

# COBIT®



*Habilitando Processos*

COBIT®  
AN ISACA® FRAMEWORK

## ISACA®

Com 95.000 membros em 160 países, a ISACA ([www.isaca.org](http://www.isaca.org)) é líder global no fornecimento de informações, certificações, padrões, apoio e experiência para a garantia e segurança relacionadas a sistemas de informação (SI), governança corporativa e gestão da Tecnologia da Informação (TI), além de conformidade e riscos a ela relacionados. Fundada em 1969, sem fins lucrativos, a ISACA acolhe conferências internacionais independentes, publica o ISACA® Journal e desenvolve padrões internacionais para auditoria e controle de SI que ajudam seus membros a garantir a confiança e o valor dos sistemas de informação. Também promove e certifica os seguintes conhecimentos e habilidades de ponta a ponta em TI que são mundialmente respeitadas Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) e Certified in Risk and Information Systems Control™ (CRISC™). A ISACA atualiza continuamente o COBIT®, o que ajuda os profissionais de TI e os líderes organizacionais a cumprirem suas responsabilidades de gestão e governança de TI, especialmente nas áreas de garantia, segurança, risco e controle, e entrega de valor para o negócio.

## QUALITY STATEMENT

*This Work is translated into Brazilian Portuguese from the English language version of COBIT® 5 Enabling Processes by the ISACA® São Paulo Chapter with the permission of ISACA®. The ISACA® São Paulo Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.*

## DECLARAÇÃO DE QUALIDADE

Esta obra foi traduzida da versão em Inglês do COBIT® 5 Enabling Process para o Português Brasileiro sob coordenação do ISACA Capítulo São Paulo detentor da permissão legal outorgada pela ISACA. O Capítulo São Paulo da ISACA assume total responsabilidade pela precisão e fidelidade da tradução.

## DISCLAIMER

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

## AVISO LEGAL

A ISACA desenvolveu esta publicação, o COBIT® 5 Enabling Process (a 'Obra'), essencialmente como um recurso educacional para profissionais de Governança Corporativa de TI (GEIT), garantia, risco e segurança. A ISACA não afirma que o uso de qualquer parte da Obra garantirá um resultado bem-sucedido. A Obra não deve ser considerada como contendo todas as informações, procedimentos e testes adequados ou exclusiva de outras informações, procedimentos e testes que sejam voltados à obtenção dos mesmos resultados. Ao determinar a adequação de qualquer informação, procedimento ou teste específico, os leitores deverão aplicar seu próprio julgamento profissional às circunstâncias específicas de GEIT, garantia, risco e segurança apresentados pelos sistemas ou ambientes de tecnologia da informação particulares.

## DIREITOS RESERVADOS

© 2012 ISACA. All rights reserved. For usage guidelines, see [www.isaca.org/COBITuse](http://www.isaca.org/COBITuse).

## ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
Email: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

COBIT® 5: Habilitando Processos  
ISBN 978-1-60420-287-8

---

Feedback: [www.isaca.org/cobit](http://www.isaca.org/cobit)

Participate in the ISACA Knowledge Center: [www.isaca.org/knowledge-center](http://www.isaca.org/knowledge-center)

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join the COBIT conversation on Twitter: #COBIT

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOFFICIAL>

Like ISACA on Facebook: [www.facebook.com/ISACAHQ](http://www.facebook.com/ISACAHQ)

**Página intencionalmente deixada em branco**

## RECONHECIMENTOS

### **ISACA DESEJA RECONHECER:**

#### **COBIT 5 Força Tarefa (2009-2011)**

John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA, Co-chair

Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MinstISP, Ravenswood Consultants Ltd., UK, Co-chair

Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia

Elisabeth Judit Antonsson, CISM, Nordea Bank, Sweden

Steven A. Babb, CGEIT, CRISC, Betfair, UK

Steven De Haes, Ph.D., University of Antwerp Management School, Belgium

Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Australia

Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria

Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, USA

Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, The Netherlands

Vernon Richard Poole, CISM, CGEIT, Sapphire, UK

Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India

#### **Equipe de desenvolvimento**

Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Belgium

Gert du Preez, CGEIT, PwC, Canada

Stefanie Grijp, PwC, Belgium

Gary Hardy, CGEIT, IT Winners, South Africa

Bart Peeters, PwC, Belgium

Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgium

#### **Participantes do Workshop**

Gary Baker, CGEIT, CA, Canada

Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, USA

Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, South Africa

Ken Buechler, CGEIT, CRISC, PMP, Great-West Life, Canada

Don Caniglia, CISA, CISM, CGEIT, FLMI, USA

Mark Chaplin, UK

Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii at Manoa, USA

Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, USA

Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Switzerland

Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA

James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA

Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA

Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia

Nicole Lanza, CGEIT, IBM, USA

Philip Le Grand, PRINCE2, Ideagen Plc, UK

Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA

Stuart MacGregor, Real IRM Solutions (Pty) Ltd., South Africa

Christian Nissen, CISM, CGEIT, FSM, CFN People, Denmark

Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, UK

Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgium

Michael Semrau, RWE Germany, Germany

Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia

Alan Simmonds, TOGAF9, TCSA, PreterLex, UK

Cathie Skoog, CISM, CGEIT, CRISC, IBM, USA

Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canada

Roger Southgate, CISA, CISM, UK

Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, USA

## RECONHECIMENTOS (CONT.)

Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium  
Greet Volders, CGEIT, Voquals N.V., Belgium  
Christopher Wilken, CISA, CGEIT, PwC, USA  
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, UK

### **Revisores Especialistas**

Mark Adler, CISA, CISM, CGEIT, CRISC, Commercial Metals Company, USA  
Wole Akpose, Ph.D., CGEIT, CISSP, Morgan State University, USA  
Krzysztof Baczkiewicz, CSAM, CSOX, Eracent, Poland  
Roland Bah, CISA, MTN Cameroon, Cameroon  
Dave Barnett, CISSP, CSSLP, USA  
Max Blecher, CGEIT, Virtual Alliance, South Africa  
Ricardo Bria, CISA, CGEIT, CRISC, Meycor GRC, Argentina  
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Belgium  
Donna Cardall, UK  
Debra Chiplin, Investors Group, Canada  
Sara Cosentino, CA, Great-West Life, Canada  
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett Packard, USA  
Philip de Picker, CISA, MCA, National Bank of Belgium, Belgium  
Abe Deleon, CISA, IBM, USA  
James Doss, ITIL Expert, TOGAF 9, PMP, SSGB, EMCCA, EMCISA, Oracle DBA, ITValueQuickStart.com, UK  
Stephen Doyle, CISA, CGEIT, Department of Human Services, Australia  
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions, Inc., USA  
Rafael Fabius, CISA, CRISC, Uruguay  
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Switzerland  
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA  
Kate Gentles, ITValueQuickStart.com, UK  
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, ITIL V3 Trainer, PRINCE2, ISO/IEC 20000 Consultant, Turkey  
Edson Gin, CISA, CISM, CFE, CIPP, SSCP, USA  
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA  
Marcelo Hector Gonzalez, CISA, CRISC, Banco Central Republic Argentina, Argentina  
Erik Guldentops, University of Antwerp Management School, Belgium  
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA  
Angelica Haverblad, CGEIT, CRISC, ITIL, Verizon Business, Sweden  
Kim Haverblad, CISM, CRISC, PCI QSA, Verizon Business, Sweden  
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, South Africa  
Eduardo Hernandez, ITIL V3, HEME Consultores, Mexico  
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, Argentina  
Michelle Hoben, Media 24, South Africa  
Linda Horosko, Great-West Life, Canada  
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants, UK  
Grant Irvine, Great-West Life, Canada  
Monica Jain, CGEIT, CSQA, CSSBB, Southern California Edison, USA  
John E. Jasinski, CISA, CGEIT, SSBB, ITIL Expert, USA  
Masatoshi Kajimoto, CISA, CRISC, Japan  
Joanna Karczewska, CISA, Poland  
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia  
Eddy Khoo S. K., Prudential Services Asia, Malaysia  
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, USA  
Alan S. Koch, ITIL Expert, PMP, ASK Process Inc., USA  
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia

## RECONHECIMENTOS (CONT.)

Jason D. Lannen, CISA, CISM, TurnKey IT Solutions, LLC, USA  
Nicole Lanza, CGEIT, IBM, USA  
Philip Le Grand, PRINCE2, Ideagen Plc, UK  
Kenny Lee, CISA, CISM, CISSP, Bank of America, USA  
Brian Lind, CISA, CISM, CRISC, Topdanmark Forsikring A/S, Denmark  
Bjarne Lonberg, CISSP, ITIL, A.P. Moller - Maersk, Denmark  
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., South Africa  
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA  
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK  
Cindy Marcello, CISA, CPA, FLMI, Great-West Life & Annuity, USA  
Nancy McCuaig, CISSP, Great-West Life, Canada  
John A. Mitchell, Ph.D., CISA, CGEIT, CEng, CFE, CITP, FBCS, FCIIA, QiCA, LHS Business Control, UK  
Makoto Miyazaki, CISA, CPA, Bank of Tokyo-Mitsubishi, UFJ Ltd., Japan  
Lucio Augusto Molina Focazio, CISA, CISM, CRISC, ITIL, Independent Consultant, Colombia  
Christian Nissen, CISM, CGEIT, FSM, ITIL Expert, CFN People, Denmark  
Tony Noblett, CISA, CISM, CGEIT, CISSP, USA  
Ernest Pages, CISA, CGEIT, MCSE, ITIL, Sciens Consulting LLC, USA  
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, UK  
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM, USA  
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, South Africa  
Andy Piper, CISA, CISM, CRISC, PRINCE2, ITIL, Barclays Bank Plc, UK  
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brazil  
Geert Poels, Ghent University, Belgium  
Dirk Reimers, Hewlett-Packard, Germany  
Steve Reznik, CISA, ADP, Inc., USA  
Robert Riley, CISSP, University of Notre Dame, USA  
Martin Rosenberg, Ph.D., Cloud Governance Ltd., UK  
Claus Rosenquist, CISA, CISSP, Nets Holding, Denmark  
Jeffrey Roth, CISA, CGEIT, CISSP, L-3 Communications, USA  
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, USA  
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgium  
Michael Semrau, RWE Germany, Germany  
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia  
Alan Simmonds, TOGAF9, TCSA, PreterLex, UK  
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canada  
Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, USA  
Marcel Sorouni, CISA, CISM, CISSP, ITIL, CCNA, MCDBA, MCSE, Bupa Australia, Australia  
Roger Southgate, CISA, CISM, UK  
Mark Stacey, CISA, FCA, BG Group Plc, UK  
Karen Stafford Gustin, MLIS, London Life Insurance Company, Canada  
Delton Sylvester, Silver Star IT Governance Consulting, South Africa  
Katalin Szenes, CISA, CISM, CGEIT, CISSP, University Obuda, Hungary  
Halina Tabacek, CGEIT, Oracle Americas, USA  
Nancy Thompson, CISA, CISM, CGEIT, IBM, USA  
Kazuhiro Uehara, CISA, CGEIT, CIA, Hitachi Consulting Co., Ltd., Japan  
Rob van der Burg, Microsoft, The Netherlands  
Johan van Grieken, CISA, CGEIT, CRISC, Deloitte, Belgium  
Flip van Schalkwyk, Centre for e-Innovation, Western Cape Government, South Africa  
Jinu Varghese, CISA, CISSP, ITIL, OCA, Ernst & Young, Canada  
Andre Viviers, MCSE, IT Project+, Media 24, South Africa  
Greet Volders, CGEIT, Voquals N.V., Belgium  
David Williams, CISA, Westpac, New Zealand  
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, UK

## RECONHECIMENTOS (CONT.)

Amanda Xu, PMP, Southern California Edison, USA

Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, South Africa

### **ISACA Diretoria**

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President

Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President

Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President

Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President

Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President

Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President

Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President

Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director

Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

### **Diretoria de Conhecimento**

Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman

Michael A. Berardi Jr., CISA, CGEIT, Bank of America, USA

John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore

Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA

Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada

Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

### **Comitê do Modelo (2009-2012)**

Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France, Chairman

Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Belgium, Past Vice President

Steven A. Babb, CGEIT, CRISC, Betfair, UK

Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore

Sergio Fleginsky, CISA, Akzo Nobel, Uruguay

John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, USA Mario C. Micallef, CGEIT, CPAA, FIA, Malta

Anthony P. Noble, CISA, CCP, Viacom, USA

Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MIInstISP, Ravenswood Consultants Ltd., UK

Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retired), Canada

Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Switzerland

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia

Robert E. Stroud, CGEIT, CA Inc., USA

### **ISACA e IT Governance Institute® (ITGI®) Affiliates and Sponsors**

American Institute of Certified Public Accountants Commonwealth Association for Corporate Governance Inc.

FIDA Inform

Information Security Forum

Institute of Management Accountants Inc. ISACA chapters

ITGI France

ITGI Japan

Norwich University

Solvay Brussels School of Economics and Management

Strategic Technology Management Institute (STMI) of the National University of Singapore

University of Antwerp Management School

## RECONHECIMENTOS (CONT.)

Enterprise GRC Solutions Inc.  
Hewlett-Packard

IBM  
Symantec Corp.

### **Voluntários para a Tradução para a Língua Portuguesa**

#### **Coordenadores**

Jose Luis Diniz, Cobit 5 Foundation, ITIL Expert, DNZ Consultoria em TI Ltda.  
Alessandro Manotti, CISA, CISM, Itaú Unibanco

#### **Equipe de tradutores**

Eder de Abreu CISA, CGEIT, CRISC, CobiT Foundation, ITIL Foundation, Deloitte  
Eduardo Massaru Notaro Kono, CISA, COBIT 5, Volkswagen Participações Ltda.  
Erick Shigueru Kumagai, CRISC, CBCP, CobiT (F), Itil v3 (F), BRF  
Fabio Justo Hildebrand CISA, CISSP, CISM, CGEIT, CRISC Dafiti (Global Fashion Group)  
Gustavo Perri Galegale, MSc, PMP, CISA, CRISC, Galegale & Associados Consultores Ltda  
Hubert Thomaz Neto, CRISC, GVT/Vivo  
Juliano Augusto Martins de Oliveira, CISA; CISM; ITIL e COBIT Foundation, Serasa Experian  
Julio Graziano Pontes , CISSP, CISM, ISO27000LA, FireMon  
Leandro Pfeifer Macedo, CRISC, MCSO, ITSM, Lpfeifer Ltda  
Marcos Gonçalves da Silva, CIA, CISA, COBIT 5F, BM&FBOVESPA  
Marcus Zabeu, CISA, CISSP, Itaú Unibanco  
Nestor Nogueira de Albuquerque, ITIL-F, ISO 2000-F, MsC, Consultor, Professor  
Ricardo Morata Canalonga, ITIL Expert, COBIT, ISO 20000, SIX SIGMA, VERAT Services TI  
Rosvelt Silva Santos, CGEIT, ITIL V3 Expert, Cobit 5 Foundation, EGV Consultoria

**Página intencionalmente deixada em branco**

## ÍNDICE

Listas das Figuras.....	13
Capítulo 1 Introdução .....	15
Capítulo 2 Cascata de Objetivos e Métricas para os Objetivos Corporativos e Objetivos de TI .....	17
Cascata de Objetivos do COBIT 5 .....	17
1º Passo. As Direcionadores das Partes Interessadas Influenciam as Necessidades das Partes Interessadas.....	17
2º Passo. Desdobramento das Necessidades das Partes Interessadas em Objetivos Corporativos.....	17
3º Passo. Cascata dos Objetivos Corporativos em Objetivos de TI .....	20
4º Passo. Cascata dos Objetivos de TI em Metas do Habilitador.....	20
Usando a Cascata de Objetivos do COBIT 5 .....	21
Benefícios da Cascata de Objetivos do COBIT 5.....	21
Usando a Cascata de Objetivos do COBIT 5 com atenção .....	21
Utilizando a Cascata de Objetivos do COBIT 5 na Prática.....	21
Métricas.....	21
Métricas dos Objetivos da Organização.....	21
Métricas dos Objetivos de TI .....	23
Capítulo 3 O modelo de processos do COBIT 5.....	27
Gerenciamento de Desempenho do Habilitador .....	29
Capítulo 4 Modelo de Referência de Processos do COBIT 5 .....	31
Processos de Governança e Gestão .....	31
Modelo .....	31
Capítulo 5 Conteúdo do Guia de Referências de Processos do COBIT 5 .....	33
Entradas e Saídas.....	33
Instruções Genéricas para Processos .....	34
Avaliar, Dirigir e Monitorar (EDM).....	37
Alinhar, Planejar e Organizar (APO).....	55
Construir, Adquirir e Implementar (BAI).....	119
Entregar, Serviço e Suporte (DSS).....	169
Monitorar, Avaliar e Analisar (MEA) .....	197
Apêndice A Mapeamento do COBIT5 e Modelos Legados da ISACA.....	211
Apêndice B Mapeamento Detalhado dos Objetivos Corporativos – Objetivos de TI.....	219
Apêndice C Mapcamento Detalhado dos Objetivos de TI – Processos de TI.....	221

