cascada a las metas de alineamiento. **La figura 4.18** incluye un conjunto de metas de alineamiento y métricas de ejemplo.

Figura 4.18—Cascada de metas: Metas y métricas de alineamiento			
Referencia	**Dimensión del BSC de TI**	**Metas de alineamiento**	**Métricas**
AG01	Financiera	Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas	• Coste de incumplimiento de TI, incluidos liquidaciones y multas, y el impacto de la pérdida reputacional • Número de problemas de incumplimiento relacionados con TI notificados al consejo de administración o que causan comentarios o descrédito públicos • Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI
AG02	Financiera	Gestión de riesgo relacionado con I&T	• Frecuencia adecuada de la actualización del perfil de riesgo • Porcentaje de las evaluaciones de riesgo empresarial, incluido el riesgo relacionado con I&T • Número de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos

Figura 4.18—Cascada de metas: Metas y métricas de alineamiento *(cont.)*

Referencia	Dimensión del BSC de TI	Metas de alineamiento	Métricas
AG03	Financiera	Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T	• Porcentaje de inversiones posibilitadas por I&T en las que los beneficios previstos se cumplen o exceden • Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
AG04	Financiera	Calidad de la información financiera relacionada con la tecnología	• Satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de TI • Porcentaje de servicios de I&T con costes operativos claramente definidos y aprobados y beneficios esperados
AG05	Cliente	Prestación de servicios de I&T conforme a los requerimientos del negocio	• Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de TI cumpla con los niveles de servicio acordados • Número de interrupciones del negocio debido a incidentes de servicios de TI • Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI
AG06	Cliente	Agilidad para convertir los requerimientos del negocio en soluciones operativas	• Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requisitos • Promedio de plazo de comercialización para servicios y aplicaciones nuevos relacionados con las I&T • Tiempo promedio para convertir los objetivos estratégicos de I&T en una iniciativa acordada y aprobada • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas
AG07	Interna	Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad	• Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público • Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público • Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público
AG08	Interna	Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	• Plazo para la ejecución de servicios y procesos empresariales • Número de programas empresariales facilitados por I&T retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica • Número de cambios en los procesos de negocio que se deben aplazar o revisar debido a problemas de integración tecnológica • Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
AG09	Interna	Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad	• Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto • Número de programas que necesitan una revisión significativa debido a defectos de calidad • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
AG10	Interna	Calidad de la información sobre gestión de I&T	• Nivel de satisfacción del usuario con la calidad, puntualidad y disponibilidad de la información de gestión relacionada con I&T, tras considerar los recursos disponibles • Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible relacionada con I&T fue un factor clave • Porcentaje de información que satisface los criterios de calidad

Figura 4.18—Cascada de metas: Metas y métricas de alineamiento *(cont.)*			
Referencia	**Dimensión del BSC de TI**	**Metas de alineamiento**	**Métricas**
AG11	Interna	Cumplimiento de I&T con las políticas internas	• Número de incidentes relacionados con el incumplimiento de las políticas relacionadas con TI • Número de excepciones a las políticas internas • Frecuencia de revisión y actualización de la política
AG12	Aprendizaje y crecimiento	Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio	• Porcentaje de empresarios con dominio de I&T (es decir, aquellos que tienen los conocimientos y comprensión de I&T requeridos para guiar, dirigir, innovar y ver las oportunidades de I&T en su área de experiencia) • Porcentaje de empresarios con dominio de TI (es decir, aquellos que tienen los conocimientos y comprensión de los dominios importantes del negocio requeridos para guiar, dirigir, innovar y ver las oportunidades de I&T para su ámbito empresarial) • Número o porcentaje de empresarios con experiencia en gestión de tecnología
AG13	Aprendizaje y crecimiento	Conocimiento, experiencia e iniciativas para la innovación empresarial	• Nivel de conciencia de los ejecutivos de negocios y comprensión de las posibilidades de innovación de las I&T • Número de iniciativas aprobadas como resultado de ideas innovadoras de I&T • Número de campeones en innovación reconocidos/premiados

Capítulo 5
Objetivos de gobierno y gestión de COBIT

5.1 Propósito

En la sección 4.2, **figura 4.2** se muestra el modelo core de COBIT, incluyendo los 40 objetivos de gobierno y gestión. **La figura 5.1** enumera todos los objetivos de gobierno y gestión, cada uno de ellos con su declaración de propósito. La declaración de propósito es una elaboración más detallada (con un nivel de detalle mayor) de cada objetivo de gobierno y gestión.

Figura 5.1—Modelo Core de COBIT: Objetivos y propósito de gobierno y gestión

Referencia	Nombre	Propósito
EDM01	Asegurar el establecimiento y el mantenimiento del marco de gobierno	Proporcionar un enfoque uniforme, integrado y alineado con el enfoque de gobierno de la empresa Las decisiones relacionadas con I&T deben hacerse en línea con las estrategias y objetivos de la empresa y el valor esperado es alcanzado. En este sentido, debe asegurarse de que los procesos relacionados con I&T se monitoricen de forma eficaz y transparente; que se cumpla con los requisitos legales, contractuales y regulatorios; y que se cumplan los requisitos de gobierno para los miembros del consejo de dirección.
EDM02	Asegurar la entrega de beneficios.	Asegurar un valor óptimo de las iniciativas, servicios y activos habilitados por I&T; la entrega rentable de soluciones y servicios; y una imagen confiable y precisa de los costes y beneficios probables para que las necesidades empresariales se satisfagan de forma eficaz y eficiente.
EDM03	Asegurar la optimización del riesgo	Asegurarse de que el riesgo de negocio relacionado con I&T no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de I&T en el valor de negocio y que se minimicen los posibles fallos de cumplimiento.
EDM04	Asegurar la optimización de recursos	Asegurarse de que las necesidades de recursos de la empresa se satisfagan de manera óptima, que los costes de I&T se optimicen, y que exista una mayor probabilidad de obtener beneficios y buena disposición para cambios futuros.
EDM05	Asegurar la participación de las partes interesadas	Asegurarse de que las partes interesadas apoyen la estrategia y la hoja de ruta de I&T, que la comunicación con las partes interesadas sea eficaz y oportuna, y que se establezcan las bases para los informes con el fin de aumentar el desempeño. Identificar las áreas de mejora y confirmar que los objetivos y estrategias relacionados con I&T se ajusten a la estrategia de la empresa.
APO01	Gestionar el marco de gestión de I&T	Implementar un enfoque uniforme de gestión para permitir que se alcancen los requisitos de gobierno empresarial, con cobertura de componentes de gobierno, como los procesos de gestión, las estructuras organizativas, los roles y las responsabilidades, las actividades confiables y repetibles, los elementos de información, las políticas y procedimientos, las habilidades y las competencias, la cultura y el comportamiento, y los servicios, infraestructura y aplicaciones.
APO02	Gestionar la estrategia	Apoyar la estrategia de transformación digital de la organización y proporcionar el valor deseado a través de una hoja de ruta con cambios incrementales. Usar un enfoque holístico en cuanto a T&I, asegurando que cada iniciativa esté claramente conectada con una estrategia global. Habilitar el cambio en todos los diversos aspectos de la organización, desde los canales y procesos a los datos, cultura, habilidades, modelo operativo e incentivos.
APO03	Gestionar la arquitectura empresarial	Representar los diferentes componentes que conforman la empresa y sus interrelaciones, así como los principios que guían su diseño y evolución a lo largo del tiempo, para posibilitar una prestación estándar, atenta y eficiente de los objetivos operativos y estratégicos.
APO04	Gestionar la innovación	Lograr ventajas competitivas, innovación empresarial, una mejor experiencia de cliente y una mayor eficacia y eficiencia operativa con el aprovechamiento de los desarrollos de I&T y las tecnologías emergentes.

Figura 5.1—Modelo Core de COBIT: Objetivos y propósito de gobierno y gestión *(cont.)*		
Referencia	**Nombre**	**Propósito**
APO05	Gestionar el portafolio	Optimizar el rendimiento del portafolio general de programas en respuesta al rendimiento individual de programas, productos y desempeño de servicios y a las cambiantes prioridades y demandas de la empresa.
APO06	Gestionar el presupuesto y los costes	Fomentar la asociación entre TI y las partes interesadas de la empresa para permitir el uso eficaz y eficiente de los recursos relacionados con I&T, y proporcionar transparencia y rendición de cuentas sobre el coste y el valor de soluciones y servicios para el negocio. Habilitar a la empresa para que tome decisiones informadas sobre el uso de soluciones y servicios de I&T.
APO07	Gestionar los recursos humanos	Optimizar las capacidades de recursos humanos para satisfacer los objetivos de la empresa
APO08	Gestionar las relaciones	Facilitar el conocimiento, habilidades y comportamientos correctos para generar mejores resultados, aumentar la credibilidad, la confianza mutua y el uso eficaz de los recursos para estimular una relación productiva con las partes interesadas de la empresa.
APO09	Gestionar los acuerdos de servicio	Asegurarse de que los productos, servicios y niveles de servicio de I&T satisfagan las necesidades actuales y futuras de la empresa.
APO10	Gestionar los proveedores	Optimizar las capacidades disponibles de I&T para apoyar la estrategia y la hoja de ruta de I&T, minimizar el riesgo asociado con proveedores que no rinden o cumplen con los requisitos y asegurar precios competitivos.
APO11	Gestionar la calidad	Asegurar la entrega consistente de soluciones y servicios tecnológicos para satisfacer los requisitos de calidad de la empresa y las necesidades de las partes interesadas.
APO12	Gestionar riesgos	Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con T&I.
APO13	Gestionar la seguridad	Mantener el impacto y la existencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.
APO14	Gestionar los datos	Asegurar el uso eficaz de activos de datos críticos para lograr las metas y objetivos empresariales.
BAI01	Gestionar los programas	Obtener el valor de negocio deseado y reducir el riesgo de retrasos, costes y erosión de valor inesperados. Para ello, se deben mejorar las comunicaciones y la participación del negocio y de los usuarios finales, asegurar el valor y la calidad de los entregables de los programas y realizar un seguimiento de los proyectos dentro de los programas y maximizar la contribución del programa al portafolio de inversiones.
BAI02	Gestionar la definición de requerimientos	Crear soluciones óptimas que satisfagan las necesidades de la empresa, mientras se minimiza el riesgo.
BAI03	Gestionar la identificación y construcción de soluciones	Asegurar una entrega ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa.
BAI04	Gestionar la disponibilidad y capacidad	Mantener la disponibilidad del servicio, la gestión eficiente de los recursos y la optimización del rendimiento del sistema a través de la predicción de los requisitos futuros de rendimiento y capacidad.
BAI05	Gestionar los cambios organizativos	Preparar y conseguir el compromiso a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.
BAI06	Gestionar los cambios de TI	Facilitar una ejecución de cambios rápida y confiable para el negocio. Mitigar el riesgo de afectar negativamente a la estabilidad o integridad del entorno que se ha modificado.
BAI07	Gestionar la aceptación y la transición de los cambios de TI	Implementar soluciones seguras y conforme a las expectativas y resultados acordados.