**Página intencionalmente deixada em branco**

## LISTA DAS FIGURAS

Figura 1 – Família de Produtos do COBIT 5.....	15
Figura 2 – Objetivo da Governança: Criação de Valor .....	17
Figura 3 – Visão Geral do Desdobramento de Objetivos .....	18
Figura 4 – Objetivos Corporativos do COBIT 5 .....	19
Figura 5 - Objetivos relacionados a TI .....	20
Figura 6 - Exemplos de Métricas de Objetivos da Organização .....	21
Figura 7 - Exemplos de Métricas para Objetivos relacionadas a TI .....	23
Figura 8 - Habilitadores do COBIT 5: Processos .....	27
Figura 9 - Principais Áreas para Governança e Gestão do COBIT 5 .....	31
Figura 10 - Modelo de Referência de Processos do COBIT 5 .....	32
Figura 11 - Saídas .....	34
Figura 12 - Processos de Controle do COBIT 4.1 e Atributos de Capacidade de Processo ISSO/IEC 15504....	35
Figura 13 - Modelos da ISACA incluídos no COBIT 5 .....	211
Figura 14 – Objetivos de Controle do COBIT 4.1 Mapeados para COBIT 5 .....	211
Figura 15 – Práticas Chave do Val IT 2.0 Cobertas pelo COBIT 5 .....	215
Figura 16 – Práticas Chave do Risk IT Cobertas pelo COBIT 5 .....	217
Figura 17 – Mapeamento dos Objetivos Corporativos do COBIT 5 com os Objetivos de TI.....	219
Figura 18 – Mapeamento dos Objetivos de TI do COBIT 5 com os Processos .....	221

**Página intencionalmente deixada em branco**

## CAPÍTULO 1 INTRODUÇÃO

COBIT 5: Habilitando Processos complementa o COBIT 5 (**figura 1**). Esta publicação contém um guia de referência detalhado para os processos definidos no modelo de referência de processo do COBIT 5



Esta publicação está estruturada da seguinte forma

- No capítulo 2, a cascata de objetivos do COBIT 5 – também explicado no modelo do COBIT 5 – é recapitulado e complementado com um conjunto de métricas exemplo para objetivos corporativos e objetivos de TI.
- No capítulo 3, o 5 de COBIT, modelo de processo é explicado e seus componentes definidos. Este capítulo explica que informações são incluídas na seção de informações detalhadas do processo. O modelo de processo do COBIT 5 inclui processos 37 de governança e gestão; este conjunto de processos é o sucessor para os processos do COBIT 4.1, Val IT e Risk IT e inclui todos os processos necessários para o tratamento de fim-a-fim de governança e gestão de empresas de TI.
- O Capítulo 4 apresenta o diagrama do modelo de referência de processos, que foi desenvolvido com base nas melhores práticas, padrões e opinião de especialistas. É importante entender que o modelo e seu conteúdo são genéricos e não prescritivos, e deve ser adaptado para se adequar à empresa. Além disso, a orientação define as práticas e atividades em um nível relativamente elevado e não descreve como o procedimento do processo deve ser definido
- O Capítulo 5 – a principal seção desta publicação – contém informações detalhadas relativas a todos os 37 processos do COBIT 5 incluídos no modelo de referência de processo
- Diversos apêndices também foram incluídos:
  - O Apêndice A contém o mapeamento entre os processos Val IT 2.0 e Risk IT do COBIT 4.1 (e seus objetivos de controle ou práticas de gestão) e seus equivalentes no COBIT 5.
  - Os Apêndices B e C contêm as tabelas de mapeamento da cascata de objetivos, por exemplo, mapeamento de objetivos corporativos em objetivos de TI e objetivos de TI em processos

**Página intencionalmente deixada em branco**

## CAPÍTULO 2

### CASCATA DE OBJETIVOS E MÉTRICAS PARA OS OBJETIVOS CORPORATIVOS E OBJETIVOS DE TI

#### CASCATA DE OBJETIVOS DO COBIT 5

As empresas existem para criar valor para suas partes interessadas. Consequentemente, qualquer empresa — comercial ou não — terá a criação de valor como um objetivo da governança. Criar valor significa realizar benefícios com uma relação ótima em relação ao uso e custos dos recursos enquanto mitiga o risco (ver figura 2). Os benefícios podem assumir muitas formas, por exemplo, financeiros para empresas comerciais ou de serviço público para entidades governamentais



As empresas têm muitas partes interessadas e ‘criar valor’ significa coisas diferentes — e por vezes conflitantes — para cada um deles. Governança tem a ver com negociar e decidir entre os interesses de valor das diversas partes interessadas. Por consequência, o sistema de governança deve considerar todos as partes interessadas ao tomar decisões sobre a avaliação dos recursos, benefícios e riscos. Para cada decisão, as seguintes perguntas podem e devem ser feitas: Para quem são os benefícios? Quem assume o risco? Que recursos são necessários?

As necessidades das partes interessadas devem ser transformadas em uma estratégia acionável pela empresa. A cascata de objetivos do COBIT 5 é o mecanismo de tradução das necessidades das partes interessadas em objetivos corporativos específicos, personalizados e acessíveis, objetivos de TI e metas do habilitador. Esta tradução permite a configuração de objetivos específicos em cada nível e em cada área da empresa em apoio aos objetivos gerais e às exigências das partes interessadas.

A cascata de objetivos do COBIT 5 é demonstrado na figura 3.

##### **1º PASSO. AS DIRECIONADORES DAS PARTES INTERESSADAS INFLUENCIAM AS NECESSIDADES DAS PARTES INTERESSADAS**

As necessidades das partes interessadas são influenciadas por diversas tendências, por exemplo, mudanças de estratégia, mudanças nos negócios e no ambiente regulatório bem como novas tecnologias.

##### **2º PASSO. DESDOBRAMENTO DAS NECESSIDADES DAS PARTES INTERESSADAS EM OBJETIVOS CORPORATIVOS**

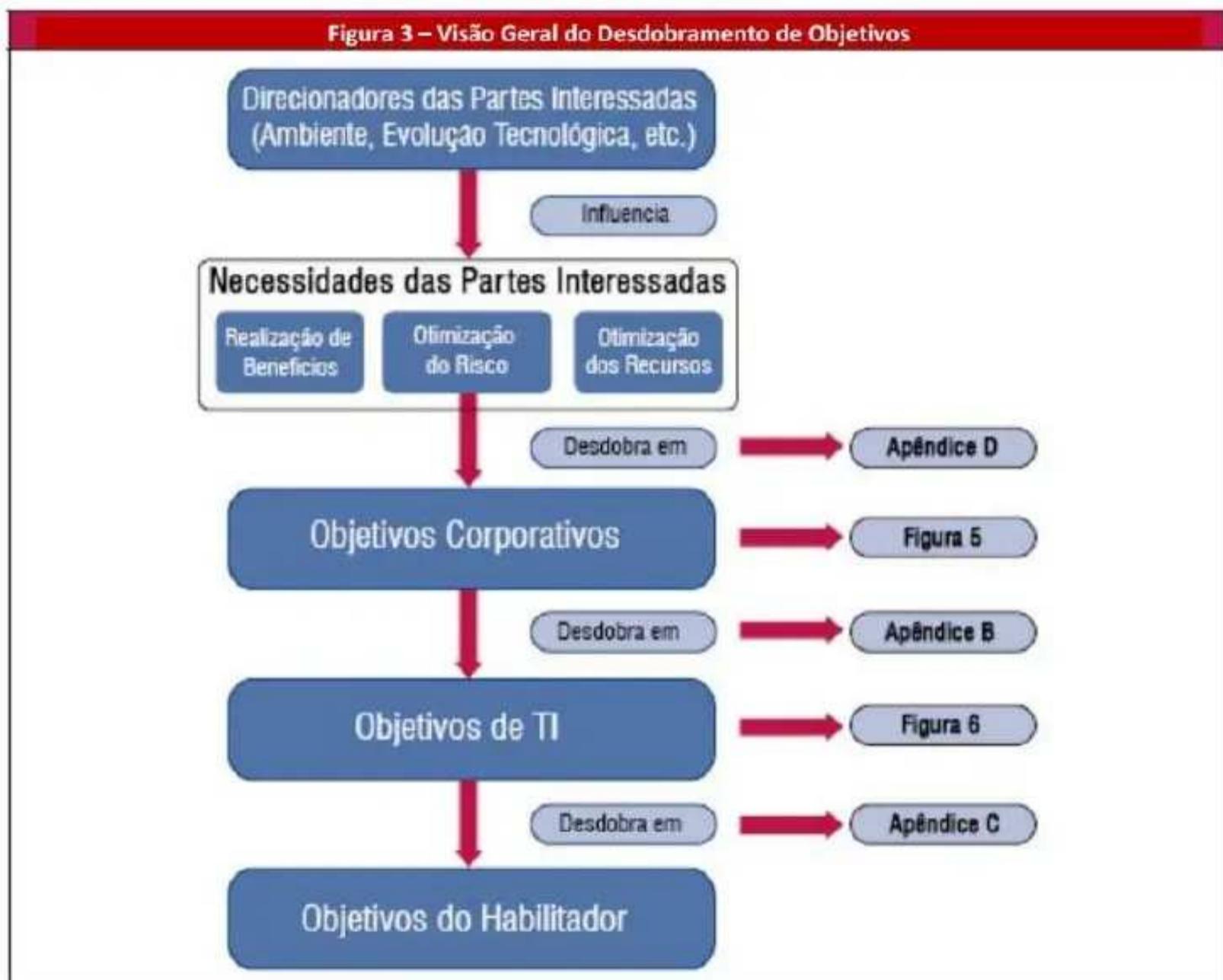
As necessidades das partes interessadas podem estar relacionadas a um conjunto de objetivos corporativos genéricos. Esses objetivos corporativos foram criados usando as dimensões do balanced scorecard (BSC)<sup>1</sup> e representam uma lista dos objetivos mais usados que uma empresa pode definir para si. Embora esta lista não seja completa, a maioria dos objetivos específicos das empresas pode ser mapeada facilmente em um ou mais

<sup>1</sup> Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, EUA, 1996.

dos objetivos corporativos genéricos.

O COBIT 5 define 17 objetivos genéricos, conforme demonstrados na **figura 4**, que incluem as seguintes informações:

- A dimensão BSC sob a qual o objetivo corporativo se enquadra
- Objetivos corporativos
- A relação entre os três principais objetivos da governança – Realização de benefícios, Otimização do risco e Otimização dos recursos ('P' significa relação primária e 'S' relação secundária, ou seja, uma relação mais fraca).



## CAPÍTULO 2: CASCATA DE OBJETIVOS E MÉTRICAS PARA OS OBJETIVOS CORPORATIVOS E OBJETIVOS DE TI

---

**Figura 4 – Objetivos Corporativos do COBIT 5**

Dimensão BSC para o Negócio	Objetivos Corporativos	Relação com os Objetivos da Governança		
		Realização de Benefícios	Otimização de Riscos	Otimização de Recursos
Financeira	01 Valor dos investimentos da empresa percebidos pelas partes interessadas	P		S
	02 Portfólio de produtos e serviços competitivos	P	P	S
	03 Gestão do risco do negócio (salvaguarda de ativos)		P	S
	04 Conformidade com as leis e regulamentos externos		P	
	05 Transparência financeira	P	S	S
Cliente	06 Cultura de serviço orientada ao cliente	P		S
	07 Continuidade e disponibilidade do serviço da empresa		P	
	08 Respostas rápidas para um ambiente de negócios em mudança	P		S
	09 Tomada de decisão estratégica com base na informação	P	P	P
	10 Otimização dos custos de prestação de serviços	P		P
Interno	11 Otimização da funcionalidade do processo de negócio	P		P
	12 Otimização dos custos do processo de negócio	P		P
	13 Gestão de programas de mudanças dos negócios	P	P	S
	14 Produtividade operacional e da equipe	P		P
	15 Conformidade com as políticas internas		P	
Crescimento e Aprendizado	16 Pessoas qualificadas e motivadas	S	P	P
	17 Cultura de inovação de produtos e negócios	P		

**3º PASSO. CASCATA DOS OBJETIVOS CORPORATIVOS EM OBJETIVOS DE TI**

A consecução dos objetivos corporativos exige uma série de resultados de TI<sup>2</sup> que são representados pelos objetivos de TI.

Objetivos de TI significam tudo o que estiver relacionado à tecnologia da informação e tecnologias relacionadas, e são estruturados de acordo com as dimensões do balanced scorecard de TI (IT BSC). O COBIT 5 define 17 objetivos de TI, relacionados na **figura 5**.

**Figura 5 – Objetivos relacionados a TI**

Dimensões BSC para a TI	Objetivo para Tecnologia da Informação Relacionada
Financeira	01 Alinhamento da estratégia do negócio e da TI
	02 Conformidade de TI e suporte para conformidade dos negócios com as leis e regulamentos externos
	03 Compromisso da gestão executiva com a tomada de decisões de TI
	04 Gestão de risco organizacional de TI
	05 Benefícios obtidos pelo investimento de TI e portfólio de serviços
	06 Transparência dos custos, benefícios e riscos de TI
Cliente	07 Prestação de serviços de TI em consonância com os requisitos de negócio
	08 Uso adequado de aplicativos, informações e soluções tecnológicas
Interna	09 Agilidade de TI
	10 Segurança da informação, infraestrutura de processamento e aplicativos
	11 Otimização de ativos, recursos e capacidades de TI
	12 Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão
	15 Conformidade de TI com as políticas internas
Treinamento e Crescimento	16 Equipes de TI e de negócios motivadas e qualificadas
	17 Conhecimento, expertise e iniciativas para inovação dos negócios

A tabela de mapeamento dos objetivos corporativos em objetivos de TI foi incluída no Apêndice B, e demonstra como cada objetivo corporativo é apoiado por diversos objetivos de TI.

**4º PASSO. CASCATA DOS OBJETIVOS DE TI EM METAS DO HABILITADOR**

Atingir os objetivos de TI exige a aplicação e o uso bem-sucedido de diversos habilitadores. Os Habilitadores incluem:

- Princípios, políticas e estruturas
- Processos
- Estruturas Organizacionais
- Cultura, éticas e comportamento
- Informação
- Serviços, infraestrutura e aplicativos
- Pessoas, habilidades e competências

Um conjunto de metas específicas e pertinentes pode ser definido para cada habilitar em apoio aos objetivos de TI. Neste documento, as metas de processo são fornecidas nas descrições detalhadas de processo. Processos são um dos habilitadores, e o Apêndice C contém o mapeamento entre os objetivos de TI e os processos do COBIT 5.

<sup>2</sup> Os resultados de TI não são obviamente o único benefício intermediário necessário para a consecução dos objetivos corporativos. Todas as demais áreas funcionais de uma empresa, tais como finanças e marketing, também contribuem para a consecução dos objetivos corporativos, mas no contexto do COBIT 5 somente as atividades e os objetivos de TI são considerados.

## USANDO A CASCATA DE OBJETIVOS DO COBIT 5

### **BENEFÍCIOS DA CASCATA DE OBJETIVOS DO COBIT 5**

A cascata de objetivos<sup>3</sup> é importante porque permite a definição das prioridades de implementação, melhoria e garantia da governança corporativa de TI com base nos objetivos (estratégicos) da empresa e no respectivo risco. Na prática, a cascata de objetivos:

- Define as metas e objetivos tangíveis e relevantes em vários níveis de responsabilidade
- Filtra a base de conhecimento do COBIT 5, com base nos objetivos corporativos, para extrair a orientação pertinente para inclusão na implementação, melhoria ou garantia de projetos específicos
- Identifica e comunica claramente como (por vezes de forma muito operacional) os habilitadores são importantes para a consecução dos objetivos corporativos

A cascata de objetivos baseia-se na pesquisa realizada pelo Instituto de Governança e Alinhamento de TI da Faculdade de Administração da Universidade de Antuérpia, na Bélgica

### **USANDO A CASCATA DE OBJETIVOS DO COBIT 5 COM ATENÇÃO**

A cascata de objetivos — com suas tabelas de mapeamento entre os objetivos corporativos e os objetivos de TI e entre os objetivos de TI e os habilitadores do COBIT 5 (inclusive processos) — não contém a verdade universal, e os usuários não devem tentar usá-lo de uma forma puramente mecânica, mas sim como uma diretriz. Há várias razões para isso, entre as quais:

- Cada empresa tem prioridades diferentes em seus objetivos, e essas prioridades podem mudar com o tempo
- As tabelas de mapeamento não fazem distinção entre o porte da empresa e/ou o setor em que ela está inserida. Elas representam uma espécie de denominador comum de como, no geral, os diferentes níveis de objetivos se inter-relacionam.
- Os indicadores usados no mapeamento consideram dois níveis de importância ou relevância, sugerindo a existência de ‘discretos’ níveis de relevância, considerando que, de fato, o mapeamento será parecido com uma constante com vários níveis de correspondência

### **UTILIZANDO A CASCATA DE OBJETIVOS DO COBIT 5 NA PRÁTICA**

A partir declaração acima, fica evidente que o primeiro passo que uma empresa sempre deverá dar ao utilizar a cascata de objetivos é personalizar o mapeamento, levando em consideração sua situação específica. Em outras palavras, cada empresa deverá criar sua próprio cascata de objetivos, compará-lo com o COBIT e depois refiná-la. Por exemplo, a empresa poderá desejar:

- Converter as prioridades estratégicas em um “peso” ou importância específica para cada um dos objetivos corporativos.
- Validar os mapeamentos da cascata de objetivos, levando em consideração seu ambiente e setor específicos, etc.

## MÉTRICAS

As páginas a seguir contêm os objetivos corporativos e os objetivos de TI, com métricas de amostra que podem ser usadas para medir a consecução de cada objetivo. Essas métricas são exemplos, e cada empresa deverá analisar a lista cuidadosamente, decidir sobre as métricas pertinentes e atingíveis para seu próprio ambiente e conceber seu próprio sistema de “scorecard”. Além das métricas abaixo, metas e métricas de processo foram incluídas nas descrições detalhadas de processo

### **MÉTRICAS DOS OBJETIVOS DA ORGANIZAÇÃO**

A **figura 6** contém todos os objetivos da organização identificados na publicação da estrutura, com métricas de exemplo para cada.

<sup>3</sup> A cascata de objetivos baseia-se na pesquisa realizada pelo Instituto de Governança e Alinhamento de TI da Faculdade de Administração da Universidade de Antuérpia, na Bélgica.

**Figura 6 – Exemplos de Métricas de Objetivos da Organização**

Dimensão BSC	Objetivo da Organização	Métrica
Financeira	01 Valor dos investimentos da empresa percebidos pelas partes interessadas	<ul style="list-style-type: none"> <li>Percentual de investimentos em que o valor gerado atende às expectativas das partes interessadas</li> <li>Percentual de produtos e serviços em que os benefícios esperados foram realizados</li> <li>Percentual de investimentos em que os benefícios reivindicados foram atingidos ou superados</li> </ul>
	02 Portfólio de produtos e serviços competitivos	<ul style="list-style-type: none"> <li>Percentual de produtos e serviços que atingem ou excedem as metas de receita e/ou participação no mercado</li> <li>Relação de produtos e serviços por fase do ciclo de vida</li> <li>Percentual de produtos e serviços que atingem ou excedem as metas de satisfação do cliente</li> <li>Percentual de produtos e serviços que proporcionam uma vantagem competitiva</li> </ul>
	03 Gestão do risco do negócio (salvaguarda de ativos)	<ul style="list-style-type: none"> <li>Percentual de objetivos de negócios críticos e serviços cobertos pela avaliação de risco</li> <li>Relação de incidentes significativos não identificados nas avaliações de risco em comparação com os incidentes totais</li> <li>Frequência de atualização do perfil de risco</li> </ul>
	04 Conformidade com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo da não conformidade com as normas, inclusive acordos e multas</li> <li>Número de problemas de não conformidade com as normas que causam comentário público ou publicidade negativa</li> <li>Número de problemas de não conformidade com as normas que dizem respeito aos acordos contratuais com parceiros comerciais</li> </ul>
	05 Transparência financeira	<ul style="list-style-type: none"> <li>Percentual de estudos de casos de investimentos com previsão de custos e benefícios claramente definidos e aprovados</li> <li>Percentual de produtos e serviços com custos operacionais e benefícios esperados definidos e aprovados</li> <li>Pesquisa de satisfação dos principais partes interessadas referente à transparência, entendimento e exatidão das informações financeiras da empresa</li> <li>Percentual do custo do serviço que pode ser alocado aos usuários</li> </ul>
Cliente	06 Cultura de serviço orientada ao cliente	<ul style="list-style-type: none"> <li>Número de interrupções de serviço ao cliente devido a incidentes relacionados aos serviços de TI (confiabilidade)</li> <li>Percentual de partes interessadas do negócio satisfeitas com o fato de que a prestação de serviço ao cliente cumpre os níveis definidos</li> <li>Número de reclamações dos clientes</li> <li>Tendência dos resultados da pesquisa de satisfação do cliente</li> </ul>
	07 Continuidade e disponibilidade do serviço da empresa	<ul style="list-style-type: none"> <li>Número de interrupções de serviço ao cliente que causam incidentes significativos</li> <li>Custo dos incidentes para a empresa</li> <li>Número de horas de processamento perdido pela empresa devido a interrupções de serviço não planejadas</li> <li>Percentual de reclamações em função das metas definidas de disponibilidade do serviço</li> </ul>
	08 Respostas rápidas para um ambiente de negócios em mudança	<ul style="list-style-type: none"> <li>Nível de satisfação da diretoria com a capacidade de resposta da empresa às novas exigências</li> <li>Número de produtos e serviços críticos apoiado por processos de negócios atualizados</li> <li>Tempo médio para transformar os objetivos corporativos estratégicos em uma iniciativa validada e aprovada</li> </ul>
	09 Tomada de decisão estratégica com base na informação	<ul style="list-style-type: none"> <li>Grau de satisfação da diretoria e gestão executiva com a tomada de decisão</li> <li>Número de incidentes causado por decisões de negócios incorretas com base em informações imprecisas</li> <li>Tempo para fornecer informações de apoio para permitir decisões de negócios eficazes</li> </ul>
	10 Otimização dos custos de prestação de serviços	<ul style="list-style-type: none"> <li>Frequência das avaliações de otimização do custo da prestação de serviço</li> <li>Tendência da avaliação de custo em comparação com os resultados do nível de serviço</li> <li>Níveis de satisfação da diretoria e da gerência executiva com os custos da prestação de serviço</li> </ul>
Interna	11 Otimização da funcionalidade do processo de negócio	<ul style="list-style-type: none"> <li>Frequência das avaliações de maturidade da capacidade do processo de negócio</li> <li>Tendência dos resultados da avaliação</li> <li>Níveis de satisfação da diretoria e dos executivos com a capacidade dos processos de negócio</li> </ul>
	12 Otimização dos custos do processo de negócio	<ul style="list-style-type: none"> <li>Frequência das avaliações de otimização do custo do processo de negócio</li> <li>Tendência da avaliação de custo em comparação com os resultados do nível de</li> </ul>

## CAPÍTULO 2: CASCATA DE OBJETIVOS E MÉTRICAS PARA OS OBJETIVOS CORPORATIVOS E OBJETIVOS DE TI

**Figura 6 – Exemplos de Métricas de Objetivos da Organização**

Dimensão BSC	Objetivo da Organização	Métrica
		<ul style="list-style-type: none"> <li>serviço</li> <li>Níveis de satisfação da diretoria e da gerência executiva com os custos de processamento do negócio</li> </ul>
	13 Gestão de programas de mudanças dos negócios	<ul style="list-style-type: none"> <li>Número de programas dentro do prazo e do orçamento</li> <li>Percentual de partes interessadas satisfeitas com o resultado do programa</li> <li>Nível de consciência das mudanças no negócio induzidas por iniciativas comerciais capacitadas por TI</li> </ul>
	14 Produtividade operacional e da equipe	<ul style="list-style-type: none"> <li>Número de programas / projetos dentro do prazo e do orçamento</li> <li>Níveis de custos e de pessoal em comparação com os parâmetros de referência (benchmarks)</li> </ul>
	15 Conformidade com as políticas internas	<ul style="list-style-type: none"> <li>Número de incidentes relacionados a não conformidade com a política</li> <li>Percentual de partes interessadas que entendem as políticas</li> <li>Percentual de políticas apoiadas por padrões e práticas de trabalho efetivos</li> </ul>
Aprendizado e Crescimento	16 Pessoas qualificadas e motivadas	<ul style="list-style-type: none"> <li>Nível de satisfação do participante com a expertise e habilidade dos funcionários</li> <li>Percentual de funcionários cujas habilidades são insuficientes para a competência requerida para seu cargo</li> <li>Percentual de funcionários satisfeitos</li> </ul>
	17 Cultura de inovação de produtos e negócios	<ul style="list-style-type: none"> <li>Nível de consciência e entendimento das oportunidades de inovação no negócio</li> <li>Satisfação do participante com os níveis de produto, expertise e ideias inovadoras</li> <li>Número de iniciativas de produtos e serviços aprovadas resultantes de ideias inovadoras</li> </ul>

### **MÉTRICAS DOS OBJETIVOS DE TI**

A figura 7 contém todos os objetivos de TI definidos na cascata de objetivos e inclui métricas de exemplo para cada objetivo.

**Figura 7 – Exemplos de Métricas para Objetivos relacionadas a TI**

Dimensão BSC	Objetivos de TI	Métrica
Financeira	01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de objetivos estratégicos e requisitos do negócio apoiados pelos objetivos estratégicos de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio de programas e serviços planejado</li> <li>Percentual de criadores de valor de TI mapeados em criadores de valor de negócio</li> </ul>
	02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo da não conformidade de TI, inclusive acordos e multas, e o impacto da perda de reputação</li> <li>Número de problemas de não conformidade de TI reportado à diretoria ou que causam comentário público ou constrangimento</li> <li>Número de problemas de não conformidade que dizem respeito aos acordos contratuais com os provedores de serviço de TI</li> <li>Cobertura das avaliações de compliance</li> </ul>
	03 Compromisso da gerência executiva com a tomada de decisões de TI	<ul style="list-style-type: none"> <li>Percentual de cargos na gerência executiva com responsabilidades bem definidas para decisões de TI</li> <li>Número de vezes que TI consta na agenda da diretoria de forma proativa</li> <li>Frequência das reuniões do comitê (executivo) de estratégia de TI</li> <li>Taxa de execução de decisões executivas de TI</li> </ul>
	04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Percentual de processos de negócio críticos, serviços de TI e programas de negócio capacitados por TI cobertos pela avaliação de risco</li> <li>Número de incidentes de TI significativos que não foram identificados na avaliação de risco</li> <li>Percentual de avaliações de risco corporativo que incluem o risco de TI</li> <li>Frequência de atualização do perfil de risco</li> </ul>
	05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	<ul style="list-style-type: none"> <li>Percentual de investimentos em capacidade de TI em que a realização do benefício é monitorada durante todo o ciclo de vida econômico</li> <li>Percentual de serviços de TI em que os benefícios esperados foram realizados</li> <li>Percentual de investimentos em capacidade de TI em que os benefícios reivindicados foram atingidos ou superados</li> </ul>
	06 Transparência dos custos,	<ul style="list-style-type: none"> <li>Percentual de estudos de casos de investimentos com previsão de custos e</li> </ul>

# COBIT® : HABILITANDO PROCESSOS

**Figura 7 – Exemplos de Métricas para Objetivos relacionadas a TI**

Dimensão BSC	Objetivos de TI	Métrica
	benefícios e riscos de TI	<ul style="list-style-type: none"> <li>benefícios de TI claramente definidos e aprovados</li> <li>Percentual de serviços de TI com custos operacionais e benefícios esperados claramente definidos</li> <li>Pesquisa de satisfação das principais partes interessadas referente à transparência, entendimento e exatidão das informações financeiras de TI</li> </ul>
Cliente	07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de interrupções do negócio devido a incidentes com o serviço de TI</li> <li>Percentual de participantes do negócio satisfeitos com o fato de que a prestação de serviço de TI cumpre os níveis de serviço definidos</li> <li>Percentual de usuários satisfeitos com a qualidade da prestação do serviço de TI</li> </ul>
	08 Uso adequado de aplicativos, informações e soluções tecnológicas	<ul style="list-style-type: none"> <li>Percentual de responsáveis por processos de negócio satisfeitos com os produtos e serviços de TI de apoio</li> <li>Nível de entendimento do usuário corporativo de como soluções tecnológicas apoiam seus processos</li> <li>Nível de satisfação dos usuários corporativos com o treinamento e os manuais do usuário</li> <li>Valor líquido atual (NPV) que mostra o nível de satisfação da empresa com a qualidade e utilidade das soluções tecnológicas</li> </ul>
Interna	09 Agilidade de TI	<ul style="list-style-type: none"> <li>Nível de satisfação dos executivos da empresa com a capacidade de resposta de TI às novas exigências</li> <li>Número de processos de negócio críticos apoiados por infraestrutura e aplicativos atualizados</li> <li>Tempo médio para transformar os objetivos estratégicos de TI em uma iniciativa validada e aprovada</li> </ul>
	10 Segurança da informação, infraestrutura de processamento e aplicativos	<ul style="list-style-type: none"> <li>Número de incidentes de segurança que causam prejuízo financeiro, interrupção do negócio ou constrangimento público</li> <li>Número de serviços de TI sem requisitos de segurança adotados</li> <li>Tempo para conceder, alterar e remover privilégios de acesso em comparação com os níveis de serviço definidos</li> <li>Frequência da avaliação de segurança em comparação com os últimos padrões e diretrizes</li> </ul>
	11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência das avaliações de otimização de custo e maturidade da capacidade</li> <li>Tendência dos resultados da avaliação</li> <li>Níveis de satisfação dos executivos de TI e da empresa com os custos e a capacidade de TI</li> </ul>
	12 Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia	<ul style="list-style-type: none"> <li>Número de incidentes com o processamento do negócio causados por erro de integração da tecnologia</li> <li>Número de mudanças no processo de negócio que tiveram de ser adiadas ou retrabalhadas por causa de problemas com a integração da tecnologia</li> <li>Número de programas corporativos capacitados por TI atrasados ou que incorreram custo adicional devido a problemas com a integração da tecnologia</li> <li>Número de aplicativos ou infraestruturas críticas operando em silos e sem integração</li> </ul>
	13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	<ul style="list-style-type: none"> <li>Número de programas / projetos dentro do prazo e do orçamento</li> <li>Percentual de participantes satisfeitos com a qualidade do programa / projeto</li> <li>Número de programas que necessitam de retrabalho significativo devido à má qualidade</li> <li>Custo de manutenção do aplicativo em comparação com o custo geral de TI</li> </ul>
	14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	<ul style="list-style-type: none"> <li>Nível de satisfação do usuário corporativo com a qualidade e pontualidade (ou disponibilidade) das informações gerenciais</li> <li>Número de incidentes com os processos de negócio causados pela indisponibilidade da informação</li> <li>Relação e extensão das decisões de negócios erradas em que a informação errada ou indisponível foi um fator importante</li> </ul>
	15 Conformidade de TI com as políticas internas	<ul style="list-style-type: none"> <li>Número de incidentes relacionados a não conformidade com a política</li> <li>Percentual de participantes que entendem as políticas</li> <li>Percentual de políticas apoiadas por padrões e práticas de trabalho efetivos</li> <li>Frequência da revisão e atualização das políticas</li> </ul>
Aprendizado e	16 Equipes de TI e de negócios	<ul style="list-style-type: none"> <li>Percentual de funcionários cujas habilidades de TI são suficientes para a</li> </ul>

## CAPÍTULO 2: CASCATA DE OBJETIVOS E MÉTRICAS PARA OS OBJETIVOS CORPORATIVOS E OBJETIVOS DE TI

**Figura 7 – Exemplos de Métricas para Objetivos relacionadas a TI**

Dimensão BSC	Objetivos de TI	Métrica
Crescimento	motivadas e qualificadas	competência requerida para seu cargo <ul style="list-style-type: none"> <li>• Percentual de funcionários satisfeitos com os seus cargos em TI</li> <li>• Número de horas de treinamento / capacitação por membro da equipe</li> </ul>
	17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>• Nível de conscientização e entendimento dos executivos da empresa das possibilidades de inovação de TI</li> <li>• Nível de satisfação do participante com os níveis de inovação, expertise e ideias de TI</li> <li>• Número de iniciativas aprovadas resultante de ideias inovadoras de TI</li> </ul>

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

---

Página intencionalmente deixada em branco

## CAPÍTULO 4

# MODELO DE REFERÊNCIA DE PROCESSOS DO COBIT 5

### CAPÍTULO 3

## O MODELO DE PROCESSOS DO COBIT 5

Processos são uma das sete categorias de habilitadores da governança e gestão de TI da empresa, já explicadas no COBIT 5, capítulo 05. As especificidades do habilitador de processos são comparadas com a descrição do habilitador genérico e apresentadas na figura 8.



Um processo é definido como “um conjunto de práticas influenciadas pelas políticas e procedimentos da empresa alimentado por diversas fontes (inclusive outros processos), que manipula as entradas e produz resultados (ex: produtos, serviços)”.