Figura 5.1—Modelo Core de COBIT: Objetivos y propósito de gobierno y gestión *(cont.)*		
Referencia	**Nombre**	**Propósito**
BAI08	Gestionar el conocimiento	Proporcionar los conocimientos e información de gestión necesarios para apoyar a todo el personal en el gobierno y gestión de I&T de la empresa y permitir la toma de decisiones informadas.
BAI09	Gestionar los activos	Tener en cuenta todos los activos de I&T y optimizar el valor proporcionado por su uso.
BAI10	Gestionar la configuración	Proporcionar información suficiente sobre los activos del servicio para facilitar que el servicio se gestione de forma eficiente. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.
BAI11	Gestionar los proyectos	Lograr los resultados definidos del proyecto y reducir el riesgo de retrasos inesperados, costes y erosión del valor mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Asegurar el valor y la calidad de los entregables del proyecto y maximizar su contribución a los programas y al portafolio de inversión definidos.
DSS01	Gestionar las operaciones	Proporcionar los resultados de los productos y servicios operativos de I&T según lo planeado.
DSS02	Gestionar las peticiones y los incidentes del servicio	Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidentes de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes.
DSS03	Gestionar los problemas	Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente y lograr su satisfacción reduciendo el número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas.
DSS04	Gestionar la continuidad	Adaptarse rápidamente, continuar las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la empresa en caso de una interrupción significativa (como amenazas, oportunidades, demandas).
DSS05	Gestionar los servicios de seguridad	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información
DSS06	Gestionar los controles de los procesos de negocio	Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio, dentro de la empresa o su operación tercerizada.
MEA01	Gestionar la monitorización del rendimiento y la conformidad	Proporcionar transparencia en el desempeño y la conformidad e impulsar el logro de las metas.
MEA02	Gestionar el sistema de control interno	Dar información transparente a las partes interesadas clave sobre la idoneidad del sistema de controles internos que permita, proporcionar credibilidad en las operaciones, confianza en el logro de los objetivos de la empresa y una comprensión adecuada del riesgo residual.
MEA03	Gestionar el cumplimiento de los requerimientos externos	Asegurarse de que la empresa cumpla con todos los requisitos externos aplicables.
MEA04	Gestionar el aseguramiento	Facilitar a la organización el diseño y desarrollo de iniciativas de aseguramiento eficaces y eficientes, proporcionando una guía sobre la planificación, alcance, ejecución y seguimiento de las revisiones de aseguramiento, usando una hoja de ruta basada en criterios de aseguramiento que sean bien acogidos.

Página intencionalmente en blanco

Capítulo 6
Gestión del Desempeño en COBIT

6.1 Definición

La gestión del desempeño es una parte fundamental de un sistema de gobierno y gestión. La «gestión del desempeño» es un término general que engloba todas las actividades y métodos. Expresa hasta qué punto funciona bien el sistema de gobierno y gestión y todos los componentes de una empresa, y cómo pueden mejorarse para alcanzar el nivel requerido. Incluye conceptos y métodos como niveles de capacidad y niveles de madurez. COBIT utiliza el término gestión del desempeño de COBIT (CPM, por sus siglas en inglés) para describir estas actividades, y el concepto forma parte íntegra del marco de referencia COBIT.

6.2 Principios de gestión del desempeño de COBIT

COBIT® 2019 se basa en los siguientes principios:

1. El modelo CPM debería entenderse y usarse fácilmente.
2. El modelo CPM debe ser consistente con, y apoyar, el modelo conceptual de COBIT. Debería facilitar la gestión del desempeño de cualquier tipo de componente del sistema de gobierno; debe ser posible gestionar el desempeño de los procesos, así como el desempeño de otros tipos de componentes (como estructuras organizativas o información), si los usuarios desean hacerlo.
3. El modelo CPM debería proporcionar resultados confiables, repetibles y relevantes.
4. El modelo CPM debe ser flexible, para poder dar soporte a los requerimientos de distintas organizaciones con distintas prioridades y necesidades.
5. El modelo CPM debería admitir distintos tipos de evaluaciones, desde autoevaluaciones a evaluaciones formales o auditorías.

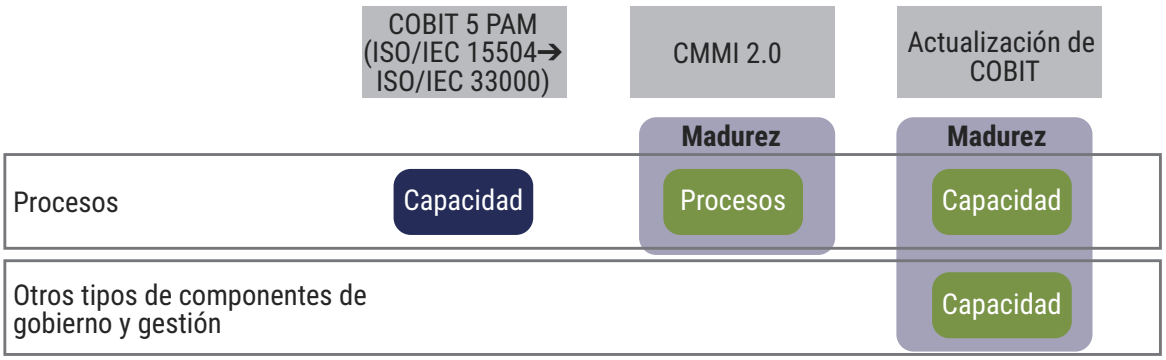
6.3 Visión general de la gestión del Desempeño de COBIT

El modelo CPM (**figura 6.1**) está en gran parte alineado y amplía los conceptos de CMMI® Development V2.0[20].

- Las actividades del proceso están asociadas con los niveles de capacidad. Esto está incluido en la guía del *Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión*.
- Otros tipos de componentes de gobierno y gestión (como las estructuras organizativas, información) también podrían tener niveles de capacidad definidos para ellos en guías futuras.
- Los niveles de madurez están asociados con áreas prioritarias (como una colección de objetivos de gobierno y gestión y los componentes subyacentes) y se alcanzarán si se obtienen todos los niveles de capacidad requeridos.

20 CMMI® *Development V2.0, CMMI Institute, EE. UU., 2018, https://cmmiinstitute.com/model-viewer/dashboard*

Figura 6.1—Niveles de capacidad



Si la empresa desea seguir usando el modelo de capacidad de procesos de COBIT 5 basado en la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC) 15504 (ahora ISO/IEC 33000, en el que los niveles de capacidad tienen muy diferentes significados), tendrá toda la información para hacerlo en el *Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión*. No serán necesarias publicaciones diferentes al modelo de evaluación de procesos (PAM) , ni se proporcionarán con COBIT® 2019.

En COBIT® 2019, los resultados explícitos del proceso o metas del proceso se sustituyen por las propias prácticas de los procesos. Esto desemboca en la situación siguiente para una evaluación ISO/IEC33000:

1. Los resultados del proceso están ahora relacionados con las prácticas del proceso de manera individual (es decir, los resultados del proceso son el cumplimiento satisfactorio de las prácticas del proceso). Nota: las prácticas del proceso se formulan como prácticas, y los resultados pueden derivarse de ello. Ejemplo: APO01.01 *Diseñar el sistema de gestión para la I&T de la empresa* tiene como resultado del proceso APO01.01: *Se diseña un sistema de gestión para la I&T de la empresa*.
2. Las prácticas base son las mismas que las prácticas del proceso de COBIT® 2019 para cada objetivo de gobierno y gestión.
3. Los productos de trabajo son lo mismo que los flujos y elementos de información bajo el componente C para cada objetivo de gobierno/gestión.

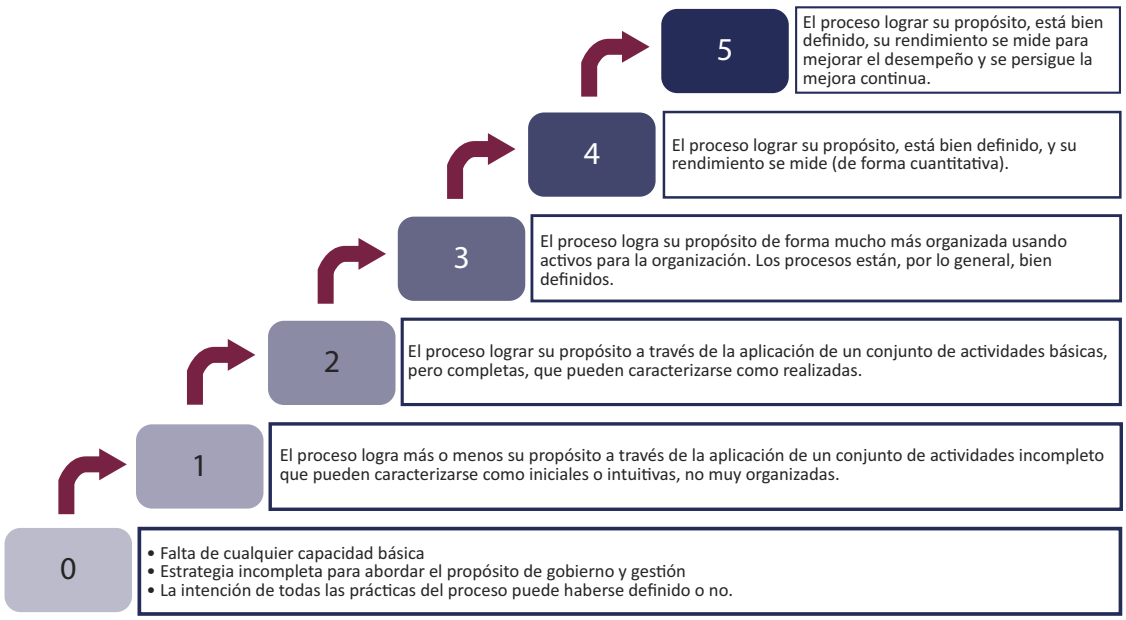
Así, la correspondencia de los resultados con las prácticas base y los productos de trabajo se hace por definición en COBIT® 2019.