O modelo de processos destaca:

- **Partes Interessadas** — Processos têm partes interessadas internas e externas, com suas próprias funções; as partes interessadas e seus níveis de responsabilidade são documentados nas Tabelas RACI. Partes interessadas externas incluem clientes, parceiros comerciais, acionistas e reguladores. Partes interessadas internas incluem o conselho, administração, funcionários e voluntários.
- **Metas** — As metas do processo são definidas como “uma declaração que descreve o resultado esperado de um processo. Um resultado pode ser um artefato, uma mudança significativa de um estado ou uma melhoria significativa na capacidade de outros processos”. Elas fazem parte da cascata de objetivos, ou seja, as metas do processo apoiam os objetivos de TI, que por sua vez apoiam os objetivos corporativos.

As metas do processo podem ser categorizadas como:

- **Metas intrínsecas** — O processo tem qualidade intrínseca? Ele é exato e está em consonância com as boas práticas? Ele cumpre as normas internas e externas?
- **Metas contextuais** — O processo foi personalizado e adaptado à situação específica da empresa? O processo é significativo, compreensível e fácil de ser aplicado?
- **Metas de acessibilidade e segurança** — O processo mantém a confidencialidade, quando necessário, é conhecido e está acessível para quem precisa deles?

Em cada nível da cascata de objetivos, e consequentemente também para os processos, métricas são definidas para aferir em que medida os objetivos são atingidos. Métricas podem ser definidas como “uma entidade quantificável que permite medir a consecução da meta de um processo. As métricas devem ser SMART (specific, measurable, actionable, relevant and timely) — específicas, mensuráveis, açãoáveis, pertinentes e tempestivas”.

Para administrar o habilitador de forma eficaz e eficiente, as métricas devem ser definidas para medir em qual medida os resultados esperados foram atingidos. Além disso, um segundo aspecto do controle de desempenho do

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

---

habilitador descreve em qual medida as boas práticas foram aplicadas. Aqui também, métricas associadas podem ser definidas para auxiliar o controle do habilitador.

- **Ciclo de vida** — Cada processo tem um ciclo de vida. Ele é definido, criado, operado, monitorado, e ajustado/atualizado ou encerrado. Práticas de processos genéricas tais como as definidas no modelo de avaliação de processo do COBIT com base no ISO/IEC 15504 podem auxiliar na definição, execução, monitoramento e otimização dos processos.
- **Boas práticas** — COBIT 5 Enabling Processes contém um modelo de referência de processo, que descreve as boas práticas internas do processo com níveis de detalhamento cada vez maiores: Práticas, atividades e atividades detalhadas:<sup>4</sup>

Práticas:

- Para cada processo do COBIT 5, as práticas de governança/gestão fornecem um conjunto completo de requisitos em alto nível para a prática e eficaz governança e gestão de TI da empresa. Elas são:
  - Declarações de ações para realização de benefícios, otimizar o nível de risco e o uso dos recursos
  - Alinhadas aos padrões e boas práticas pertinentes geralmente aceitos
  - Genéricas e, portanto, devem ser adaptadas para cada empresa
  - Coberturas para os especialistas em TI e em negócios do processo (de ponta a ponta)
- O órgão de governança da empresa e a administração devem fazer escolhas relacionadas a estas práticas de governança e gestão:
  - Selecionando as que são aplicáveis e decidindo quais serão implementadas
  - Adicionando e/ou adaptando as práticas conforme necessário
  - Definindo e adicionando práticas não relacionadas a TI para integração nos processos de negócios
  - Escolhendo como implementá-las (frequência, amplitude, automação, etc.)
  - Aceitando o risco da não implementar aquelas que possam ser aplicáveis

**Atividades** - No COBIT, as principais ações a serem tomadas na operação do processo

- São definidas como “orientação para alcançar as práticas de gestão para obter sucesso na governança e gestão de TI da empresa”. As atividades do COBIT 5 disponibilizam informações sobre como, por que e o que implementar em cada prática de governança e gestão para melhorar o desempenho de TI e/ou abordar o risco da solução de TI e da prestação de serviço. Este material é útil para:
  - A administração, prestadores de serviços, usuários finais e profissional de TI que precisam planejar, desenvolver, executar ou monitorar a TI da empresa
  - Profissionais de garantia que possam ser questionados sobre suas opiniões em relação às implementações atuais ou propostas ou as melhorias necessárias
- Um conjunto completo de atividades genéricas e específicas que fornecem uma abordagem que inclui todas as etapas necessárias e suficientes para alcançar a principal prática de governança-PG (GP – Governance Practice) / prática de gestão-PG (MP – Management Practice). Elas fornecem orientação em alto nível, a um nível abaixo do GP/MP para avaliar o desempenho efetivo e considerar potenciais melhorias. As atividades:
  - Descrevem um conjunto de etapas de implementação orientadas à ação necessárias e suficientes para atingir um GP/MP
  - Consideram as entradas e saídas do processo
  - Tem como base os padrões e boas práticas geralmente aceitos
  - Apoiam o estabelecimento de funções e responsabilidades bem definidas
  - Não são prescritivas e devem ser adaptadas e desenvolvidas em procedimentos específicos adequados à empresa
- **Atividades detalhadas** — As atividades podem não ter um nível suficiente de detalhamento para a implementação e orientação adicional talvez tenha de ser:
  - Obtida a partir de padrões e boas práticas pertinentes específicos tais como ITIL, ISO/IEC série 27000 e PRINCE2
  - Desenvolvida como atividades específicas ou mais bem detalhadas como desenvolvimentos adicionais na família de produtos do próprio COBIT 5
- **Entradas e saídas** — As entradas e saídas do COBIT 5 são os produtos do trabalho/artefatos do processo

---

<sup>4</sup> Somente práticas e atividades são desenvolvidas de acordo com o projeto atual. Os níveis mais detalhados estão sujeitos a desenvolvimento(s) adicional (ais), por exemplo, os diversos guias profissionais podem fornecer orientação mais detalhada para suas áreas. Além disso, orientação adicional pode ser obtida através dos padrões e estruturas relacionados, conforme indicado nas descrições detalhadas do processo.

## CAPÍTULO 4

### MODELO DE REFERÊNCIA DE PROCESSOS DO COBIT 5

---

considerados necessários para apoiar a operação do processo. Elas possibilitam decisões importantes, fornecem um registro e uma prova de auditoria das atividades do processo e permitem o acompanhamento em caso de incidente. Elas são definidas em um importante nível da prática de governança/gestão, podem incluir alguns produtos do trabalho usados somente dentro do processo e frequentemente são entradas essenciais para outros processos.<sup>5</sup>

*Boas práticas externas podem existir em qualquer forma ou nível de detalhamento e a maioria se refere a outros padrões e estruturas. Os usuários podem consultar essas boas práticas externas em todas as ocasiões, visto que o COBIT está alinhado com estes padrões, quando pertinente, e as informações de mapeamento serão disponibilizadas.*

#### GERENCIAMENTO DE DESEMPENHO DO HABILITADOR

Empresas esperam resultados positivos da aplicação e uso dos habilitadores. Para controlar o desempenho dos habilitadores, as perguntas abaixo terão de ser monitoradas e posteriormente respondidas — com base em métricas — periodicamente:

- As necessidades das partes interessadas foram consideradas?
- As metas do habilitador foram atingidas?
- O ciclo de vida do habilitador é controlado?
- Boas práticas foram aplicadas?

No caso do habilitador de processo, os primeiros dois marcadores tratam do resultado efetivo do processo. As métricas usadas para mensurar em qual medida as metas foram atingidas podem ser chamadas de “indicadores de resultado”. No COBIT 5: Enabling Processes diversas métricas são definidas para cada Objetivo do Processo. Os dois últimos marcadores tratam do funcionamento real do próprio habilitador e as métricas para essa finalidade podem ser chamadas de “indicadores de progresso” (também, conhecido como performance ou execução).

**Nível de capacidade do processo** — O COBIT 5 possui um esquema de avaliação da capacidade do processo com base no ISO/IEC 155004 Isto é discutido no capítulo 8 do COBIT 5 e mais orientações estão disponíveis em publicações separadas do ISACA COBIT 05 Em suma, o nível de capacidade do processo mede a consecução das metas e a aplicação das boas práticas.

**Relações com outros habilitadores** — As interações entre os processos e as demais categorias de habilitadores existem através das seguintes relações:

- Processos necessitam de informações (como um dos tipos de entrada) e podem produzir informações (como um produto do trabalho).
- Processos necessitam de estruturas organizacionais e funções para funcionar, conforme demonstrado nas tabelas RACI, por exemplo, comitê de orientação de TI, comitê de risco corporativo, conselho, auditoria, diretor de TI (CIO), diretor executivo (CEO).
- Processos produzem, e também requerem, capacidades de serviço (infraestrutura, aplicativos, etc.)
- Processos podem e irão depender de outros processos.
- Processos produzem ou necessitam de políticas e procedimentos para garantir a consistência da implementação e execução.
- Aspectos culturais e comportamentais determinam a qualidade da execução dos processos.

---

<sup>5</sup> As entradas e saídas que ilustram o COBIT 5 não serão consideradas uma lista completa porque fluxos de informações adicionais podem ser definidos, dependendo do ambiente e da estrutura do processo de uma empresa específica.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

---

Página intencionalmente deixada em branco

## CAPÍTULO 4

# MODELO DE REFERÊNCIA DE PROCESSOS DO COBIT 5

## CAPÍTULO 4

### MODELO DE REFERÊNCIA DE PROCESSOS DO COBIT 5

#### PROCESSOS DE GOVERNANÇA E GESTÃO

Um dos princípios que norteiam o COBIT é a distinção feita entre governança e gestão. Em consonância com este princípio, seria esperado que todas as empresas implementassem diversos processos de governança e diversos processos de gestão que forneceriam total governança e gestão de TI da empresa.

Ao considerar os processos de governança e gestão no contexto da empresa, a diferença entre os tipos de processos reside nos objetivos dos processos:

- **Processos de governança** — Os processos de governança tratam dos objetivos de governança do participante, criação de valor, otimização dos riscos e dos recursos — e incluem práticas e atividades voltadas à avaliação das opções estratégicas, fornecendo orientação para TI e monitorando o resultado (EDM Avaliar, Dirigir e Monitirar — em consonância com os conceitos do padrão ISO/IEC 38500).
- **Processos de gestão** — Em consonância com as definições de gestão, práticas e atividades dos processos de gestão cobrem as áreas de responsabilidade de PBRM (plan, build, run and monitor) de TI da empresa e devem fornecer cobertura de TI de ponta a ponta.

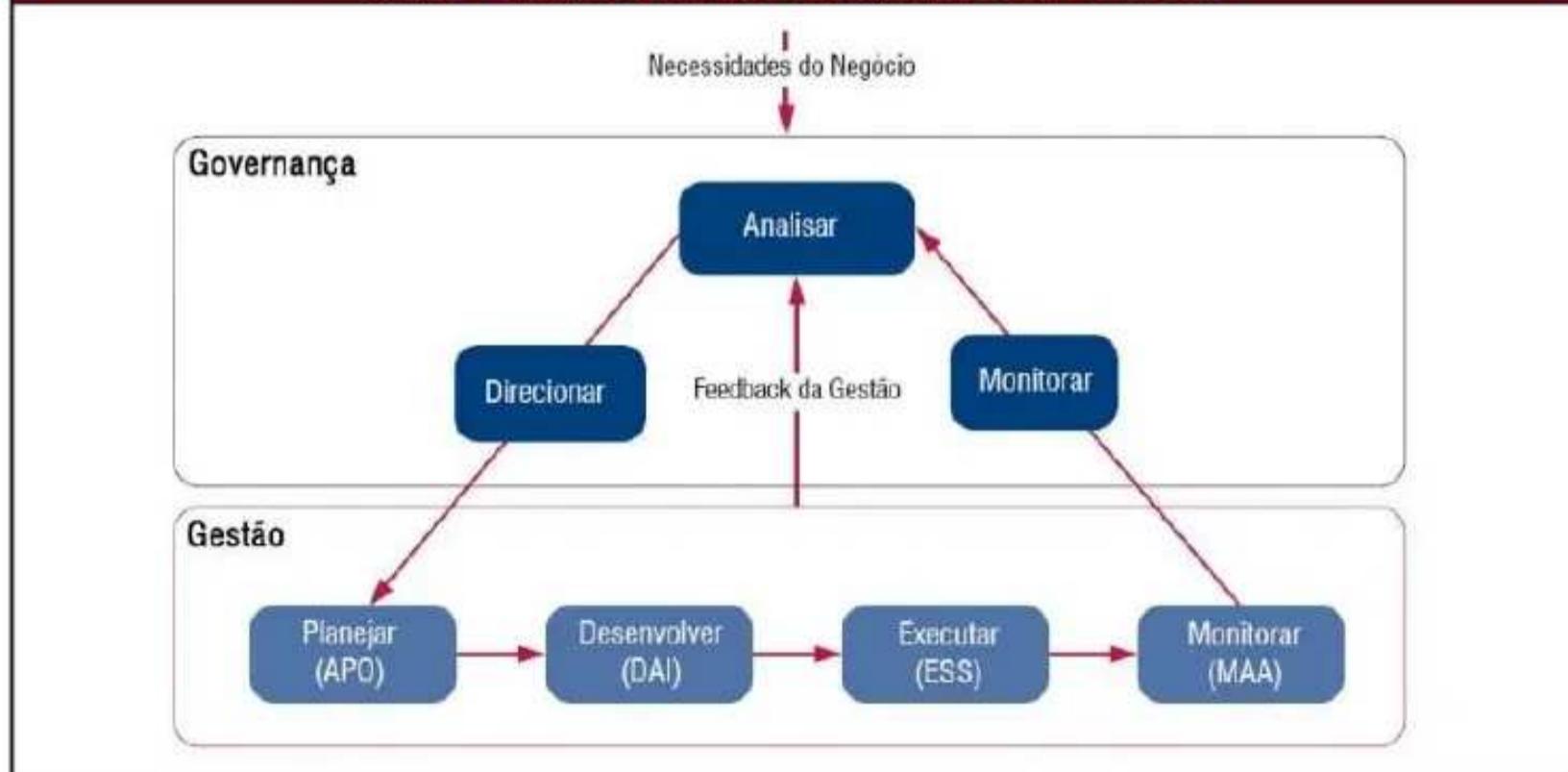
Embora o resultado dos tipos de processos seja diferente e destinado a um público diferente, internamente, do contexto do processo em si, todos os processos requerem atividades de “planejamento”, “construção”, “execução” e “monitoramento” (PBRM) das atividades do processo.

#### MODELO

O COBIT 5 não é prescritivo, mas a partir do texto acima fica claro que ele defende que as empresas implementem processos de governança e gestão de tal forma que as principais áreas sejam cobertas, conforme demonstrado na **figura 9**.

Na teoria, uma empresa pode organizar seus processos conforme julgar adequado, contanto que todos os objetivos de governança e gestão necessários sejam cobertos. Empresas de menor porte podem ter menos processos; empresas de maior porte e mais complexas poderão ter muitos processos, todos para cobrir os mesmos objetivos.

**Figura 9 – Principais Áreas para Governança e Gestão do COBIT 5**



O COBIT 5 inclui um modelo de referência de processo, que define e descreve em detalhes diversos processos de governança e gestão. Isso fornece um modelo de referência de processo que representa todos os processos

# COBIT® : HABILITANDO PROCESSOS

normalmente encontrados nas atividades de TI de uma empresa, oferecendo um modelo de referência comum compreensível aos administradores operacionais de TI e administradores de negócios. O modelo de processo proposto é um modelo completo e abrangente, mas não é o único modelo de processo possível. Cada empresa deve definir seu próprio conjunto de processos, considerando sua situação específica.

Incorporar um modelo operacional e uma linguagem comum para todas as partes da empresa envolvidas nas atividades de TI é uma das etapas mais importantes e críticas da boa governança. Isso também fornece uma estrutura para medição e monitoramento do desempenho de TI, comunicação com os prestadores de serviços e integração das melhores práticas de gestão.

O modelo de referência de processo do COBIT 5 subdivide os processos de governança e gestão de TI da empresa em duas áreas de atividades principais — governança e gestão — divididas em dois domínios de processos:

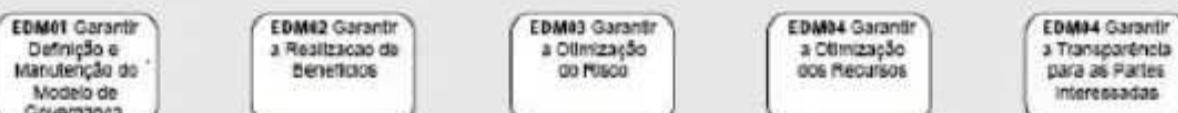
- **Governança** — Este domínio contém cinco processos de governança; e práticas de EDM (Avaliar, Dirigir e Monitirar) são definidas dentro de cada processo.
- **Gestão** — Estes quatro domínios estão em consonância com as áreas de responsabilidade de PBRM (uma evolução dos domínios do COBIT 4.1) e proporcionam uma cobertura de TI de ponta a ponta. Cada domínio contém diversos processos, como no COBIT 4.1 e versões anteriores. Embora, conforme já mencionado, a maioria dos processos requeira atividades para “planejar”, “implementar”, “executar” e “monitorar” o processo ou o problema específico a ser abordado (por exemplo, qualidade, segurança), eles são alocados em domínios de acordo com a área de atividade mais relevante em relação a TI da empresa.

O modelo de referência de processo do COBIT 5 é o sucessor do modelo de processo do COBIT 4.1, e conta ainda com a integração dos modelos de processo Risk IT e Val IT. A **figura 10** mostra o conjunto completo de 37 processos de governança e de gestão do COBIT 5.

**Figura 10 – Modelo de Referência de Processos do COBIT 5**

## Processos para Governança Corporativa de TI

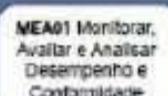
### Avaliar, Orientar e Monitorar



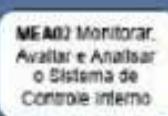
### Alinhar, Planejar e Organizar



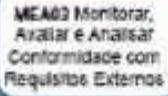
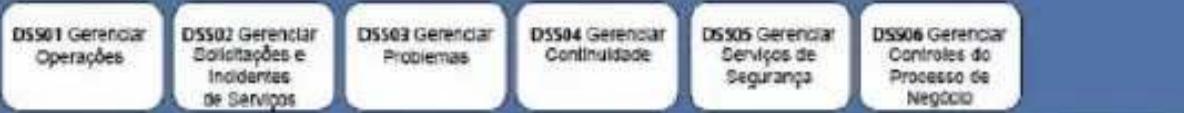
### Monitorar, Avaliar e Analisar



### Desenvolver, Adquirir e Implementar



### Executar, Atender e Apoiar



## Processos para Gestão Corporativa de TI

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Este capítulo descreve o conteúdo detalhado relacionado aos processos de governança e gestão do COBIT 05. As seguintes informações serão incluídas para cada processo, em consonância com o modelo de processo explicado no capítulo anterior:

- **Identificação do processo** — Na primeira página:
  - Rótulo do processo — O prefixo do domínio (EDM, APO, BAI, DSS, MEA) e o número do processo
  - Nome do processo — Uma curta descrição, indicando o assunto principal do processo
  - Área do processo — Governança ou gestão
  - Nome do domínio
- **Descrição do processo** — Uma visão geral daquilo que o processo faz e uma visão geral em alto nível de como o processo alcança seu objetivo
- **Declaração de objetivo do processo** — Uma descrição do objetivo geral do processo
- **Informações sobre a cascata de objetivos** — Referência e descrição dos principais objetivos de TI apoiados pelo processo,<sup>6</sup> e métricas para medir a consecução dos objetivos de TI
- **Objetivos e Métricas do Processo** — Um conjunto de metas de processo e um número limitado de métricas de exemplo
- **Tabela RACI** — Uma sugestão de atribuição do nível de responsabilidade das práticas de processo para diferentes funções e estruturas. As funções corporativas listadas possuem um sombreado mais escuro do que o das funções de TI. Os diferentes níveis de envolvimento são:
  - R(esponsável) - **Quem está realizando a tarefa?** As funções que tiverem o principal interesse operacional na realização da atividade relacionada e criarem o resultado esperado
  - (prest)A (contas) - **Quem responde pelo sucesso da tarefa?** Isso atribui a responsabilidade global para realizar a tarefa (Em quem termina a atividade operacional?). Levar em conta que o papel mencionado é o menor nível adequado de prestação de contas; e há naturalmente, níveis mais elevados de responsabilidade que são responsáveis também. Para habilitar o modelo de aprovações da organização a responsabilidade é discriminada na medida do possível. A prestação de contas não indica que o papel não tem atividades operacionais; é muito provável que o papel fique envolvido na tarefa. Como princípio básico, a prestação de contas não pode ser compartilhada.
  - C(onsultado)- **Quem é responsável pelas entradas?** As principais funções que fornecem entrada. Observe que também fica a critério das funções responsáveis obterem as informações junto a outras unidades ou parceiros externos; no entanto, as entradas provenientes das funções relacionadas serão consideradas e, se necessário, ações adequadas deverão ser tomadas para escalação, inclusive a informação do responsável pelo processo e/ou do comitê diretor.
  - I(nformado) - **Quem recebe a informação?** As funções informadas sobre a consecução e/ou resultados da tarefa. A função de “responsável”, evidentemente, sempre deverá receber informação adequada para supervisionar a tarefa, da mesma forma que as funções responsáveis por sua área de interesse
- Descrição detalhada das práticas do processo — Para cada prática:
  - Título e descrição da prática
  - Entradas e saídas da prática, com indicação de origem e destino
  - Atividades do processo, maior detalhamento das práticas
- Orientação relacionada — Referências a outros padrões e indicação para orientação adicional

## ENTRADAS E SAÍDAS

As descrições detalhadas de processo contêm — no nível das práticas de governança e gestão — entradas e saídas. De modo geral, cada saída é enviada para um ou um número limitado de destino, geralmente outra prática de processo do COBIT. Essa saída então se torna uma entrada para o seu destino. No entanto, há diversas saídas que possuem muitos destinos, por exemplo, todos os processos do COBIT ou todos os processos dentro de um domínio. Por motivos de legibilidade, essas saídas NÃO são listadas como entradas nesses processos. Uma lista completa dessas saídas foi incluída na **figura 11**.

<sup>6</sup> Apenas as Metas de TI relacionadas com um 'P' na tabela de mapeamento entre os objetivos e processos relacionados a TI (figura 17) estão listados aqui.



Para algumas/saidas, o destino “interno” é mencionado. Isto significa que a entrada/saída ocorre entre atividades dentro do mesmo processo.

**Figura 11 – Saídas**

<b>Saídas para todos os Processos</b>		
<b>Da Prática</b>	<b>Descrição da Saída</b>	<b>Destino</b>
APO13.02	Plano de tratamento de risco de Segurança da informação	TodosEDM; TodosAPO; TodosBAI; TodosDSS; All MEA
<b>Saídas para todos os Processos de Governança</b>		
<b>Da Prática</b>	<b>Descrição da Saída</b>	<b>Destino</b>
EDM01.01	Princípios guia de governança corporativa	Todos EDM
EDM01.01	Modelo de tomada de decisão	Todos EDM
EDM01.01	Níveis de Autoridade	Todos EDM
EDM01.02	Comunicação da Governança Corporativa	Todos EDM
EDM01.03	Feedback da efetividade de governança e desempenho	Todos EDM
<b>Saídas para todos os Processos de Gestão</b>		
<b>Da Prática</b>	<b>Descrição da Saída</b>	<b>Destino</b>
APO01.01	Regras básicas de comunicação	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO01.03	Políticas relacionadas a TI	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO01.04	Comunicação dos Objetivos de TI	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO01.07	Oportunidades de melhoria dos processos	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO02.06	Pacote de Comunicação	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO11.02	Padrões de Gestão da Qualidade	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO11.04	Objetivos e métricas de processo de qualidade de serviço	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO11.06	Comunicação de melhoria contínua e boas práticas	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO11.06	Exemplos de boas práticas a serem compartilhados	TodosAPO; TodosBAI; TodosDSS; TodosMEA
APO11.06	Resultados do Benchmark de Revisão da Qualidade	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA01.02	Objetivos de Monitoração	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA01.04	Relatórios de Desempenho	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA01.05	Planos de Remediação e atribuições	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.01	Resultados da monitoração e revisões de controlos internos	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.01	Resultados de benchmarking e outras avaliações	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.03	Planejamento e critério de Self-assessments	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.03	Resultados das revisões self-assessments	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.04	Deficiências de Controle	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.04	Ações de Remediação	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.06	Plano de Garantia (Assurance)	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.08	Refinamento de Escopo	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.08	Resultados da Revisão de Garantia (Assurance)	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA02.08	Relatório de Revisão de Garantia (Assurance)	TodosAPO; TodosBAI; TodosDSS; TodosMEA
MEA03.02	Comunicação da mudança dos requisitos de compliance	TodosAPO; TodosBAI; TodosDSS; TodosMEA

## INSTRUÇÕES GENÉRICAS PARA PROCESSOS

As atividades nas descrições detalhadas de processo descrevem o propósito funcional do processo – o qual o processo presume entregar. Estes serão diferentes para cada processo, porque cada processo tem objetivos de

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

processos distintos

Existem também instruções de como o processo será executado, exemplo: Instruções genéricas de como construir, executar, monitorar e melhorar o processo referido. Essas instruções são genéricas e semelhantes para cada processo.

No COBIT 4.1, os controles de processo continham boas práticas que não eram específicas para qualquer processo, mas eram genéricas e aplicáveis a todos os processos. Esses controles de processos eram similares a alguns dos atributos genéricos do modelo de maturidade do COBIT 4.1.

No COBIT 5, é utilizado um esquema de avaliação de capacidade de processos em conformidade com a ISO/IEC 155004 Nesse esquema os atributos de capacidade pertencentes a um maior nível de capacidade descrevem maior e melhor proficiência na construção do processo, dessa maneira substituindo eficientemente os controles de processo do COBIT 4.1.

Essa é uma instrução importante relacionada aos processos, e por essa razão que a **figura 12** contém uma análise de alto nível dos controles de processo do COBIT 4.1 e seu equivalente aos atributos de capacidade baseados na ISO/IEC 15504 que são embasamento para satisfazer os processos.

**Figura 12 – Processos de Controle do COBIT 4.1 e Atributos de Capacidade de Processo ISO/IEC 15504**

COBIT 4.1		Atributos de Capacidade de Processo ISO/IEC 15504	
PC1	Metas e Objetivos do Processo	PA 2.1	Atributo de gestão de desempenho
PC2	Propriedade do Processo	PA 2.1	Atributo de gestão de desempenho
PC3	Repetitividade do processo	PA 3.1	Atributo de definição de processo
PC4	Papéis e Responsabilidades	PA 2.1 PA 3.2	Atributo de gestão de desempenho Atributo de implementação de processo
PC5	Política, Planos e Procedimentos	PA 2.1	Atributo de gestão de desempenho
PC6	Processo de Melhoria de Desempenho	PA 2.1 PA 5.2	Atributo de gestão de desempenho Atributo de otimização de processo

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

---

Página intencionalmente deixada em branco

## AVALIAR, DIRIGIR E MONITORAR (EDM)

- 01 Garantir a Definição e Manutenção do Modelo de Governança**
- 02 Garantir a Realização de Benefícios**
- 03 Garantir a Otimização do Risco**
- 04 Garantir a Otimização de Recursos**
- 05 Garantir a Transparéncia às Partes Interessadas**

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

<b>EDM01 - Garantir a Definição e Manutenção do Modelo de Governança</b>	<b>Área: Governança</b> <b>Domínio: Avaliar, Dirigir e Monitorar</b>
<b>Descrição do Processo</b>	
Analisar e articular os requerimentos da governança corporativa de TI, colocando em prática e mantendo efetiva as estruturas de habilitadores, princípios, processos e práticas, com clareza de responsabilidades e autoridade para alcançar a missão, metas e objetivos da organização.	
<b>Descrição do Objetivo de Processo</b>	
Implementar uma abordagem consistente, integrada e alinhada com a abordagem de governança corporativa. Para garantir que as decisões de TI são tomadas em linha com as estratégias e objetivos corporativos, garantir que os processos de TI são acompanhados de forma eficiente e transparente, conformidade verificada aos requisitos legais e regulatórios, alcance dos requisitos de governança aos membros do Conselho de Administração.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de metas estratégicas e requisitos corporativos, suportados pelas metas estratégicas de TI.</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio dos programas e serviços.</li> <li>Percentual dos direcionadores de valor de TI mapeados a direcionadores de valor ao negócio.</li> </ul>
03 Compromisso da gerência executiva com a tomada de decisões de TI	<ul style="list-style-type: none"> <li>Percentual de papéis da gestão executiva com prestação de contas definidas em relação às decisões de TI.</li> <li>Número de vezes que TI está na agenda do Conselho de Administração de maneira proativa.</li> <li>Frequência das reuniões de comitê estratégico (executivo) de TI.</li> <li>Frequência de decisões executivas relacionadas a TI</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de interrupções de negócio relacionadas a incidentes em serviços de TI</li> <li>Percentual de partes interessadas no negócio satisfeitas em relação ao alinhamento dos níveis de serviço à entrega dos serviços de TI</li> <li>Percentual dos usuários satisfeitos com a qualidade dos serviços de TI</li> </ul>
Objetivos e Métricas do Processo	
Objetivo do Processo	Métricas Relacionadas
01 O modelo de tomada de decisão estratégica para TI é eficiente e alinhado com os requisitos internos e externos e das partes interessadas.	<ul style="list-style-type: none"> <li>Ciclo de tempo real vs. pretendido para decisões mais importantes.</li> <li>Nível de satisfação das partes interessadas (medida através de pesquisas).</li> </ul>
02 O Sistema de governança de TI está integrado à Organização	<ul style="list-style-type: none"> <li>Número de papéis, responsabilidades e autoridades que são definidas, atribuídas e aceitas pelas respectivas gestões de negócio e TI.</li> <li>Quantidade de princípios de governança de TI acordados que são evidenciados nos processos e práticas (porcentagem de processos e práticas com rastreabilidade clara aos princípios)</li> <li>Número de ocorrências de falta de conformidade aos padrões éticos e comportamento profissional.</li> </ul>
03 Garantia (Assurance) é obtida pela premissa de que o sistema de governança de TI está operando de maneira eficiente.	<ul style="list-style-type: none"> <li>Frequência de revisões independentes de governança de TI</li> <li>Frequência de governança de TI reportando ao comitê executivo e conselho de administração.</li> <li>Número de problemas de governança de TI reportados.</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

EDM01 Tabela RACI

Prática de Governança	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Conforme RH	Auditores	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>EDM01.01</b> Avaliar o sistema de governança	A	R	C	C	R	R					C	C	C	C	C	R	C	C	C	C	C				
<b>EDM01.02</b> Dirigir o sistema de governança	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	
<b>EDM01.03</b> Monitorar o sistema de governança	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

EDM01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM01.01 Avaliar o sistema de governança.</b> Continuamente identificar e envolver as partes interessadas da organização, documentar o entendimento dos requisitos, e fazer um julgamento sobre o desenho atual e futuro da governança corporativa de TI.	MEA03.02	<ul style="list-style-type: none"> <li>• Comunicação das mudanças aos requisitos de conformidade.</li> </ul>	<ul style="list-style-type: none"> <li>• Princípios de orientação para Governança Corporativa</li> </ul>	Todos EDM APO01.01 APO01.03
	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>• Tendências do ambiente de negócio</li> <li>• Normas e regulamentação</li> <li>• Guia para modelo de tomada de decisão de Governança</li> <li>• Estatuto interno da organização</li> </ul>	<ul style="list-style-type: none"> <li>• Modelo de tomada de decisão</li> <li>• Níveis de autoridade</li> </ul>	Todos EDM APO01.01  Todos EDM APO01.02
<b>Atividades</b>				
01 Analisar e identificar os fatores internos e externos ambientais (obrigações legais, regulamentares e contratuais) e tendências no ambiente de negócios que podem influenciar o desenho da governança.				
02 Determinar a importância da TI e seu papel no que diz respeito ao negócio.				
03 Considerar regulamentos externos, leis e obrigações contratuais e determinar como eles devem ser aplicados dentro da governança corporativa de TI.				
04 Alinhar o uso ético do processamento de informações e seu impacto na sociedade, o ambiente natural, e os interesses internos e externos das partes interessadas com o direcionamento, metas e objetivos da organização.				
05 Determinar as implicações do ambiente geral de controle da organização no que diz respeito à TI.				
06 Articular os princípios que irão orientar o desenho da governança e a tomada decisão de TI.				
07 Compreender a cultura de tomada de decisões da organização e determinar o melhor modelo de tomada de decisão de TI				
08 Determinar os níveis adequados de delegação da autoridade, incluindo limites pré-estabelecidos para as decisões de TI.				