6.4 Gestión del desempeño de los procesos

6.4.1 Niveles de capacidad del proceso

COBIT® 2019 admite un esquema de capacidad de procesos basado en CMMI. El proceso dentro de cada objetivo de gobierno y gestión puede funcionar con distintos niveles de capacidad, que van de 0 a 5. El nivel de capacidad es una medida de lo bien que se ha implementado y funciona un proceso. **La figura 6.2** muestra el modelo, los niveles de capacidad incrementales y las características generales de cada uno.

Figura 6.2—Niveles de capacidad para los procesos



El modelo core de COBIT asigna niveles de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos y las actividades requeridas para alcanzar los distintos niveles de capacidad. Ver *Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión* para más detalles.

6.4.2 Calificar las actividades del proceso

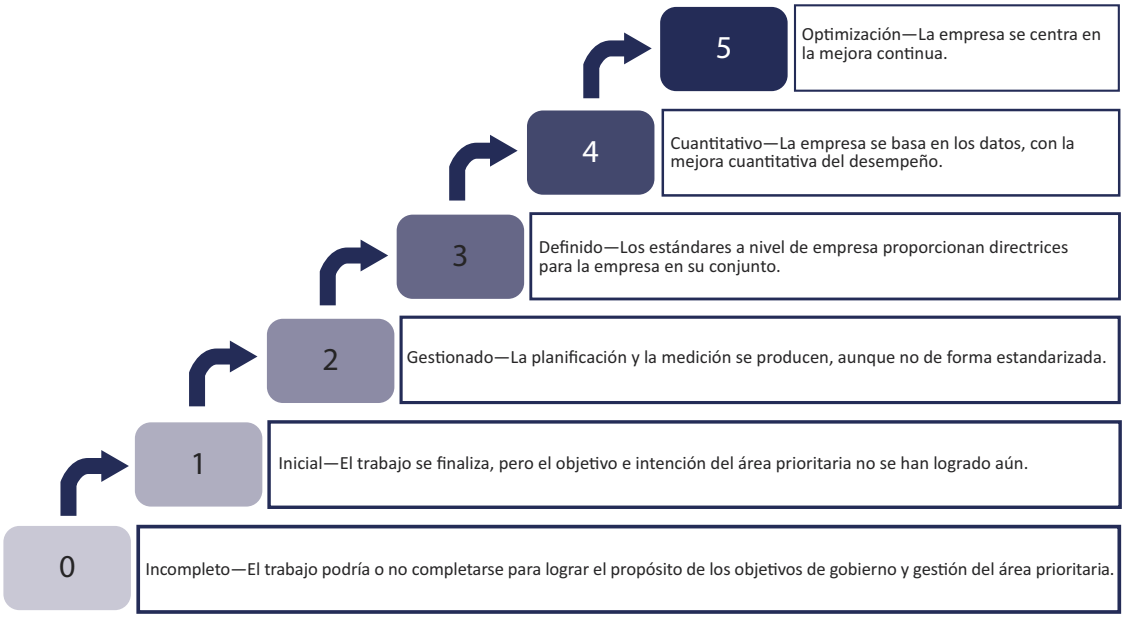
Un nivel de capacidad puede alcanzarse en distinto grado, lo cual puede expresarse mediante una serie de calificaciones. El rango de calificaciones disponible depende del contexto en el que se realiza la evaluación del desempeño:

- Algunos métodos formales que conducen a una certificación independiente usan una serie de calificaciones binarias de aprobado/falla.
- Métodos menos formales (usados con frecuencia en contextos de mejora del desempeño) funcionan mejor con una serie de calificaciones más amplio, como el conjunto siguiente:
  - *Completamente*—El nivel de capacidad se alcanza para más del 85 por ciento. (Este sigue siendo un juicio personal, pero puede corroborarse mediante el examen o evaluación de los componentes del habilitador, como las actividades del proceso, las metas del proceso o las buenas prácticas de la estructura organizativa).
  - *Largamente*—El nivel de capacidad se alcanza para entre el 50 por ciento y el 85 por ciento.
  - *Parcialmente*—El nivel de capacidad se alcanza para entre el 15 por ciento y el 50 por ciento.
  - *No*—El nivel de capacidad se alcanza para menos del 15 por ciento.

6.4.3 Niveles de madurez del área prioritaria

En ocasiones se requiere un nivel más alto para expresar el desempeño sin la granularidad aplicable a las calificaciones individuales de capacidad del proceso. Los niveles de madurez pueden usarse para ese propósito. COBIT® 2019 define los niveles de madurez como una medida de desempeño a nivel del área prioritaria, como se muestra en **la figura 6.3**.

Figura 6.3—Niveles de madurez para áreas prioritarias



Los niveles de madurez están asociados con áreas prioritarias (por ej. una colección de objetivos de gobierno y gestión y los componentes subyacentes) y un cierto nivel de madurez se alcanzará si todos los procesos incluidos en el área prioritaria alcanzan ese nivel de capacidad específico.

6.5 Gestión del desempeño de otros componentes del sistema de gobierno

6.5.1 Gestión del desempeño de las estructuras organizativas

Aunque no existe ningún método formal ni aceptado de forma general para evaluar las estructuras organizativas, pueden evaluarse de modo menos formal según los criterios siguientes. Para cada criterio, pueden definirse una serie de subcriterios, relacionados con los distintos niveles de capacidad. Los criterios son:

- La ejecución satisfactoria de esas prácticas del proceso ante los que la estructura (o rol) organizativo rinde cuentas o es responsable [una A o una R, respectivamente, en una matriz de asignación de responsabilidades por cargo. R: Responsable,A: Quien rinde cuentas, C: Consultado, I: Informado (RACI)]
- La aplicación satisfactoria de una serie de buenas prácticas para estructuras organizativas, como:
  - Principios operativos
    - La estructura organizativa se establece formalmente.
    - La estructura organizativa tiene un mandato claro, documentado y bien entendido.
    - Se documentan los principios operativos.
    - Las reuniones regulares tienen lugar conforme se define en los principios operativos.
    - Los informes/actas de reuniones están disponibles y son útiles.
  - Composición
    - La estructura organizativa se establece formalmente.

  - Alcance (Span) del control
    - La estructura organizativa tiene un mandato claro, documentado y bien entendido.
    - Se documentan los principios operativos.
    - Las reuniones regulares tienen lugar conforme se define en los principios operativos.
    - Los informes/actas de reuniones están disponibles y son útiles.
  - Nivel de autoridad y derechos de decisión
    - Los derechos de decisión de la estructura organización están definidos y documentados.
    - Los derechos de decisión de la estructura organizativa son respetados y cumplidos (también un asunto de cultura/comportamiento).
  - Delegación de autoridad
    - La delegación de autoridad se implementa de forma significativa.
  - Procedimientos de escalamiento
    - Los procedimientos de escalamiento se definen y aplican.
- La aplicación satisfactoria de una serie de prácticas de gestión de estructuras organizativas (prácticas no funcionales que surgen desde el punto de vista de la estructura organizativa):
  - Los objetivos de desempeño de las estructuras organizativas se identifican.
  - El desempeño de las estructuras organizativas se planifica y supervisa.
  - El desempeño de la estructura organizativa se ajusta para cumplir con los planes.
  - Los recursos e información necesarios para las estructuras organizativas se identifican, se ponen a disposición, se asignan y se utilizan.
  - Las interfaces entre la estructura organizativa y otras partes interesadas se gestionan para garantizar una comunicación eficaz y una asignación clara de responsabilidad.
  - Las evaluaciones regulares resultan en la mejora continua requerida de la estructura organizativa, en su composición, mandato o cualquier otro parámetro.

En cuanto a los procesos, los niveles de capacidad bajos requieren que se satisfaga un subconjunto de estos criterios, y niveles de capacidad altos requieren que se satisfagan todos los criterios. Pero, como ya se ha indicado, no existe un esquema generalmente aceptado para evaluar estructuras organizativas. Sin embargo, esto no evita que una empresa defina su propio esquema de capacidades para estructuras organizativas.