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

EDM01 Práticas de Processo, Entradas/Saídas e Atividades				
Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM01.02 Dirigir o sistema de governança</b> Informar os líderes e obter o seu apoio, convencimento e compromisso. Orientar as estruturas, processos e práticas para governança de TI em conformidade com os princípios acordados no desenho da governança, modelos de tomada de decisão e níveis de autoridade. Definir as informações necessárias para o reconhecimento da tomada de decisão.			<ul style="list-style-type: none"> <li>Governança de comunicações corporativas.</li> <li>Abordagem de sistema de recompensas</li> </ul>	Todos EDM AP001.04  AP007.03 AP007.04
Atividades				
01 Comunicar os princípios de governança de TI e alinhar com a gerência executiva no intuito de estabelecer o reconhecimento e o empenho da liderança				
02 Estabelecer ou delegar a implementação das estruturas de governança, processos e práticas de acordo com os princípios definidos.				
03 Atribuir responsabilidade, autoridade e prestação de contas alinhado aos princípios definidos de governança, modelos de tomada de decisão e delegação.				
04 Garantir que a comunicação e mecanismos de reporte fornecem responsabilidades pela supervisão e informações adequadas para a tomada de decisão				
05 Assegurar que os funcionários sigam as orientações relevantes para o comportamento ético e profissional, garantindo que as consequências de não conformidade são conhecidas e aplicadas.				
06 Assegurar o estabelecimento de um sistema de recompensa para promover a mudança cultural desejável.				
Prática de Governança	Entradas		Saídas	
<b>EDM01.03 Monitorar o sistema de governança</b> Monitorar a eficácia e o desempenho da governança corporativa de TI. Avaliar se o sistema de governança e mecanismos implementados (incluindo estruturas, princípios e processo) estão funcionando de forma eficaz e permitem a supervisão adequada de TI.	De	Descrição	Descrição	Para
	MEA01.04	<ul style="list-style-type: none"> <li>Relatórios de desempenho</li> </ul>	<ul style="list-style-type: none"> <li>Feedback de efetividade e desempenho da governança</li> </ul>	Todos EDM AP001.07
	MEA01.05	<ul style="list-style-type: none"> <li>Status e resultado das ações</li> </ul>		
	MEA02.01	<ul style="list-style-type: none"> <li>Resultado de benchmarking e outras avaliações</li> <li>Resultados de monitoramento e revisões de controles internos</li> </ul>		
	MEA02.03	<ul style="list-style-type: none"> <li>Resultado de revisões de self-assessments</li> </ul>		
	MEA02.06	<ul style="list-style-type: none"> <li>Planos de Garantia (Assurance)</li> </ul>		
	MEA03.03	<ul style="list-style-type: none"> <li>Confirmações de Conformidade</li> </ul>		
	MEA03.04	<ul style="list-style-type: none"> <li>Relatórios de problemas de não conformidades e causas raízes</li> <li>Relatórios de Garantia (Assurance) de conformidade</li> </ul>		
	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>Prestação de Contas</li> <li>Relatórios de Auditoria</li> </ul>		

**EDM01 Práticas de Processo, Entradas/Saídas e Atividades**

Atividades
01 Avaliar a eficácia e o desempenho da responsabilidade e autoridade delegada às partes interessadas, relacionada à governança corporativa de TI.
02 Avaliar periodicamente se mecanismos validados para governança de TI (estruturas, princípios, processos, etc.) estão estabelecidos e funcionam de forma eficaz.
03 Avaliar a eficácia do modelo de governança e identificar ações para corrigir quaisquer desvios encontrados
04 Manter a supervisão do escopo que satisfaz obrigações (regulamentares, legislação, tribunais, contratuais), políticas internas, normas e orientações profissionais.
05 Fazer a supervisão da eficácia e cumprimento do sistema corporativo de controle.
06 Monitorar de forma regular e rotineira os mecanismos para garantir que o uso da TI está em conformidade com as obrigações relevantes (regulamentares, legislação, tribunais, contratuais), padrões e diretrizes

**EDM01 Orientação Relacionada**

Padrão Relacionado	Referência Detalhada
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	
ISO/IEC 38500	
King III	5.1 . O conselho de administração deve ser responsável pela governança de tecnologia da informação (TI). 5.03 O conselho de administração deve delegar a gestão da responsabilidade para a implementação de um modelo de governança de TI.
Organisation for Economic Co-operation and Development (OECD)	Princípios de Governança Corporativa

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

EDM02 - Garantir a Realização de Benefícios		Área: Governança Domínio: Avaliar, Dirigir e Monitorar
<b>Descrição do Processo</b>		
Optimizar a contribuição de valor agregado ao negócio através dos processos de negócios, serviços de TI e ativos de TI resultantes de investimentos realizados pela TI a custos aceitáveis.		
<b>Descrição do Objetivo de Processo</b>		
Defender o valor ideal das iniciativas, serviços e ativos de TI; entregas de soluções e serviços com custo eficiente; e uma imagem confiável e precisa dos custos e benefícios prováveis, para que as necessidades de negócios sejam suportadas de forma eficaz e eficiente.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
<b>Objetivos de TI</b>		<b>Métricas Relacionadas</b>
01 Alinhamento da estratégia de negócios e de TI		<ul style="list-style-type: none"> <li>Percentual de objetivos e necessidades estratégicas da organização suportados pelas metas estratégicas de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio de programas e serviços planejados.</li> <li>Percentual de direcionadores de valor de TI mapeados para direcionadores de valor de negócio</li> </ul>
05 Benefícios obtidos pelo investimento de TI e portfólio de serviços		<ul style="list-style-type: none"> <li>Percentual dos investimentos aprovados onde a realização do benefício é monitorada através de todo o ciclo de vida econômico.</li> <li>Percentual dos serviços de TI, onde os benefícios esperados são realizados.</li> <li>Percentual dos investimentos aprovados onde os benefícios declarados são atingidos ou ultrapassados</li> </ul>
06 Transparência dos custos, benefícios e riscos de TI.		<ul style="list-style-type: none"> <li>Percentual de casos de investimento de negócio com custos e benefícios relacionados a TI claramente definidos e aprovados conforme o esperado.</li> <li>Percentual de serviços de TI com custos operacionais e benefícios esperados claramente definidos e aprovados.</li> <li>Pesquisa de satisfação das principais partes interessadas sobre o nível de transparência, compreensão e veracidade das informações financeiras de TI</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio		<ul style="list-style-type: none"> <li>Número de interrupções nos negócios devido a incidentes de serviço</li> <li>Percentual das partes interessadas do negócio satisfeitas com o atendimento da entrega de serviços em relação aos níveis de serviços estabelecidos.</li> <li>Percentual dos usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
17 Conhecimento, expertise e iniciativas para inovação dos negócios		<ul style="list-style-type: none"> <li>Nível de percepção dos executivos de negócios e compreensão das possibilidades de inovação em TI</li> <li>Nível de satisfação das partes interessadas, com níveis de especialização em inovação e ideias em TI.</li> <li>Número de iniciativas aprovadas resultantes de ideias inovadoras em TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>		
<b>Objetivo do Processo</b>		<b>Métricas Relacionadas</b>
01 A organização está fixando o valor ideal de seu portfólio ativado de iniciativas, serviços e bens de TI.		<ul style="list-style-type: none"> <li>Nível de satisfação gestão executiva com ele é a entrega de valor agregado e custo.</li> <li>Desvio entre investimento desejado e portfólio de investimento real</li> <li>Nível de satisfação das partes interessadas com a capacidade da organização em obter valor agregado a partir de iniciativas de TI.</li> </ul>
02 A melhor solução de valor agregado é derivada do investimento em TI por meio da eficácia das práticas de gestão de valor na organização.		<ul style="list-style-type: none"> <li>Número de incidentes que ocorrem devido a omissão ou qualquer tentativa de negligenciar os princípios e práticas estabelecidas de gestão de valor agregado.</li> <li>Percentual das iniciativas de TI do portfólio geral onde o valor está sendo gerenciado completamente através do seu completo ciclo de vida.</li> </ul>
03 Investimentos de TI individualizados contribuem para a melhor razão de valor agregado.		<ul style="list-style-type: none"> <li>Pesquisas para medir o nível de satisfação das partes interessadas com o progresso em relação às metas identificadas e entrega de valor agregado</li> <li>Percentual obtido do valor agregado esperado.</li> </ul>

EDM02 Tabela RACI

Prática de Governança	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>EDM02.01</b> Avaliar a otimização do valor agregado	A	R	R	C	R	R			C	C	C	C	C	C	C	C	C	R	C	C	I	I	I	I		
<b>EDM02.02</b> Diracionar a otimização de valor agregado.	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I		
<b>EDM02.03</b> Monitorar a otimização de valor agregado.	A	R	R	C	R	R			R	C	C	C	C	C	C	C	C	R	C	C	C	C	C	C		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

EDM02 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM02.01 Avaliar a otimização do valor agregado</b> Continuamente avaliar o portfólio de investimentos, serviços e ativos de TI para determinar a probabilidade de atingir os objetivos corporativos, entregando valor a um custo razoável. Identificar e fazer julgamento sobre quaisquer mudanças de direção que precisam ser fornecidas à gestão para otimizar a criação de valor agregado.	APO02.05	• Direção estratégica	• Avaliação do Alinhamento Estratégico	APO02.04 APO05.03
	APO05.02	• Expectativas de retorno de investimento	• Avaliação dos portfólios de investimentos e serviços	APO05.03 APO05.04 APO06.02
	APO05.03	• Programas selecionados com marcos de Retorno de Investimento (ROI)		
	APO05.06	• Resultado dos benefícios e comunicação relacionada		
	BAI01.06	• Resultado revisado por fases		
Atividades				
01 Entender requisitos das partes interessadas, questões estratégicas de TI, tais como a dependência de TI; e conhecimentos de tecnologia e capacidades sobre o significado real e potencial da TI para a estratégia corporativa.				
02 Compreender os elementos mais importantes da governança necessária para a entrega confiável, segura e rentável de valor ideal a partir da utilização serviços, bens e recursos de TI, existentes e novos.				
. Compreender e regularmente discutir as oportunidades que podem surgir com a mudança corporativa habilitada por tecnologias atuais, novas ou emergentes, e otimizar o valor agregado criado a partir dessas oportunidades.				
04 Entender o que constitui o valor agregado para a organização, e considerar o quanto ele é comunicado, entendido e aplicado de forma adequada em todos os processos da organização.				
05 Avaliar o grau de eficácia da organização e estratégias de TI, integrada e alinhada dentro da organização e com os objetivos corporativos para entrega de valor agregado.				
06 Compreender e considerar a eficácia de papéis, responsabilidades, prestação de contas e unidades de tomada de decisão em assegurar a criação de valor a partir de investimentos, serviços e bens de TI.				

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

**EDM02 Práticas de Processo, Entradas/Saídas e Atividades**

07 Considerar a robustez da gestão dos investimentos, serviços e ativos de TI no alinhamento com a gestão de valor agregado da organização e práticas de gestão financeira.

08 Avaliar o portfólio de investimentos, serviços e ativos para o alinhamento com os objetivos estratégicos da organização; rentabilidade corporativa, financeira e não financeira; riscos, tanto o risco nas entregas e riscos dos benefícios; alinhamento dos processos de negócios; eficácia em termos de aplicabilidade, disponibilidade e capacidade de resposta; e eficiência em termos de custo, redundância e sustentabilidade técnica.

Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM02.02 Direcionar a otimização de valor agregado.</b> Direcionar princípios e práticas de gestão de valor agregado para viabilizar a realização do valor ideal dos investimentos de TI em todo o seu ciclo de vida económico.			<ul style="list-style-type: none"> <li>• Tipos e critérios de investimento</li> </ul>	APO05.01 APO05.03
			<ul style="list-style-type: none"> <li>• Requisitos de revisão por fase</li> </ul>	BAI01.01

**Atividades**

01 Definir e comunicar tipos de portfólio e de investimento, categorias, critérios e ponderações relativas aos critérios para permitir a pontuação geral de valor agregado.

02 Definir os requisitos para a fase de revisão e outros comentários para justificar a importância do investimento para a organização e os riscos associados, à programação, planos de financiamento e da entrega de recursos e benefícios mais importantes e contribuição permanente ao valor agregado.

03 Direcionar a gestão para considerar potencial de usos inovadores em TI que permitam a organização responder a novas oportunidades ou desafios, realizar novos negócios, aumentar a competitividade, ou melhorar os processos.

04 Direcionar quaisquer alterações necessárias na atribuição da prestação de contas, responsabilidades para a execução do portfólio de investimentos e entrega de valor agregado a partir dos processos de negócio e serviços.

05 Definir e comunicar em nível corporativo os objetivos de entrega de valor e medidas para atingir os resultados para permitir uma monitoração eficaz.

06 Direcionar as alterações necessárias para o portfólio de investimentos e serviços para realinhamento dos objetivos e/ou restrições atuais e esperados da organização.

07 Recomendar a consideração de potenciais inovações, mudanças organizacionais ou melhorias operacionais que poderiam impulsionar o crescimento do valor para a organização a partir de iniciativas de TI.

Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM02.03 Monitorar a otimização de valor agregado.</b> Monitorar os principais objetivos e métricas para determinar a extensão em que o negócio está gerando o valor agregado esperado e os benefícios para a organização a partir dos investimentos e serviços de TI. Identificar problemas significativos e considerar ações corretivas.	APO05.04	<ul style="list-style-type: none"> <li>• Relatórios de desempenho do portfólio de investimentos.</li> </ul>	<ul style="list-style-type: none"> <li>• Avaliação e</li> <li>• Desempenho do portfólio e programa de investimentos</li> </ul>	APO05.04 APO06.05 BAI01.06
			<ul style="list-style-type: none"> <li>• Ações corretivas para aprimorar a entrega de valor agregado</li> </ul>	EDM05.01 APO05.04 APO06.02 BAI01.01

**Atividades**

01 Definir um conjunto equilibrado de objetivos de desempenho, métricas, metas e benchmarks. Métricas deverão atender as medidas de atividade e resultados, incluindo indicadores de atingimento antecipado e atraso para os resultados, bem como um equilíbrio adequado de medidas financeiras e não financeiras. Revisão e aprovação com as outras funções de TI e negócios, e outras partes interessadas relevantes.

02 Coletar dados relevantes, oportunos, tempestivos, confiáveis e precisos para relatar o progresso na entrega de valor agregado contra as metas definidas. Obter uma visão sucinta de alto nível, do portfólio, programa e desempenho de TI (capacidades técnicas e operacionais) que suportem a tomada de decisões, e garantir que os resultados esperados estão sendo alcançados.

03 Obter o portfólio de investimentos regulares e relevantes, programa e relatórios de desempenho de TI (tecnológicos e funcionais). Analisar os progressos da organização para objetivos identificados e em qual medida os objetivos planejados foram alcançados, resultados obtidos, metas de desempenhos atendidas e riscos mitigados.

04 Tomar medidas de gestão adequadas após a revisão de relatórios, conforme necessário, para garantir a otimização do valor agregado.

05 Assegurar após a revisão de relatórios, que as ações corretivas iniciadas e controladas possuem gestão adequada.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

EDM02 Orientação Relacionada	
Padrão Relacionado	Referência Detalhada
COSO	
ISO/IEC 38500	
King III	5.2 . TI deve estar alinhada com os objetivos de desempenho e sustentabilidade da organização. 5.4 . O conselho deve monitorar e avaliar os investimentos e gastos relevantes em TI.

# COBIT® 6 : HABILITANDO PROCESSOS

EDM03 Garantir a Otimização do Risco	Área: Governança Domínio: Avaliar, Dirigir e Monitorar
<b>Descrição do Processo</b> Certificar-se de que o apetite e tolerância ao risco da organização são compreendidos, articulados e comunicados, e que o risco ao valor agregado da organização relacionado com o uso da TI é identificado e controlado.	
<b>Descrição do Objetivo de Processo</b> Garantir que o risco da organização relacionado a TI não excede o apetite e tolerância ao risco, os impactos em relação aos riscos da TI são identificados e controlados em relação aos ativos da organização, e o potencial de falhas de conformidade é minimizado.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Percentual dos processos críticos de negócio, serviços, processos de negócios atendidos pela TI na avaliação dos riscos.</li> <li>Número de incidentes significativos relacionados a TI que não foram identificados na avaliação de risco</li> <li>Percentagem de avaliações de risco que incluem riscos relacionados a TI</li> <li>Frequência de atualização ou validação do perfil de risco</li> </ul>
06 Transparência dos custos, benefícios e riscos de TI	<ul style="list-style-type: none"> <li>Percentual dos casos de negócios de investimento com custos e benefícios esperados relacionados a TI claramente definidos e aprovados.</li> <li>Percentual dos serviços de TI com custos operacionais e benefícios esperados claramente definidos e aprovados.</li> <li>Pesquisas de satisfação com as principais partes interessadas a respeito do nível de transparência, compreensão e veracidade das informações financeiras de TI</li> </ul>
10 Segurança da informação, infraestrutura de processamento e aplicativos	<ul style="list-style-type: none"> <li>Número de incidentes de segurança causando prejuízos financeiros, interrupção dos negócios ou exposição pública.</li> <li>Quantidade de serviços de TI com implementação pendente dos requisitos de segurança.</li> <li>Tempo para conceder, alterar e remover privilégios de acesso comparado aos níveis de serviço acordados.</li> <li>Frequência das avaliações de segurança em relação às normas e diretrizes mais recentes</li> </ul>
15 Conformidade de TI com as políticas internas	<ul style="list-style-type: none"> <li>Número de incidentes relacionados a não conformidades às políticas internas.</li> <li>Percentual das partes interessadas que entendem as políticas internas.</li> <li>Percentual das políticas apoiadas por normas e procedimentos de trabalho eficazes.</li> <li>Frequência de revisão e atualização das políticas internas</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Limites de risco são definidos e comunicados e os riscos mais prioritários relacionados a TI são conhecidos.	<ul style="list-style-type: none"> <li>Nível de alinhamento entre o risco de TI e de risco da organização</li> <li>Número de riscos potenciais de TI identificados e gerenciados</li> <li>Estimativa de atualização da avaliação dos fatores de risco</li> </ul>
02 A organização está gerenciando riscos corporativos críticos de TI de forma eficaz e eficiente.	<ul style="list-style-type: none"> <li>Por cento dos projetos da organização que consideram os riscos de TI.</li> <li>Percentual dos planos de ação relacionados aos riscos de TI executados no prazo.</li> <li>Percentual de riscos relevantes que foram eficazmente mitigados.</li> </ul>
03 Risco corporativo relacionado a TI não excede o apetite ao risco sendo identificado e controlado o impacto do risco de TI em relação ao valor dos ativos da organização.	<ul style="list-style-type: none"> <li>Nível de impacto inesperado a organização.</li> <li>Percentual dos riscos de TI que excedem a tolerância de risco da organização.</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

EDM03 Tabela RACI

Prática de Governança	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (CDO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Conselho de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>EDM03.01</b> Avaliar a gestão de risco	A	R	C	C	R	C	R		I	R	C	I	C	C	C	R	C								C	
<b>EDM03.02</b> Diracionar a gestão de risco.	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I		
<b>EDM03.03</b> Monitorar a gestão dos riscos.	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	C		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

EDM03 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM03.01 Avaliar a gestão de risco</b> Continuamente examinar e avaliar o efeito do risco sobre o uso atual e futuro da TI na organização. Considerar se o apetite de risco da organização é adequado e se o risco para o valor da organização relacionado ao uso da TI é identificado e controlado.	APO12.01	• Assuntos e fatores de Riscos emergentes	• Orientação de apetite ao risco	APO12.03
		Referência externa ao COBIT	• Princípios de gestão de risco corporativo	• Níveis aprovados de tolerância ao risco APO12.01
<b>Atividades</b>				
01 Determinar o nível de risco de TI relacionado com o risco que a organização está disposta a tomar para atingir os seus objetivos (apetite de risco).				
02 Avaliar e aprovar propostas de limites de tolerância ao risco de TI em relação aos níveis de risco e de oportunidade aceitáveis da organização.				
03 Determinar o escopo do alinhamento da estratégia de risco de TI para a estratégia de risco corporativo.				
04 Avaliar de forma proativa e antecipada os fatores do risco de TI e as decisões corporativas estratégicas pendentes para garantir que a organização esteja consciente dos riscos e das decisões que são tomadas.				
05 Determinar que o uso de TI é objeto de análise de risco adequada e sujeita a processo de avaliação, conforme descrito em padrões nacionais e internacionais relevantes.				
06 Avaliar as atividades de gestão de riscos para garantir o alinhamento entre a capacidade das perdas de TI e a tolerância da organização.				
Prática de Governança	Entradas		Saídas	
<b>EDM03.02 Direccionar a gestão de risco</b> Diracionar a implementação de práticas de gestão de risco para fornecer segurança razoável de que práticas de gestão do risco de TI são adequadas para garantir que o risco de TI observado não excede o apetite de risco do conselho de administração.	APO12.03	De	Descrição	Descrição
		Perfil de risco agregado incluindo o status das ações de gestão de risco	Políticas de gestão de risco	APO12.01
		Referência externa ao COBIT	Principais objetivos a serem monitorados pela gestão de riscos	APO12.01
		Gerenciamento de risco corporativo (ERM) perfis e planos de mitigação	Processo aprovado para medir a gestão de risco	APO12.01

# COBIT® 5 : HABILITANDO PROCESSOS

## EDM03 Práticas de Processo, Entradas/Saídas e Atividades

Atividades
01 Promover uma cultura de conscientização dos riscos de TI e capacitar a organização para identificar de forma proativa os riscos de TI, oportunidades e impactos potenciais aos negócios
02 Direcionar a integração da estratégia de risco de TI e das operações com as decisões de risco estratégicos e operações da organização.
03 Direcionar o desenvolvimento de planos de comunicação de risco (abrangendo todos os níveis da organização), bem como os planos de ação de risco.
04 Dirigir a implementação direta dos mecanismos apropriados para responder rapidamente às mudanças aos riscos e reportar imediatamente aos níveis adequados de gestão, apoiados por princípios acordados de escalada (o que reportar, quando, onde e como).
05 Criar diretrizes para que premissas de risco, oportunidades, problemas e preocupações possam ser identificados e relatados por qualquer pessoa a qualquer momento. Risco deve ser gerido em conformidade com as políticas e procedimentos publicados e encaminhado para os tomadores de decisão relevantes.
06 Identificar as principais metas e métricas de processos de governança e gestão de risco a serem monitorados, e aprovar as abordagens, métodos, técnicas e processos para capturar e relatar as informações de medição.

## Prática de Governança

Entradas	Saídas		
De	Descrição	Para	Descrição
APO12.02	<ul style="list-style-type: none"> <li>• Resultados das análises de risco</li> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• Ações corretivas para direcionar os desvios na gestão de riscos.</li> </ul>	APO12.06
APO12.04	<ul style="list-style-type: none"> <li>• Oportunidades para aceitação de grandes riscos</li> <li>• Resultados das avaliações de riscos realizadas por terceiros</li> <li>• Análise de risco e relatórios do perfil de risco para as partes interessadas</li> </ul>	<ul style="list-style-type: none"> <li>• Questões de gestão de riscos para o Conselho de Administração</li> </ul>	EDM05.01

## Atividades

01 Monitorar o escopo da gestão do perfil de risco dentro dos limites do apetite de risco.
02 Monitorar principais metas e métricas de governança de riscos e processos de gestão em relação aos objetivos, analisar as causas de eventuais desvios, e iniciar ações corretivas para resolver as causas raízes.
03 Habilitar avaliação do progresso da empresa em direção às metas identificadas pelas principais partes interessadas.
04 Reportar quaisquer problemas de gestão de risco para o conselho ou comitê executivo.

## EDM03 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
COSO/ERM	
ISO/IEC 31000	Modelo para Gestão de Riscos
ISO/IEC 38500	
King III	5.5 TI deve fazer parte integrante da gestão de risco da organização. 5.7 Comitês de riscos e de auditoria devem auxiliar o conselho de administração no exercício das suas responsabilidades de TI.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

EDM04 Garantir a Otimização de Recursos	Área: Governança Domínio: Avaliar, Dirigir e Monitorar
<b>Descrição do Processo</b> Certifique-se de que as capacidades adequadas e suficientes relacionadas a TI (pessoas, processos e tecnologia) estão disponíveis para apoiar os objetivos corporativos de forma eficaz a um custo eficiente.	
<b>Descrição do Objetivo de Processo</b> Assegurar que as necessidades de recursos da organização são cumpridas de maneira eficiente, os custos de TI são otimizados, e há uma maior probabilidade de realização do benefício e preparação para mudanças futuras.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
09 Agilidade de TI	<ul style="list-style-type: none"> <li>Nível de satisfação dos executivos de negócios com TI e a capacidade de resposta a novos requisitos</li> <li>Número de processos críticos de negócio suportados por arquitetura atualizada de infraestrutura e aplicações</li> <li>Tempo médio para transformar objetivos estratégicos de TI em iniciativas acordadas e aprovadas</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência da avaliação de maturidade e análise de otimização de custos</li> <li>Tendência dos resultados da avaliação</li> <li>Níveis de satisfação dos executivos de negócio e de TI relacionados aos custos e capacidades de TI</li> </ul>
16 Equipes de TI e de negócios motivadas e qualificadas	<ul style="list-style-type: none"> <li>Percentual dos funcionários que possuem habilidades de TI suficientes e competência necessária para assumir seu respectivo papel na organização</li> <li>Percentual dos funcionários satisfeitos com as suas funções relacionadas com a TI</li> <li>Número de horas de treinamento / formação por funcionário</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 As necessidades de recursos da organização são atendidas com eficiência de recursos.	<ul style="list-style-type: none"> <li>Nível de feedback das partes interessadas sobre a otimização de recursos</li> <li>Número de benefícios (por exemplo, redução de custos) conseguida através da utilização eficiente dos recursos</li> <li>Número de desvios do plano de recursos e estratégias de arquitetura corporativa</li> </ul>
02 Os recursos são alocados da melhor forma às prioridades dentro das restrições orçamentárias corporativas.	<ul style="list-style-type: none"> <li>Número de desvios e exceções aos princípios de gestão de recursos</li> <li>Percentual dos projetos com a alocação adequada de recursos.</li> </ul>
03 A utilização eficiente dos recursos é obtida ao longo do alcance dos seus ciclos de vida econômicos.	<ul style="list-style-type: none"> <li>Percentual de reutilização dos componentes da arquitetura</li> <li>Percentual dos projetos e programas com status de médio ou alto risco devido a questões de gestão de recursos</li> <li>Número dos objetivos de gestão de desempenho alcançados.</li> </ul>

# COBIT® 5 : HABILITANDO PROCESSOS

EDM04 Tabela RACI

Prática de Governança	Conselho de Administração	Diretor Executivo   Presidente (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escrítorio de Programas e Projetos (PMO)	Escrítorio de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>EDM04.01</b> Avaliar a gestão de recursos	A	R	C	C	R	R	I	C	C	C	C	C	C	C	C	C	R	C	C	C	I	I	I	I	I
<b>EDM04.02</b> Dirionar a gestão de recursos.	A	R	C	C	R	I	R	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
<b>EDM04.03</b> Monitorar a gestão de recursos	A	R	C	C	R	I	R	I	I	I	C	C	C	C	C	C	R	C	C	C	I	I	I	I	I

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

EDM04 Práticas de Processo, Entradas/Saídas e Atividades

Práticas de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM04.01 Avaliar a gestão de recursos</b> Examinar continuamente e fazer avaliações sobre a necessidade atual e futura relacionados aos recursos de TI, opções para mobilização dos recursos (incluindo estratégias de terceirização), e princípios de atribuição e gestão para atender as necessidades da organização de maneira eficiente.	APO02.04	• Lacunas e mudanças necessárias para atingir o objetivo de maturidade	• Princípios de orientação para alocação de recursos e competências.	APO02.01 APO07.01 BAI03.11
	APO07.03	• Plano de desenvolvimento de competências	• Princípios de orientação para a arquitetura corporativa	AP003.01
	APO10.02	• Resultados e decisões das avaliações de fornecedores	• Plano de recursos aprovados	AP002.05 AP007.01 AP009.02

## Atividades

- 01 Examinar e avaliar a estratégia atual e futura, das opções para fornecer recursos de TI e desenvolvimento de competências para atender às necessidades atuais e futuras (incluindo opções de terceirização).
- 02 Definir os princípios para orientar a alocação e gestão dos recursos e capacidades para que a TI possa atender as necessidades da empresa, com a maturidade e capacidade necessária de acordo com as prioridades acordadas e restrições orçamentárias.
- 03 Rever e aprovar as estratégias corporativas do plano de recursos e arquitetura para a entrega de valor agregado e redução de riscos com os recursos alocados.
- 04 Entender os requisitos para alinhar a gestão de recursos com o planejamento corporativo financeiro e de recursos humanos (RH).
- 05 Definir princípios para a gestão e controle da arquitetura corporativa.

Práticas de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM04.01 Direccionar o gerenciamento de recursos</b> Garantir a implementação de princípios de gestão de recursos para permitir a utilização eficiente dos recursos de TI ao longo do alcance dos seus ciclos de vida econômicos.			<ul style="list-style-type: none"> <li>• Comunicação das estratégias de mobilização dos recursos</li> <li>• Responsabilidades atribuídas para a gestão de recursos</li> <li>• Princípios para a preservação dos recursos</li> </ul>	APO02.06 APO07.05 APO09.02
				APO01.02 DSS06.03
				APO01.04

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

EDM04 Práticas de Processo, Entradas/Saídas e Atividades						
Atividades						
01 Comunicar e impulsionar a adoção das estratégias de gestão de recursos, princípios, e planos de recursos e estratégias de arquitetura corporativa acordados.						
02 Atribuir responsabilidades para execução da gestão de recursos.						
03 Definir objetivos principais, medidas e métricas para gestão de recursos.						
04 Estabelecer princípios relacionados com a proteção dos recursos						
05 Alinhar a gestão de recursos com o planejamento financeiro e RH da organização						
Práticas de Governança		Entradas		Saídas		
EDM04.03 Monitorar a gestão de recursos		De	Descrição	Descrição		
Monitorar as principais metas e métricas dos processos de gestão de recursos e estabelecer como desvios ou problemas serão identificados, rastreados e reportados para correção.				• Comentários sobre alocação e eficácia dos recursos e competências.		
				EDM05.01 APO02.05 APO07.05 APO09.05		
Atividades						
01 Monitorar a alocação e otimização dos recursos de acordo com os objetivos e prioridades da organização usando metas e métricas acordadas.						
02 Monitorar TI estratégias de fornecedores, estratégias de arquitetura corporativa, recursos e capacidades de TI para garantir que as necessidades atuais e futuras da organização possam ser cumpridas.						
03 Monitorar o desempenho de recursos aos objetivos acordados, analisar a causa de desvios e iniciar medidas corretivas para resolver as causas raízes.						
EDM04 Orientação Relacionada						
Padrão Relacionado		Referência Detalhada				
ISO/IEC 38500						
King III		5.6 . O conselho deve assegurar que os ativos de informação são geridos de maneira eficaz.				
The Open Group Architecture Forum (TOGAF) 9		Componentes TOGAF para um Conselho, Governança e Maturidade de Arquitetura Modelos para mapear a otimização de recursos.				



## EDM05 Garantir a Transparência para as Partes Interessadas

Área: Governança

Dominio: Avaliar, Dirigir e Monitorar

**Descrição do Processo**

Garantir que a medição e o reporte do desempenho e da conformidade corporativa de TI são transparentes, com as partes interessadas aprovando metas e métricas e as ações de remediação necessárias.

**Declaração de Propósito do Processo**

Garantir que a comunicação com as partes interessadas seja eficaz e tempestiva e que a base para reporte seja estabelecida para aumentar o desempenho, identificar áreas para melhorias e confirmar que os objetivos e estratégias relacionados a TI estejam em linha com a estratégia corporativa.

**O processo suporta a realização de um conjunto primário de objetivos de TI:**

Objetivos de TI	Métricas Relacionadas
03 Compromisso da gerência executiva com a tomada de decisões de TI	<ul style="list-style-type: none"> <li>Percentual de papéis da gerência executiva com obrigações claramente definidas para decisões de TI</li> <li>Número de vezes que a TI está na agenda conselho de maneira proativa</li> <li>Frequência das reuniões do comitê (executivo) estratégico de TI</li> <li>Taxa de execução de decisões executivas relacionadas a TI</li> </ul>
06 Transparência dos custos, benefícios e riscos de TI	<ul style="list-style-type: none"> <li>Percentual de estudos de caso de investimentos com custos e benefícios esperados em relação a TI claramente definidos e aprovados</li> <li>Percentual de serviços de TI com custos operacionais e benefícios esperados claramente definidos e aprovados</li> <li>Pesquisa de satisfação com as partes interessadas sobre o nível de transparência, compreensão e precisão das informações financeiras de TI</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de eventos disruptivos de negócios devido a incidentes em serviços de TI</li> <li>Percentual de partes interessadas da área de negócios satisfeitas que o serviço de TI prestado atende aos níveis de serviço definidos</li> <li>Percentual de usuários satisfeitos com a qualidade do serviço de TI prestado</li> </ul>

**Objetivos e Métricas do Processo**

Objetivo do Processo	Métricas Relacionadas
01 O reporte às partes interessadas está de acordo com os requisitos das partes interessadas.	<ul style="list-style-type: none"> <li>Data da última revisão dos requisitos de reporte</li> <li>Percentual de partes interessadas cobertas nos requisitos de reporte</li> </ul>
02 O reporte é completo, tempestivo e preciso.	<ul style="list-style-type: none"> <li>Percentual de relatórios que não são entregues no prazo</li> <li>Percentual de relatórios contendo informações imprecisas</li> </ul>
03 A comunicação é eficaz e as partes interessadas estão satisfeitas.	<ul style="list-style-type: none"> <li>Nível de satisfação das partes interessadas com o reporte</li> <li>Número de falhas no reporte de requisitos obrigatórios</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Avaliar, Dirigir e Monitorar

EDM05 Tabela RACI

Prática de Governança	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
EDM05.01 Avaliar requisitos de reporte das partes interessadas.	A	R	C	C	C	I										C	C	R	I				I			
EDM05.02 Orientar comunicação e reporte com partes interessadas.	A	R	C	C	C	I										C	C	R	I				I			
EDM05.03 Monitorar comunicação com partes interessadas.	A	R	C	C	C	I										C	C	R	I				I			

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

EDM05 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Governança	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>EDM05.01 Avaliar requerimentos de reporte das partes interessadas.</b>  Examinar e julgar continuamente os requisitos atuais e futuros de comunicação e reporte às partes interessadas, incluindo requisitos de reporte obrigatórios (ex. regulatório) e comunicação com outras partes interessadas. Estabelecer os princípios para a comunicação.	EDM02.03	• Ações para aumentar a entrega de valor	• Avaliação dos requisitos de reporte corporativos	MEA01.01
	EDM03.03	• Questões de Gestão de risco para o Conselho	• Princípios de reporte e comunicação	MEA01.01
	EDM04.03	• Feedback sobre a alocação e eficácia dos recursos e capacidades		
	MEA02.08	• Escopo refinado		

## Atividades

01 Examinar e julgar os requisitos atuais e futuros de reportes obrigatórios relacionados ao uso de TI na organização (regulação, legislação, common law, contratual), incluindo a extensão e a frequência.