6.5.2 Gestión de desempeño de elementos de información

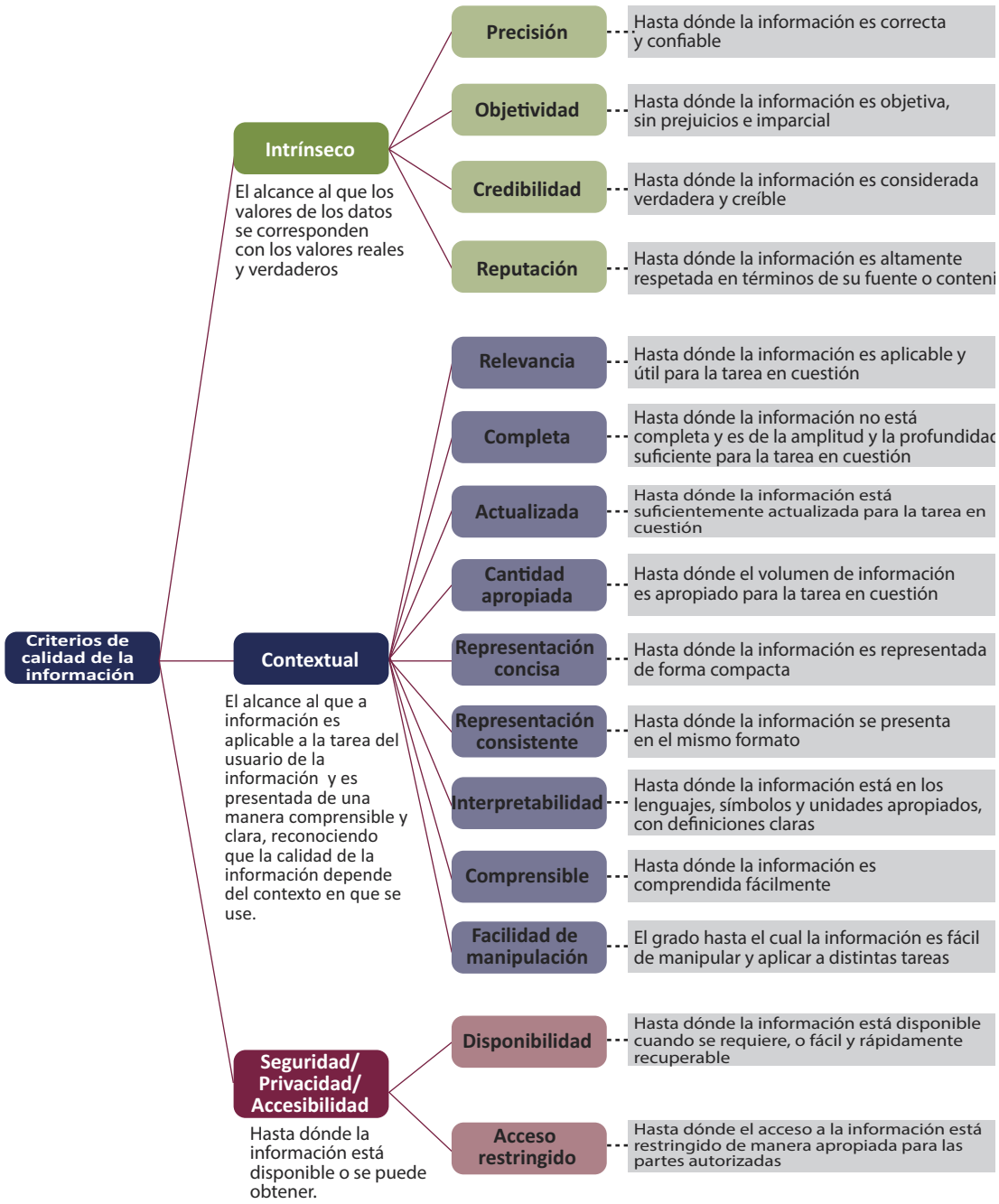
El componente del elemento de información para un sistema de gobierno de I&T es más o menos equivalente a los productos de trabajo del proceso como se describe en el *Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión*.

Aunque no existe ningún método formal ni aceptado de forma general para evaluar los elementos de información, pueden evaluarse de modo menos formal según el modelo de referencia de información presentado por primera vez en *COBIT® 5: Información Catalizadora*.[21]

Este modelo define tres criterios de calidad principales para la información y 15 subcriterios, como se muestra en **la figura 6.4**.

21 Ver ISACA, *COBIT® 5: Información catalizadora, sección 3.1.2 Metas, EE. UU., 2013, http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*

Figura 6.4—Modelo de referencia de la información Criterio de calidad para la información



Un elemento de información puede evaluarse considerando el grado de los criterios de calidad relevantes, como se definen en **la figura 6.4**, se han alcanzado.

6.5.3 Gestión del desempeño de la cultura y el comportamiento

Para el componente de gobierno de la cultura y el comportamiento, debería ser posible definir una serie de comportamientos deseables (y/o no deseables) para el buen gobierno y gestión de TI, y asignar distintos niveles de capacidad a cada uno.

Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión define aspectos del componente de la cultura y el comportamiento para la mayoría de objetivos. A partir de ahí, es posible evaluar hasta qué grado se cumplen estas condiciones o comportamientos.

El contenido de áreas prioritarias, que incluyen una serie de comportamientos deseados más detallados, se desarrollará más adelante. Se sugiere al usuario consultar *isaca.org/cobit* para obtener la guía del área prioritaria más reciente y disponible.

Página intencionalmente en blanco

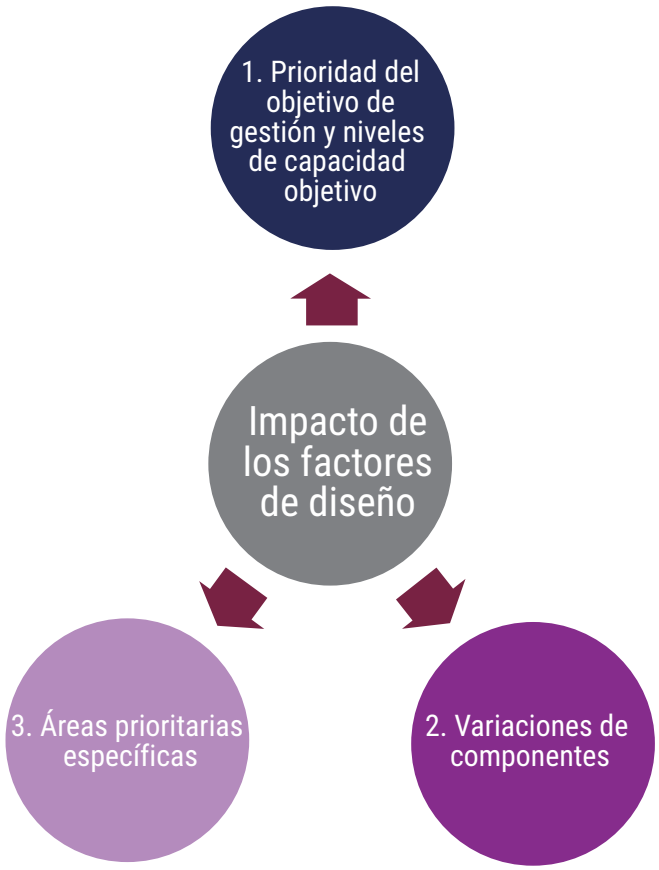
Capítulo 7
Diseño de un sistema de gobierno personalizado

7.1 Impacto de factores de diseño

Esta sección proporciona una visión general a alto nivel del impacto potencial de los factores de diseño de un sistema de gobierno para I&T de la empresa. También describe, a alto nivel, un flujo de trabajo para el diseño personalizado de un sistema de gobierno para la empresa. Puede encontrarse más información sobre estas materias en la *guía de diseño de COBIT® 2019*.

Los factores de diseño influyen de modo distinto en la personalización del sistema de gobierno de una empresa. Esta publicación distingue tres tipos distintos de impacto, ilustrados en **la figura 7.1**.

Figura 7.1—Impacto de los factores de diseño en un sistema de gobierno y gestión



1. **Gestión de prioridad/selección del objetivo**—El modelo core de COBIT incluye 40 objetivos de gobierno y gestión, consistiendo cada uno del proceso y una serie de componentes relacionados. Estos son intrínsecamente equivalentes; no hay ningún orden de prioridad natural entre ellos. Sin embargo, los factores de diseño pueden influir en esta equivalencia y hacer que algunos objetivos de gobierno y gestión sean más importantes que otros, a veces hasta el extremo de que algunos objetivos de gobierno y gestión pasen a ser insignificantes. En la práctica, esta mayor importancia se traduce en el establecimiento de unos niveles de capacidad por alcanzar más altos para objetivos de gobierno y gestión importantes.

Ejemplo: Cuando una empresa identifica la(s) meta(s) más relevante(s) de la lista de metas empresariales y aplica la cascada de metas, esto llevará a una selección de objetivos de gestión prioritarios. Por ejemplo, cuando EG01 *El portafolio de productos y servicios competitivos* es calificado muy alto por una empresa, hará que el objetivo de gestión APO05 *Gestionar el portafolio* sea una parte importante de este sistema de gobierno de la empresa.

Ejemplo: Una empresa que es muy adversa al riesgo dará más prioridad a los objetivos de gestión que aspiren a gobernar y gestionar el riesgo y la seguridad. Objetivos de gobierno y gestión del EDM03 *Asegurar la optimización del riesgo*, APO12 *Gestionar riesgos,* APO13 *Gestionar la seguridad* y DSS05 *Gestionar los servicios de seguridad* se convertirán en una parte importante de ese sistema de gobierno de la empresa y tendrá unos niveles de capacidad objetivos más altos definidos para ellos.

Ejemplo: Una empresa que opera en un entorno de grandes amenazas requerirá un alto nivel de capacidad de los procesos relacionados con la seguridad: APO13 *Gestionar la seguridad* y DSS05 *Gestionar los servicios de seguridad.*

Ejemplo: Una empresa en la que el rol de TI es estratégico y crucial para el éxito del negocio requerirá una gran participación de los roles relacionados con TI en las estructuras organizativas, un conocimiento profundo del negocio por parte de los profesionales de TI (y viceversa) y un foco en procesos estratégicos como APO02 *Gestionar la estrategia* y APO08 *Gestionar las relaciones*.

2. **Variación de componentes**—Los componentes deben alcanzar los objetivos de gobierno y gestión. Algunos factores de diseño pueden influir en la importancia de uno o más componentes o pueden requerir variaciones específicas.

Ejemplo: Las pequeñas y medianas empresas podrían no necesitar un conjunto completo de roles y estructuras organizativas, como se mostraba en el modelo core de COBIT, pero podrían usar una serie reducida. Esta serie reducida de objetivos de gobierno y gestión y los componentes incluidos se define en el área prioritaria de pequeñas y medianas empresas.[22]

Ejemplo: Una empresa que opera en un entorno muy regulado podría atribuir mayor importancia a *productos de trabajo y políticas y procedimientos documentados* y algunos roles, como la función de oficial de cumplimiento.

Ejemplo: Una empresa que usa DevOps en el desarrollo de soluciones y operaciones requerirá actividades específicas, estructuras organizativas, cultura, etc., centradas en BAI03 *Gestionar la identificación y construcción de soluciones* y DSS01 *Gestionar las operaciones*.

3. **Necesidad para áreas prioritarias específicas**—Algunos factores de diseño, como el panorama de amenazas, riesgo específico, métodos de desarrollo a cumplir y configuración de la infraestructura, impulsará la necesidad para variar el contenido del modelo core de COBIT para un contexto determinado.

Ejemplo: Las empresas que adoptan un método DevOps requieren un sistema de gobierno con una variante de diversos procesos de COBIT genéricos, descritos en la guía del área prioritaria de DevOps[23] para COBIT.

Ejemplo: Las pequeñas y medianas empresas tienen menos personal, menos recursos de TI, y líneas de mando jerárquicas más cortas y directas, y difieren en muchos aspectos de las empresas grandes. Por ese motivo, su sistema de gobierno para I&T tendrá que ser menos costoso, comparado con las grandes empresas. Esto se describe en la guía del área prioritaria de PYMES de COBIT.[24]

22 En el momento de la publicación de *Marco de referencia COBIT® 2019: Introducción y metodología, el contenido del área prioritaria de pequeñas y medianas empresas estaba en desarrollo y no se había publicado aún.*

23 En el momento de la publicación de *Marco de referencia COBIT® 2019: Introducción y metodología, el contenido del área prioritaria de DevOps estaba en desarrollo y no se había publicado.*

24 En el momento de la publicación de *Marco de referencia COBIT® 2019: Introducción y metodología, el contenido del área prioritaria de pequeñas y medianas empresas estaba en desarrollo y no se había publicado aún.*

7.2 Fases y pasos del proceso de diseño

La figura 7.2 ilustra el flujo propuesto para el diseño de un sistema de gobierno personalizado.

Figura 7.2—Flujo de trabajo del diseño del sistema de gobierno

Las distintas fases y pasos del proceso de diseño, como se ilustran en **la figura 7.2**, resultarán en recomendaciones para priorizar los objetivos de gobierno y gestión o componentes del sistema de gobierno relacionados con estos, para alcanzar niveles de capacidad, o para adoptar variantes específicas de un componente del sistema de gobierno.

Algunos de estos pasos o sub-pasos podrían derivar en recomendaciones contradictorias, lo cual es inevitable cuando se consideran un gran número de factores de diseño, la naturaleza genérica en su conjunto de la guía del factor de diseño y las tablas de correspondencia utilizadas.

Se sugiere poner todas las recomendaciones obtenidas durante los distintos pasos en un canvas de diseño y, en la última fase del proceso de diseño, resolver (hasta donde sea posible) los conflictos entre los elementos del canvas de diseño y acabar el diseño. No hay una fórmula mágica. El diseño final será una decisión que variará según el caso, dependiendo de todos los elementos del canvas de diseño. Si siguen estos pasos, las empresas lograrán un sistema de gobierno adaptado a sus necesidades.

Página intencionalmente en blanco

Capítulo 8
Implementar el gobierno de TI de la empresa

8.1 Propósito de la guía de implementación COBIT

La *Guía de implementación de COBIT® 2019* destaca una visión de gobierno de I&T que abarca toda la empresa. Esta guía reconoce que I&T está en todas las área de las empresas y que no es ni posible ni es una buena práctica separar las actividades empresariales y las de TI. El gobierno y gestión de I&T de la empresa debería, por tanto, implementarse como una parte integral del gobierno de la empresa, cubriendo todas las áreas de responsabilidad funcionales de TI y del negocio.

Una de las razones comunes de por qué algunas implementaciones de sistemas de gobierno fracasan es que no se inician y se gestionan apropiadamente como programas para asegurar que se obtengan los beneficios. Los programas de gobierno deben estar patrocinados por la dirección ejecutiva, tener un alcance apropiado y definir objetivos que sean alcanzables. Esto permite a la empresa asimilar el ritmo del cambio según lo previsto. La gestión de programas se aborda, por ello, como una parte íntegra del ciclo de vida de la implementación.

También se asume que mientras que se recomienda un enfoque de programa y proyecto para impulsar de forma eficaz iniciativas de mejora, la meta es además establecer una práctica empresarial normal y un método sostenible para gobernar y gestionar las I&T empresariales como cualquier otro aspecto del gobierno de la empresa. Por este motivo, el método de implementación está basado en empoderar a las partes interesadas de la empresa y de TI y los distintos actores que se apropien de las decisiones y actividades de gobierno y gestión relacionados con TI facilitando y permitiendo el cambio. El programa de implementación se cierra cuando el proceso para centrarse en las prioridades relacionadas con TI y la mejora del gobierno genera un beneficio medible, y el programa ha pasado a integrarse en la actividad empresarial continua.

Puede encontrarse más información sobre estas materias en la *Guía de implementación de COBIT® 2019*.

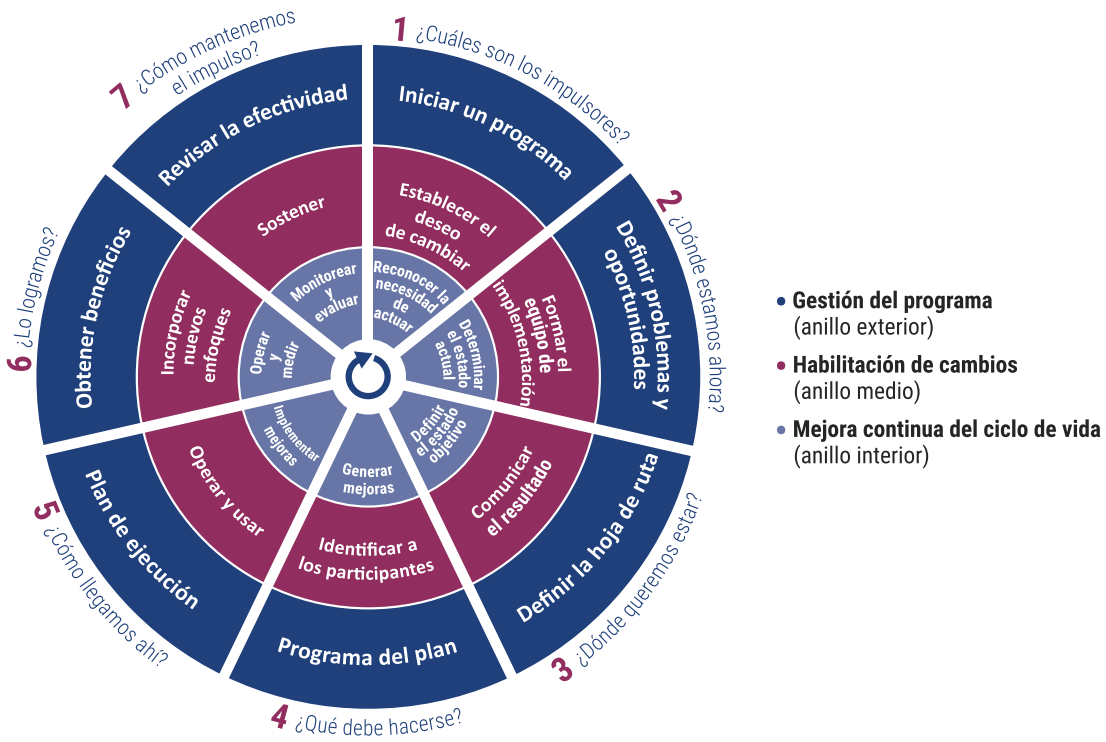
8.2 Método de Implementación de COBIT

Hay siete fases que componen el método de implementación de COBIT:

- ¿Cuáles son los impulsores?
- ¿Dónde estamos ahora?
- ¿Dónde queremos estar?
- ¿Qué debe hacerse?
- ¿Cómo llegamos ahí?
- ¿Lo logramos?
- ¿Cómo mantenemos el impulso?

El método de Implementación de COBIT se resume en **la figura 8.1**.

Figura 8.1—Hoja de ruta de implementación COBIT



8.2.1 Fase 1: ¿Cuáles son los impulsores?

La fase 1 del método de implementación identifica los impulsores de cambio actuales y crea a nivel de la gestión ejecutiva el deseo de cambiar que se expresa como una descripción de un caso de negocio. Un impulsor del cambio es un evento interno o externo, una condición o problema importante que sirve como estímulo para el cambio. Eventos, tendencias (industria, mercado o técnica), falta de rendimiento, implementaciones de software e incluso las metas empresariales pueden actuar todos como impulsores del cambio.

El riesgo asociado a la implementación del propio programa se describe en el caso de negocio y se gestiona a lo largo del ciclo de vida. La preparación, mantenimiento y monitorización de un caso de negocio son disciplinas fundamentales e importantes para justificar, apoyar y a continuación garantizar resultados satisfactorios para cualquier iniciativa, incluida la mejora del sistema de gobierno. Ellos aseguran un foco continuo en los beneficios del programa y su obtención.

8.2.2 Fase 2: ¿Dónde estamos ahora?

La fase 2 alinea los objetivos relacionados con I&T con las estrategias y el riesgo empresarial y prioriza las metas empresariales más importantes, alineando metas y procesos. La *Guía de diseño COBIT® 2019* proporciona distintos factores de diseño para contribuir a la selección.

Dependiendo de las metas empresariales y de las relacionadas con TI seleccionadas y otros factores de diseño, la empresa debe identificar los objetivos de gobierno y gestión críticos y los procesos subyacentes que tengan la capacidad suficiente para asegurar resultados satisfactorios. La dirección debe conocer su capacidad actual y dónde podría haber deficiencias. Esto puede lograrse mediante una evaluación del estado actual de la capacidad de los procesos seleccionados.

8.2.3 Fase 3: ¿Dónde queremos estar?

La fase 3 establece un objetivo de mejora seguido de un análisis de brechas para identificar posibles soluciones.

Algunas soluciones serán ganancias rápidas y otras serán tareas más retadoras a largo plazo. La prioridad debería otorgarse a los proyectos cuya consecución resulte más fácil y que probablemente proporcionen los mayores beneficios. Las tareas a más largo plazo deben desglosarse en partes gestionables.

8.2.4 Fase 4: ¿Qué debe hacerse?

La fase 4 describe cómo planificar soluciones factibles y prácticas definiendo proyectos apoyados por casos de negocio justificables y un plan de cambio para la implementación. Un caso de negocio bien desarrollado puede contribuir a garantizar que los beneficios del proyecto se identifiquen y monitoricen continuamente.

8.2.5 Fase 5: ¿Cómo llegamos ahí?

La fase 5 contempla la implementación de las soluciones propuesta a través de prácticas diarias y estableciendo medidas y sistemas de monitorización para garantizar que se logra el alineamiento con el negocio, y poder medir el desempeño.

Para tener éxito, se requiere conciencia, comunicación, comprensión y compromiso por parte de la alta dirección, y propiedad de los dueños de los procesos del negocio y de TI afectados.

8.2.6 Fase 6: ¿Lo logramos?

La fase 6 se centra en la transición sostenible de las prácticas de gobierno y gestión mejoradas a operaciones empresariales normales. Se centra además en la monitorización de las mejoras usando las métricas de desempeño y los beneficios esperados.

8.2.7 Fase 7: ¿Cómo mantenemos el impulso?

La fase 7 revisa el éxito general de la iniciativa, identifica otros requerimientos de gobierno y gestión y refuerza la necesidad de una mejora continua. También prioriza más oportunidades para mejorar el sistema de gobierno.

La gestión de programas y proyectos se basa en buenas prácticas y proporciona puntos de control en cada una de las siete fases para garantizar que el desempeño del programa va por buen camino, el caso de negocio y el riesgo están actualizados, y la planificación de la fase siguiente se ha ajustado como corresponde. Se asume que el enfoque estándar de la empresa se seguirá.

Puede encontrarse más ayuda sobre la gestión de programas y proyectos en los objetivos de gestión de COBIT BAI01 *Gestionar los programas* y BAI11 *Gestionar los proyectos*. Aunque la presentación de informes no se menciona de forma explícita en ninguna de las fases, se trata de un hilo continuo durante todas las fases e iteraciones.

8.3 Relación entre la Guía de diseño *COBIT® 2019* y la Guía de implementación *COBIT® 2019*

El flujo de trabajo explicado en la *Guía de diseño COBIT® 2019* tiene los siguientes puntos de conexión con la *Guía de implementación de COBIT® 2019*. La *Guía de diseño COBIT® 2019* elabora una serie de tareas definidas en la *Guía de implementación de COBIT® 2019*. **La figura 8.2** muestra una visión general panorámica de estos puntos de conexión. Puede encontrarse más información detallada en la *Guía de diseño COBIT® 2019*.

Figura 8.2—Puntos de conexión entre *la Guía de diseño COBIT* y *la Guía de implementación COBIT*

Guía de implementación COBIT		*Guía de diseño COBIT*
Fase 1:¿Cuáles son los impulsores? [Tareas de mejora continua (por sus siglas en ingles, CI)]	→	**Paso 1:**Entender el contexto y estrategia de la empresa.
Fase 2:¿Dónde estamos ahora? (tareas CI)	→	**Paso 2:**Determinar el alcance inicial del sistema de gobierno **Paso 3:**Perfeccionar el alcance del sistema de gobierno **Paso 4:**Finalizar el diseño del sistema de gobierno
Fase 3:¿Dónde queremos estar? (tareas CI)	→	**Paso 4:**Finalizar el diseño del sistema de gobierno.

Capítulo 9
Comience con COBIT: Construyendo el Caso

9.1 Caso de negocio

La práctica empresarial común dicta la preparación de un caso de negocio para analizar y justificar el inicio de un gran proyecto y/o la inversión financiera. Este ejemplo se proporciona como una guía no prescriptiva, genérica para fomentar la preparación de un caso de negocio para justificar la inversión en un programa de implementación GETI. Cada empresa tiene sus propios motivos para mejorar el GETI y su propio método para la preparación de casos de negocio. Esto puede ir desde un método detallado con el énfasis en beneficios cuantificados a una perspectiva cualitativa de mayor nivel. Las empresas deberían seguir enfoques de casos de negocios internos y justificaciones de inversión actuales, si existen. Este ejemplo y las directrices de esta publicación se proporcionan para ayudar a centrarse en los temas que deberían abordarse en un caso de negocio.

> *El supuesto a modo de ejemplo es Acme Corporation, una gran empresa multinacional con una mezcla de unidades de negocio tradicionales y consolidadas, así como negocios basados en Internet que adoptan las últimas tecnologías. Muchas de las unidades de negocio se han adquirido y existen en varios países con distintos entornos políticos, culturales y económicos locales. El equipo central de la dirección ejecutiva se ha visto influenciado por las últimas directrices de gobierno empresarial, incluido COBIT, que llevan utilizándose centralmente durante algún tiempo. Quieren asegurarse de que la expansión rápida y la adopción de TI avanzada proporcione el valor esperado; también pretenden gestionar nuevos riesgos significativos. Por tanto, han ordenado a la empresa en su conjunto la adopción de una estrategia GETI uniforme. Esta estrategia incluye la participación de los profesionales de auditorías y riesgos y la presentación de informes anuales internos por parte de la dirección de la unidad de negocio sobre la idoneidad de los controles en todas las entidades.*

Aunque el ejemplo se deriva de situaciones reales, no refleja ninguna empresa actual existente.

9.2 Resumen ejecutivo

Este caso de negocio describe el alcance del programa GETI propuesto para Acme Corporation conforme a COBIT.

Es preciso un caso de negocio propiamente dicho para garantizar que el consejo de administración y las unidades de negocio de Acme Corporation aceptan la iniciativa e identifican los posibles beneficios. Acme Corporation monitorizará el caso de negocio para garantizar que los beneficios esperados se han obtenido.

El alcance, en términos de las entidades empresariales que conforman Acme Corporation, es global. Se admite que se aplicará algún tipo de priorización en todas las entidades durante la fase inicial del programa GETI debido a los recursos limitados del programa.

Varias partes interesadas muestran su interés en los resultados del programa GETI, desde la junta directiva a los gerentes locales de cada entidad de Acme Corporation, así como las partes interesadas externas, como los accionistas y organismos gubernamentales.

Deben tenerse en cuenta algunos problemas significativos, así como el riesgo, de la implementación del programa GETI a la escala global precisada. Uno de los mayores desafíos es la naturaleza emprendedora de muchas de las empresas de internet, así como el modelo de negocio descentralizado o federado que existe dentro de Acme Corporation.

El programa GETI se alcanzará centrándose en la capacidad de los procesos de Acme y otros componentes del sistema de gobierno relacionados con estos, definidos en COBIT, y relevantes para cada unidad de negocio. Los objetivos de gobierno y gestión relevantes y priorizados a los que prestará atención cada entidad se identificarán por medio de un taller facilitado por los miembros del programa GETI. Los objetivos comenzarán con las metas estratégicas y empresariales de cada unidad, así como los supuestos de riesgo empresarial relacionados con TI que corresponden a la unidad de negocio particular.

El objetivo del programa GETI consiste en asegurar que se cuente con un sistema de gobierno adecuado, incluidas las estructuras de gobierno, y que se aumente el nivel de capacidad e idoneidad de los procesos de TI relevantes. La expectativa es que conforme aumente la capacidad de un proceso de TI, lo hagan también su eficiencia y calidad. Simultáneamente, el riesgo asociado disminuirá de forma proporcional. De esta forma, cada unidad de negocio puede alcanzar beneficios empresariales reales.

Una vez que se establece el proceso de evaluación del nivel de capacidad dentro de cada unidad de negocio, se anticipa que las autoevaluaciones seguirán dentro de cada una de ellas a modo de práctica empresarial normal.

El programa GETI se ejecutará en dos fases diferenciadas. La primera fase es la fase de desarrollo, en la que el equipo desarrollará y pondrá a prueba la estrategia y el conjunto de herramientas que se usarán en el conjunto de Acme Corporation. Al final de la fase 1, los resultados se presentarán a la dirección del grupo para su aprobación final. Una vez que se haya obtenido la aprobación final, en forma de caso de negocio aprobado, el programa GETI se desplegará en el resto de la entidad conforme a lo acordado (implementación, fase 2).

Debe tenerse en cuenta que el programa GETI no es el responsable de implementar las acciones correctivas identificadas por cada unidad de negocio. El programa GETI únicamente consolidará e informará de los avances que le haya hecho llegar cada unidad.

La última tarea que deberá completar el programa GETI será la de ofrecer los resultados de forma sostenible de aquí en adelante. Este aspecto requerirá tiempo y bastante debate y desarrollo. Este debate y desarrollo debería desembocar en una mejora de los mecanismos de presentación de informes y cuadros de mandos actual.

Se ha preparado un presupuesto inicial para la fase de desarrollo del programa GETI. El presupuesto se detalla en un calendario aparte. También se establecerá un presupuesto detallado para la fase 2 del proyecto, que la dirección del grupo presentará para su aprobación.

9.3 Antecedentes

GETI es una parte integral del gobierno empresarial en su conjunto y se centra en el desempeño de TI y la gestión de riesgos atribuibles a la dependencia en TI de la empresa.

TI forma parte de las operaciones de las empresas de Acme Corporation. Para muchos, internet es el core de sus operaciones. Por ello, GETI sigue la estructura de gestión del grupo: un formato descentralizado. La dirección de cada unidad de negocio/filial es responsable de asegurar la implementación de los procesos adecuados relevantes para GETI.

Anualmente, la dirección de cada filial importante deberá enviar un informe formal por escrito al comité de riesgos apropiado, que será un subgrupo del consejo de dirección. En este informe se detallará el grado de implementación de la política GETI durante el año financiero. Deberá informarse de aquellas excepciones significativas en cada reunión programada del comité de riesgos correspondiente.

El consejo de dirección, ayudado por los comités de auditoría y riesgo, asegurará que el desempeño del grupo GETI sea evaluado, monitorizado, reportado y publicado en un resumen de cuentas GETI, como parte del informe anual integral de la empresa. El resumen de cuentas se basará en los informes obtenidos de los equipos de riesgo, cumplimiento y auditoría interna y la dirección de cada una de las filiales importantes. Proporcionará, tanto a las partes interesadas internas como externas, toda la información relevante y confiable acerca de la calidad del desempeño del grupo GETI.

Los servicios de auditoría interna proporcionarán el aseguramiento a la dirección y al comité de auditoría sobre la idoneidad y eficacia de GETI.

El riesgo empresarial de las TI se comunicará y debatirá como parte del proceso de gestión de riesgos en los registros de riesgos presentado al comité de riesgos correspondiente.

9.4 Desafíos del negocio

Debido a la naturaleza omnipresente de las TI y al ritmo de evolución de la tecnología, se requiere un marco confiable para controlar de forma adecuada el entorno de TI y evitar brechas de control que pudieran exponer a la empresa a un riesgo inaceptable.

El objetivo no es impedir las operaciones de TI de las distintas entidades operativas. En lugar de ello, se trata de mejorar el perfil de riesgo de las entidades de forma que tenga sentido desde el punto de vista empresarial y proporcionar una mayor eficacia y calidad del servicio al tiempo que se cumple de forma explícita, no solo con la Carta estatutaria del grupo GETI de Acme Corporation, sino también con cualquier otro precepto legislativo, regulatorio y/o contractual.

Algunos ejemplos de puntos de dolor son:[25]

- Complejos esfuerzos de aseguramiento de TI debido a la naturaleza emprendedora de muchas de las unidades de negocio
- Modelos operativos de TI complejos debido a los modelos de negocio basados en servicios de internet en uso
- Entidades dispersas geográficamente formadas por diversas culturas e idiomas
- El modelo de control de negocio descentralizado/federado y enormemente autónomo utilizado por el grupo
- Implementación de niveles razonables de gestión de TI, dado el personal altamente técnico y, en ocasiones, volátil de TI
- El equilibrio de TI frente a los impulsores de la empresa para las capacidades innovadora y la agilidad empresarial y la necesidad de gestionar el riesgo y contar con un control adecuado
- El establecimiento de niveles de riesgo y tolerancia para cada unidad de negocio
- Una necesidad creciente de concentrarse en el cumplimiento de la regulación (privacidad) y los requisitos de cumplimiento contractuales [Sector de tarjetas de pago (PCI)].
- Hallazgos de auditorías regulares sobre controles de TI deficientes relacionados con la calidad del servicio de TI
- Entrega satisfactoria y dentro del plazo de servicios nuevos e innovadores en un mercado altamente competitivo

9.4.1 Análisis de brechas y meta

En la actualidad, no existe una estrategia o marco a nivel de grupo para GETI o uso de buenas prácticas y estándares de TI. Entre las unidades de negocio locales, hay distintos niveles de adopción de buenas prácticas con respecto a GETI. Por ello, tradicionalmente se ha prestado muy poca atención al nivel de capacidad de procesamiento de las TI Según la experiencia adquirida, los niveles son, por lo general, bajos.

El objetivo del programa GETI es, por tanto, aumentar el nivel de capacidad y adecuación de los procesos y controles de TI apropiados para cada unidad de negocio de forma prioritaria.

El resultado debería ser que se ha identificado y articulado un riesgo significativo y que la dirección puede abordar el riesgo e informar sobre su estado. Como el nivel de capacidad de cada unidad de negocio aumenta, la calidad y eficiencia debería aumentar también de forma proporcional y el perfil de riesgo empresarial de TI de cada unidad debería disminuir.

Por último, el valor de negocio debería aumentar, como consecuencia de una GETI eficaz.[26]

25 Esta enumeración es un subgrupo de la enumeración de la sección 4.5 (Factores de diseño) y se incluye también en la *Guía de implementación de COBIT® 2019.*

26 Existe un estudio empírico que respalda esta conclusión. Por ejemplo, ver *op cit De Haes, Joshi y van Grembergen.*

9.4.2 Alternativas consideradas

Existen muchos marcos de TI, cuya misión individual es la de controlar aspectos significativos de las TI. El marco de referencia COBIT es considerado por muchos como el marco de control y GETI más importante del mundo. Ya está siendo implementado por algunas filiales de Acme Corporation.

Acme eligió a COBIT como su marco preferido para la implementación de GETI y debería, por ello, ser adoptado por todas sus filiales.

COBIT no tiene por qué implementarse en su totalidad; solo debe implementarse en aquellas áreas relevantes de la filial o unidad de negocio correspondiente, teniendo en cuenta lo siguiente:

1. La fase de desarrollo de cada entidad en el ciclo de vida del negocio
2. Los objetivos de negocio de cada entidad
3. La importancia de las TI para la unidad de negocio
4. El riesgo empresarial relacionado con las TI al que se enfrenta cada entidad
5. Los requerimientos legales y contractuales
6. Otras razones pertinentes

Si una filial o unidad de negocio específica ha aplicado ya otro marco, o se planifica una implementación en el futuro, la implementación debe corresponderse con COBIT, por razones de elaboración de informes, auditoría y transparencia del control interno.

9.5 Solución propuesta

El programa GETI se planifica en dos fases distintas.

9.5.1 Fase 1. Pre-planificación

La fase 1 del programa GETI es la fase de desarrollo. Durante esta fase del programa, se llevan a cabo los pasos siguientes:

1. Se finaliza la estructura del equipo principal entre las partes interesadas y los implicados en el proyecto.
2. El equipo principal completa la formación básica en COBIT.
3. Se llevan a cabo talleres con el equipo principal para definir una estrategia para el grupo.
4. Se crea una comunidad online dentro de Acme Corporation, para que actúe como foro para el intercambio de conocimientos.
5. Se identifican todas las partes interesadas y sus necesidades.
6. Las estructuras, roles y responsabilidades del consejo, las reglas de toma de decisiones y los acuerdos para la presentación de informes se clarifican y re-alinean, si es necesario.
7. Se desarrolla y mantiene un caso de negocio para el programa GETI, como base para la implementación satisfactoria del programa.
8. Se crea un plan de comunicación para los principios rectores, las políticas y los beneficios esperados a lo largo del programa.
9. Se desarrollan las herramientas de evaluación y elaboración de informes para su uso durante el ciclo de vida del programa y aun después que finalice.
10. Se pone a prueba la estrategia en una entidad local. Esta actividad se realiza para facilitar la logística y el perfeccionamiento de la estrategia y las herramientas.
11. La estrategia perfeccionada se aplica de forma experimental en una de las entidades externas. De este modo se entienden y cuantifican las dificultades que conlleva la ejecución de la fase de evaluación del programa GETI bajo condiciones de negocio más complejas.

12. Se presenta el caso de negocio y la estrategia final, incluido un plan de roll-out ante la dirección ejecutiva de Acme Corporation para su aprobación.

9.5.2 Fase 2. Implementación del programa

El programa GETI se ha diseñado para iniciar un programa continuado de mejora continua, basado en un ciclo de vida facilitado, iterativo, siguiendo los pasos siguientes:

1. Determinar los factores de mejora de GETI tanto desde el punto de vista del grupo Acme Corporation como a nivel de las unidades de negocio.
2. Determinar el estado actual de GETI.
3. Determinar el estado deseado de GETI (tanto a corto como a largo plazo).
4. Determinar que debe implementarse a nivel de la unidad de negocio para facilitar los objetivos de negocio locales, y alinearse así con las expectativas del grupo.
5. Implementar los proyectos de mejora identificados y acordados a nivel de las unidades de negocio locales.
6. Obtener y monitorizar los beneficios.
7. Sostener la nueva forma de trabajo manteniendo el impulso actual.

9.5.3 Alcance del programa

El programa GETI abarcará:

1. Todas las entidades del grupo: Sin embargo, se priorizará a las entidades conforme a la interacción, debido a los recursos limitados del programa.
2. El método de priorización. Deberá acordarse con la dirección de Acme Corporación, pero podría hacerse conforme a lo siguiente:
   a. Tamaño de la inversión
   b. Ingresos/contribución al grupo
   c. Perfil de riesgo desde la perspectiva del grupo
   d. Una combinación de estos criterios
3. La lista de entidades que se cubrirán durante el año financiero actual. Esta lista debería finalizarse y acordarse con la dirección de Acme Corporation.

9.5.4 Metodología del programa y alineamiento

El programa GETI cumplirá su mandato usando una estrategia de taller interactivo impartido en todas las entidades.

La estrategia empieza con los objetivos de negocio y los dueños objetivo, normalmente el CEO y el director financiero (CFO). Esta estrategia debe garantizar que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados del negocio.

Cuando se han cubierto los objetivos de negocio, la prioridad se centra en las operaciones de TI, generalmente bajo el control del director general de tecnología (CTO) o el director de información (CIO). A nivel de operaciones de TI, se consideran más detalles sobre los riesgos y objetivos de negocio relacionados con las TI.

Los objetivos de negocio y TI, así como los riesgos de negocio de TI, se combinan a continuación en una herramienta (basada en las directrices COBIT), que proporcionará una serie de áreas prioritarias dentro de los procesos COBIT para su consideración por parte de la unidad de negocio. De este modo, la unidad de negocio puede priorizar sus medidas correctivas para abordar las áreas de riesgo de TI.

9.5.5 Entregables del programa

Como se ha mencionado anteriormente, un objetivo global del programa GETI es incorporar las buenas prácticas de GETI a las operaciones continuas de las diversas entidades del grupo.

El programa GETI dará lugar a resultados específicos para permitir a Acme Corporation aprovechar la consecución de los objetivos pretendidos. Entre ellos se incluyen:

1. El programa GETI facilitará el intercambio de conocimiento interno a través de la plataforma de intranet y aprovechará las relaciones actuales con los proveedores en beneficio de las unidades de negocio individuales.
2. Se crearán informes detallados de cada facilitación con las unidades de negocio derivados de la herramienta de evaluación del programa GETI. Los informes incluirán:
   a. Los objetivos de negocio priorizados actuales, y los objetivos de TI consiguientes, basados en COBIT
   b. El riesgo relacionado con TI identificado por la unidad de negocio de forma estandarizada, y las áreas prioritarias acordadas en las que se centrará la unidad de negocio dependiendo de los procesos y prácticas de COBIT y otros componentes recomendados.
3. Se crearán informes generales de progreso sobre el alcance de unidades de negocio de Acme Corporation pretendidas por parte del programa GETI.
4. Los informes consolidados del grupo cubrirán:
   a. El progreso de las unidades de negocio involucradas en sus proyectos de implementación acordados, conforme a la monitorización acordada de las métricas de rendimiento
   b. Visión de riesgo de TI consolidado en todas las entidades de Acme Corporation
   c. Requerimientos específicos del comité(s) de riesgos
5. Se generará un informe financiero del presupuesto del programa comparado con el montante actual desembolsado.
6. Se creará una monitorización e informe de beneficios, con respecto a los objetivos y métricas de valor definidos por la unidad de negocio.

9.5.6 Riesgo del programa

A continuación, se muestran lo que se consideran posibles tipos de riesgo para el inicio y continuación satisfactoria del programa GETI de Acme Corporation. El riesgo se mitigará centrándose en la habilitación de cambios y se monitorizará y abordará de forma continua a través de revisiones del programa y un registro del riesgo. Estos tipos de riesgo son:

1. El compromiso y apoyo de la dirección al programa, tanto a nivel de grupo como a nivel de las unidades de negocio locales
2. Demostrar la creación de valor y beneficios reales a cada entidad local a través de la adopción del programa. Las entidades locales deberían querer adoptar el proceso por el valor que crea, en lugar de hacerlo por la política establecida.
3. La participación activa de la dirección local en la implementación del programa
4. Identificar a las partes interesadas clave de cada entidad para su participación en el programa
5. La visión empresarial dentro de los cargos de dirección de TI
6. La integración satisfactoria con cualquier otra iniciativa de gobierno o cumplimiento que exista en el grupo
7. Las estructuras de comités adecuadas para supervisar el programa. Por ejemplo, el progreso del programa GETI en su conjunto podría pasar a ser un punto de la agenda del comité ejecutivo de TI. También deberán constituirse equivalentes locales. Esto podría replicarse a nivel geográfico, así como a nivel de las filiales locales del grupo, donde fuera necesario.

9.5.7 Partes interesadas

En los resultados del programa GETI, se han identificado las partes interesadas siguientes:

1. Comité de riesgos
2. Comité ejecutivo de TI
3. Equipo de gobierno
4. Personal de cumplimiento
5. Dirección regional
6. Dirección ejecutiva a nivel local (incluida la dirección de TI)
7. Servicios de auditoría interna

Se recopilará y publicará una estructura final que contiene los nombres individuales de las partes interesadas después de consultarlo con la dirección del grupo.

El programa GETI precisa que las partes interesadas identificadas proporcionen lo siguiente:

1. Directrices sobre la dirección general del programa GETI. Estas directrices incluyen las decisiones sobre asuntos importantes de gobierno definidos en una matriz RACI del grupo conforme a las directrices de COBIT. También incluye el establecimiento de prioridades, el acuerdo sobre financiación y la aprobación de objetivos de valor.
2. Aceptación de los entregables y monitorización de los beneficios esperados del programa GETI

9.5.8 Análisis de coste-beneficio

El programa debería identificar los beneficios esperados y monitorizar que se está generando el valor real del negocio a partir de la inversión. La gestión local debería motivar y apoyar el programa. Una buena GETI debería derivar en beneficios que se establecerán como objetivos específicos para cada unidad de negocio y se monitorizarán y medirán durante la implementación para asegurar que se han obtenido. Los beneficios incluyen:

1. Maximizar el aprovechamiento de oportunidades de negocio a través de TI, al tiempo que se mitiga el riesgo de negocio relacionado con TI a niveles aceptables, asegurando así que el riesgo se pondera de forma responsable con respecto a la oportunidad en todas las iniciativas empresariales
2. Respaldar los objetivos del negocio mediante inversiones clave e ingresos óptimos de esas inversiones, alineando así directamente las iniciativas y objetivos de TI con la estrategia del negocio
3. Cumplimiento legislativo, regulatorio y contractual al igual que el cumplimiento de los procedimientos y política internos
4. Una estrategia uniforme para medir y monitorizar el progreso, la eficiencia y la eficacia
5. Una mejor calidad en la prestación del servicio
6. Un coste más bajo de las operaciones de TI y/o una mayor productividad de TI realizando más trabajo de forma constante con menos tiempo y menos recursos

Los costes centrales incluirán el tiempo requerido para la gestión del programa por parte del grupo, los recursos de asesoría externos y los cursos de formación iniciales. Estos costes centrales se han estimado para la fase 1. El coste de los talleres de evaluación para los directivos de las unidades de negocio y responsables de procesos a título individual (asistencia, lugar de realización del taller, facilitadores y otros costes relacionados) se financiarán localmente y se proporcionará una estimación. Las iniciativas de mejora de proyecto específicas para cada unidad de negocio se estimarán en la fase 2 y se considerarán en base a cada caso y en su conjunto. Esto permitirá al grupo maximizar la eficiencia y la estandarización.

9.5.9 Desafíos y factores de éxito

La figura 9.1 resume los retos que podrían afectar al programa GETI durante el periodo de implementación del mismo y los factores críticos de éxito que deberían abordarse para asegurar un resultado satisfactorio.

Figura 9.1—Desafíos y medidas planificadas de Acme Corporation

Desafío	Factor crítico de éxito —Medidas planificadas
Incapacidad de obtener y mantener el respaldo para mejorar los objetivos	• Mitigar a través de estructuras de comités dentro del grupo (que deberán ser acordadas y constituidas).
Brecha de comunicación entre TI y el negocio	• Involucrar a todas las partes interesadas.
Coste de mejoras superior a beneficios percibidos	• Priorizar la identificación de beneficios.
Falta de confianza y buenas relaciones entre TI y la empresa	• Fomentar una comunicación abierta y transparente acerca del rendimiento, vinculada a la gestión del rendimiento corporativo. • Priorizar las interfaces del negocio y la mentalidad de servicio. • Publicar los resultados positivos y lecciones aprendidas para contribuir a establecer y mantener la credibilidad. • Garantizar que el CIO mantenga la credibilidad y el liderazgo a la hora de generar confianza y relaciones. • Formalizar los roles y responsabilidades de gobierno en el negocio para que quede clara la rendición de cuentas por las decisiones tomadas. • Identificar y comunicar la evidencia de problemas reales, riesgos que deben evitarse y beneficios que deben obtenerse (en términos empresariales) relacionados con las mejoras propuestas. • Priorizar una planificación que facilite los cambios.
Falta de comprensión del entorno de Acme por parte de los responsables del programa GETI	• Aplicar una metodología de evaluación uniforme.
Distintos niveles de complejidad (técnica, organizativa, modelo operativo)	• Tratar a las entidades de forma individualizada. Beneficiarse de las lecciones aprendidas e intercambiar conocimientos.
Entender los marcos, procesos y prácticas de GETI	• Formar y hacer de mentores.
Resistencia al cambio	• Asegurar la implementación del ciclo de vida también incluye cambios en las actividades de facilitación.
Adopción de mejoras	• Facilitar la capacitación local a nivel de entidad.
Dificultad a la hora de integrar GETI en los modelos de gobierno de los socios externos	• Involucrar a proveedores/terceros en las actividades de GETI. • Incorporar condiciones y el derecho a una auditoría en los contratos.
Fallo a la hora de cumplir con los compromisos de implementación de GETI	• Gestionar las expectativas. • Simplificar, ser realistas y prácticos. • Desglosar el proyecto global en proyectos pequeños factibles, logrando experiencia y beneficios.
Intentar no hacer demasiadas cosas a la vez; que TI intente resolver problemas extremadamente difíciles y/o complejos	• Aplicar los principios de gestión del programa y proyecto. • Utilizar hitos. • Priorizar tareas 80/20 (80 por ciento de beneficio con 20 por ciento de trabajo) y tener cuidado a la hora de establecer secuencias en el orden correcto. Capitalizar las ganancias rápidas. • Generar confianza/credibilidad. Contar con las habilidades y experiencias para simplificar y ser prácticos. • Reutilizar lo que ya se tiene como base.

Figura 9.1—Desafíos y medidas planificadas de Acme Corporation *(cont.)*	
Desafío	**Factor crítico de éxito —Medidas planificadas**
TI en modo apagar incendios y/o no priorizar bien y no poder centrarse en GETI	• Aplicar buenas habilidades de liderazgo. • Obtener el compromiso e impulso de la alta dirección para que los empleados puedan centrase en GETI. • Abordar las causas raíz del entorno operativo (intervención externa, dirección priorizando TI). • Aplicar una disciplina más férrea/gestión de peticiones del negocio. • Obtener ayuda externa.
Ausencia de las habilidades y competencias de TI requeridas, como entender el negocio, los procesos, habilidades sociales	• Enfocarse en una planificación de cambio organizativo: ▪ Desarrollo ▪ Capacitación ▪ Coaching ▪ Tutoría ▪ Retroalimentación al proceso de contratación ▪ Entrenamiento / capacitación cruzada
Mejoras no adoptadas ni aplicadas	• Usar una estrategia individual con principios acordados para la entidad local. Su implementación debe ser práctica.
Resulta difícil mostrar o demostrar los beneficios	• Identificar las métricas de desempeño.
Pérdida de interés y motivación	• Generar un compromiso a nivel de grupo, incluida la comunicación.

Página intencionalmente en blanco

Capítulo 10
COBIT y otros estándares

10.1 Reglas/Guia Principal

Una de las reglas de oro que se aplicó a lo largo de todo el desarrollo de COBIT® 2019 fue mantener la posición de COBIT como marco paraguas (umbrela framework). Esto significa que COBIT sigue alineado con una serie de estándares, marcos y/o regulaciones relevantes.

En este contexto, alineamiento significa que COBIT no contradice ninguna directriz de los estándares relacionados. Al mismo tiempo, es importante recordar que COBIT no copia los contenidos de dichos estándares relacionados. En su lugar, suele proporcionar informaciones o referencias equivalentes a las directrices vinculadas.

10.2 Lista de estándares referenciados

Entre los estándares y directrices utilizadas durante el desarrollo de la actualización de COBIT® 2019 se encuentran:

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense,* Versión 6.1, agosto 2016
- Cloud standards and good practices:
  - Amazon Web Services (AWS®)
  - *Security Considerations for Cloud Computing*, ISACA
  - *Controls and Assurance in the Cloud: Using COBIT® 5*, ISACA
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)℠ model, 2014
- CMMI® Development V2.0, CMMI Institute, USA, 2018
- Comité de Organizaciones Patrocinadoras (COSO) Enterprise Risk Management (ERM) Framework, junio 2017
- Comité europeo de normalización (CEN), *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016
- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security 2016*
- Normativa de la Organización Internacional de Normalización / Comisión Electrotécnica Internacional (ISO/CEI)
  - ISO/CIE 20000-1:2011(E)
  - ISO/CIE 27001:2013/Cor.2:2015(E)
  - ISO/CIE 27002:2013/Cor.2:2015(E)
  - ISO/CIE 27004:2016(E)
  - ISO/CIE 27005:2011(E)
  - ISO/CIE 38500:2015(E)
  - ISO/CIE 38502:2017(E)
- Information Technology Infrastructure Library (ITIL®) v3, 2011
- Institute of Internal Auditors® (IIA®), “Core Principles for the Professional Practice of Internal Auditing”
- *King IV Report on Corporate Governance™*, 2016

- Normativa del Instituto de Estándares y Tecnología de Estados Unidos (NIST):
  - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, abril 2018
  - Special Publication 800-37, Revisión 2 (Borrador), mayo 2018
  - Special Publication 800-53, Revisión 5 (Borrador), agosto 2017
- "Options for Transforming the IT Function Using Bimodal IT," *MIS Quarterly Executive* (documentación técnica)
- *A Guide to the Project Management Book of Knowledge: PMBOK® Guide, 6.ª Edición*, 2017
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT™ Reference Architecture, versión 2.0
- The Open Group Standard TOGAF® versión 9.2, 2018
- The TBM Taxonomy, The TBM Council