02 Examinar e julgar os requisitos atuais e futuros de reportes a outras partes interessadas relacionados ao uso de TI na organização, incluindo a extensão e a frequência.

03 Manter princípios para comunicação com partes interessadas externas e internas (incluindo formatos de comunicação e canais de comunicação) e para aceitação e conclusão dos relatórios pelas partes interessadas.

Práticas de Governança	Entradas		Saídas	
	De	Descrição	De	Descrição
<b>EDM05.02 Orientar comunicação e reporte com partes interessadas.</b>  Assegurar o estabelecimento de comunicação e reporte eficazes às partes interessadas, incluindo mecanismos para garantir a qualidade e a integridade das informações, supervisão dos relatórios obrigatórios e criando uma estratégia de comunicação com as partes interessadas.	APO12.04	• Análise de riscos e relatórios de perfil de risco para as partes interessadas	• Regras para validação e aprovação de relatórios obrigatórios	MEA01.01
			• Diretrizes de escalonamento	MEA01.05

# COBIT® 5 : HABILITANDO PROCESSOS

## EDM05 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
Prática de Governança		Entradas	Saídas	
<b>EDM05.03 Monitorar comunicação com partes interessadas.</b> Monitorar a eficácia da comunicação com as partes interessadas. Analisar mecanismos que garantem a precisão, confiabilidade e eficácia e verificar se os requisitos das diferentes partes interessadas são atendidos.	MEA02.08	<ul style="list-style-type: none"> <li>• Relatório de análise de asseguração</li> <li>• Resultados da análise de asseguração</li> </ul>	<ul style="list-style-type: none"> <li>• Análise da eficácia dos relatórios</li> </ul>	MEA01.01 MEA03.04
Atividades				
01 Analisar periodicamente a eficácia dos mecanismos que garantem a precisão, confiabilidade e eficácia dos reportes obrigatórios.				
02 Analisar periodicamente a eficácia dos mecanismos de, e resultados da, comunicação com partes interessadas externas e internas.				
03 Determinar se os requisitos das diferentes partes interessadas são atendidos.				

## EDM05 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
COSO	
ISO/IEC 38500	
King III	

# ALINHAR, PLANEJAR E ORGANIZAR (APO)

- 01 Gerenciar a estrutura de gestão de TI.
- 02 Gerenciar a estratégia.
- 03 Gerenciar arquitetura da organização.
- 004 Gerenciar inovação.
- 05 Gerenciar portfolio.
- 06 Gerenciar orçamento e custos.
- 07 Gerenciar recursos humanos.
- 08 Gerenciar relacionamentos.
- 09 Gerenciar contratos de prestação de serviços.
- 10 Gerenciar fornecedores.
- 11 Gerenciar qualidade.
- 12 Gerenciar riscos.
- 13 Gerenciar segurança

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

APO01 Gerenciar a Estrutura de Gestão de TI	Área: Gestão Domínio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b>	
Esclarecer e manter a missão e a visão da governança corporativa de TI. Implementar e manter mecanismos e autoridades para gerir a informação e o uso de TI na organização para suporte dos objetivos de governança em linha com princípios e políticas de orientação.	
<b>Declaração de Propósito do Processo</b>	
Prover uma abordagem de gerenciamento consistente para permitir que os requisitos de governança corporativa sejam cumpridos, cobrindo processos de gestão, estruturas organizacionais, papéis e responsabilidades, atividades confiáveis e repetíveis e habilidades e competências.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de objetivos e requisitos estratégicos corporativos suportados por objetivos estratégicos de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio de programas e serviços planejado</li> <li>Percentual de direcionadores de valor de TI mapeados em função de direcionadores de valor de negócios</li> </ul>
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo da não conformidade de TI, incluindo acordos e multas e o impacto da perda de reputação</li> <li>Número de não conformidades relacionadas a TI reportadas ao conselho de administração ou que causaram críticas públicas ou constrangimento</li> <li>Número de não conformidades relacionadas a acordos contratuais com provedores de serviço de TI</li> <li>Cobertura das análises de conformidade</li> </ul>
09 Agilidade de TI	<ul style="list-style-type: none"> <li>Nível de satisfação dos executivos de negócios com a capacidade de resposta da TI para novos requerimentos</li> <li>Número de processos críticos de negócios suportados por infraestrutura e aplicações atualizadas</li> <li>Tempo médio para transformar objetivos estratégicos de TI em uma iniciativa acordada e aprovada</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência de análises de capacidade da maturidade e de otimização de custos</li> <li>Tendência dos resultados das análises</li> <li>Nível de satisfação dos executivos de negócios e de TI com os custos e capacidades relacionadas a TI</li> </ul>
15 Conformidade de TI com as políticas internas	<ul style="list-style-type: none"> <li>Número de incidentes relacionados a não conformidade com políticas</li> <li>Percentual das partes interessadas que entendem as políticas</li> <li>Percentual de políticas suportadas por padrões efetivos e práticas de trabalho</li> <li>Frequência de revisão e atualização de políticas</li> </ul>
16 Equipes de TI e de negócios motivadas e qualificadas	<ul style="list-style-type: none"> <li>Percentual da equipe com habilidades relacionadas a TI suficientes para a competência requerida para o seu papel</li> <li>Percentual da equipe satisfeita com seu papel relacionado a TI</li> <li>Número de horas de aprendizado/treinamento por membro da equipe</li> </ul>
17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>Nível de consciência e entendimento dos executivos de negócios quanto às possibilidades de inovação de TI</li> <li>Nível de satisfação das partes interessadas com os níveis de expertise e ideias para inovação de TI</li> <li>Número de iniciativas aprovadas resultantes de ideias inovadoras de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Um conjunto eficaz de políticas está definido e mantido.	<ul style="list-style-type: none"> <li>Percentual de políticas, padrões e outros habilitadores documentados e atualizados ativos</li> <li>Data da última atualização do modelo e dos habilitadores</li> <li>Número de exposições a risco devido a inadequações no desenho do ambiente de controles</li> </ul>
02 Todos estão cientes das políticas e de como elas devem ser implementadas.	<ul style="list-style-type: none"> <li>Número de pessoas que participou de sessões de treinamento ou de aprendizado</li> <li>Percentual de fornecedores terceirizados que possuem contratos definindo requisitos de controle</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

EDMO1 Tabela RACI

	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Segurança da Informação	Gerente de Contabilidade dos Negócios	Oficial de Privacidade
<b>Prática de Governança</b>																									
<b>APO01.01</b> Definir a estrutura organizacional.	C	C	C	C	I	C					R	I	I	A	C	C	C	R	C	C	C	C			
<b>APO01.02</b> Estabelecer papéis e responsabilidades.					I	C		C			C	C	C	A	C	C	C	R	C	C	C	C			
<b>APO01.03</b> Manter os habilitadores do sistema de gerenciamento.	C	A	C	R	C	C	I		C	C	C	C	C	C	R			R							
<b>APO01.04</b> Comunicar objetivos e direcionadores de gerenciamento.	A	R	R	R	I	R	I	I	I	R	R	I	I	I	I	R	I	I	I	I	I	I	I		
<b>APO01.05</b> Otimizar o posicionamento da função de TI.	C	C	C	C	A	C					C	C	C	R	C	C	C	R	C	C	C				
<b>APO01.06</b> Definir a propriedade das informações (dados) e sistemas.	I	I	C	A	R						C	C	C	C	C				C	C				C	C
<b>APO01.07</b> Gerenciar o melhoramento contínuo de processos.			A	R		R		R		C	I	C	C	R	R	R	R	R	R	R	R	R	R		
<b>APO01.08</b> Manter a conformidade com políticas e procedimentos.	A			R		R		R		R	R	C	I	R	R	R	R	R	R	R	R	R	R		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO01.01 Definir a estrutura organizacional.</b> Estabelecer uma estrutura organizacional interna e estendida que reflete as necessidades do negócio e as prioridades de TI. Colocar em prática as estruturas de gerenciamento requeridas (ex: comitês) que permitam que a tomada de decisão gerencial ocorra de maneira mais eficaz e eficiente.	EDM01.01	<ul style="list-style-type: none"> <li>• Modelo de tomada de decisão</li> <li>• Guia de princípios de governança corporativa</li> </ul>	<ul style="list-style-type: none"> <li>• Definição da estrutura e funções da organização</li> </ul>	APO03.02
	APO03.02	<ul style="list-style-type: none"> <li>• Modelo de arquitetura de processos</li> </ul>	<ul style="list-style-type: none"> <li>• Diretrizes operacionais da organização</li> <li>• Regras básicas de comunicação</li> </ul>	APO03.02 Todos APO Todos BAI Todos DSS Todos MEA
<b>Atividades</b>				
01 Definir o escopo, funções internas e externas, papéis internos e externos e capacidades e direitos de decisão necessários, incluindo aquelas atividades de TI realizadas por terceiros.				
02 Identificar decisões necessárias para a realização de resultados corporativos e da estratégia de TI e para o gerenciamento e execução dos serviços de TI.				
03 Estabelecer o envolvimento das partes interessadas que são críticas na tomada de decisão (responsável, presta contas, consultado ou informado).				
04 Alinhar a organização de TI ao modelo organizacional da arquitetura corporativa.				
05 Definir o foco, papéis e responsabilidades de cada função dentro da estrutura organizacional de TI.				
06 Definir as estruturas e relacionamentos do gerenciamento para suportar as funções e papéis de gerenciamento e de execução, alinhados ao conjunto de diretrizes de governança.				
07 Estabelecer um comitê estratégico de TI (ou equivalente) no nível do conselho de administração. Esse comitê deve garantir que a governança de TI, como parte da governança corporativa, é endereçada adequadamente; aconselhar no direcionamento estratégico; e revisar grandes investimentos em nome do conselho de administração completo.				
08 Estabelecer um comitê direutivo de TI (ou equivalente), composto de executivos, gestores de negócios e de TI, para determinar a priorização de programas de investimentos habilitados pela TI em linha com a estratégia de negócios e prioridades corporativas; acompanhar o andamento de projetos e resolver conflitos de recursos; e monitorar os níveis de serviço e as melhorias no serviço.				
09 Prover diretrizes para cada estrutura de gerenciamento (incluindo mandato, objetivos, participantes da reunião, periodicidade, controle, supervisão e fiscalização), assim como os insumos requeridos e os resultados esperados das reuniões.				
10 Definir regras básicas de comunicação por meio da identificação das necessidades de comunicação e implementação dos planos baseados nessas necessidades, considerando as comunicações de cima para baixo, de baixo para cima e horizontal.				
11 Estabelecer e manter uma estrutura otimizada de coordenação, comunicação e conexão entre as funções de negócios e de TI da organização e com entidades externas à organização.				
12 Verificar regularmente a adequação e a eficácia da estrutura organizacional.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas			Saídas
	De	Descrição	Descrição	
<b>APO01.02 Estabelecer papéis e responsabilidades.</b> Estabelecer, acordar e comunicar papéis e responsabilidades do pessoal de TI, bem como outras partes interessadas com responsabilidades pela TI corporativa, que refletem claramente as necessidades gerais do negócio e os objetivos de TI e a autoridade, a responsabilidade e a obrigação de prestar contas do pessoal relevante.	EDM01.01	• Níveis de autoridade	• Definição de papéis e responsabilidades relacionados a TI	DSS05.04
	EDM04.02	• Responsabilidades atribuídas para o gerenciamento de recursos	• Definição das práticas de supervisão	APO07.01
	APO07.03	• Planos de desenvolvimento de habilidades • Matriz de habilidades e competências		
	APO11.01	• Papéis, responsabilidades e direitos de decisão do sistema de gestão da qualidade (SGQ)		
	APO13.01	• Declaração de escopo do sistema de gestão da segurança da informação (SGSI)		
	DSS06.03	• Níveis de autoridade definidos • Papéis e responsabilidades definidos		

## Atividades

- 01 Estabelecer, acordar e comunicar os papéis e responsabilidades relacionados a TI a todo o pessoal da organização, de acordo com as necessidades e objetivos de negócios. Delinear claramente responsabilidades e obrigações de prestar contas, especialmente para tomadas de decisão e aprovações.
- 02 Considerar os requisitos da organização e de continuidade dos serviços de TI quando da definição de papéis, incluindo requisitos de backup e de treinamento cruzado de pessoal.
- 03 Fornecer insumos para o processo de continuidade do serviço de TI por meio da manutenção das informações de contato e da descrição de papéis atualizada na organização.
- 04 Incluir, nas descrições de papéis e responsabilidades, a aderência às políticas e procedimentos de gerenciamento, ao código de ética e às práticas profissionais.
- 05 Implementar práticas de supervisão adequadas para garantir que os papéis e responsabilidades são exercidos apropriadamente, para analisar se todo o pessoal possui autoridade e recursos suficientes para executar seus papéis e responsabilidades e para avaliar o desempenho geral. O nível de supervisão deve estar em linha com a sensibilidade da posição e extensão das responsabilidades atribuídas.
- 06 Garantir que a obrigação de prestar contas é definida por meio de papéis e responsabilidades.
- 07 Estruturar papéis e responsabilidades para reduzir a possibilidade de uma única função comprometer um processo crítico.

Prática de Gestão	Entradas			Saídas
	De	Descrição	Descrição	
<b>APO01.03 Manter os habilitadores do sistema de gerenciamento.</b> Manter os habilitadores do sistema de gerenciamento e ambiente de controles para a TI corporativa e garantir que eles estão integrados e alinhados com a filosofia e estilo operacional de governança e gestão da organização. Esses habilitadores incluem a comunicação clara de expectativas/requisitos. O sistema de gerenciamento deve encorajar cooperação entre divisões e trabalho em equipe, promover a conformidade e o melhoramento contínuo e lidar com desvios no processo (incluindo falhas).	EDM01.01	• Guia de princípios de governança corporativa	• Políticas relacionadas a TI	Todos APO Todos BAI Todos DSS Todos MEA
	APO02.05	• Roteiro estratégico		
	APO12.01	• Questões e fatores de risco emergentes		
	APO12.02	• Resultados das análises de risco		

# COBIT® : HABILITANDO PROCESSOS

## APO01 Práticas de Processo, Entradas/Saídas e Atividades

Atividades
01 Obter um entendimento da visão, do direcionamento e da estratégia da organização.
02 Considerar o ambiente interno da organização, incluindo cultura e filosofia de gerenciamento, tolerância ao risco, segurança, valores éticos, código de conduta, obrigação de prestar contas e requisitos para integridade do gerenciamento.
03 Derivar e integrar princípios de TI com princípios de negócios.
04 Alinhar o ambiente de controles de TI com o ambiente geral das políticas de TI, governança de TI, modelos de processos de TI e modelos de riscos e controles existentes em nível corporativo. Analisar boas práticas ou requisitos específicos da indústria (ex: regulamentações específicas da indústria) e integrá-las sempre que necessárias.
05 Alinear com quaisquer padrões de governança e de gestão nacionais e internacionais e códigos de conduta aplicáveis e avaliar boas práticas disponíveis, tais como COSO Internal Control—Integrated Framework e COSO Enterprise Risk Management—Integrated Framework.
06 Criar um conjunto de políticas para direcionar as expectativas de controle de TI em tópicos relevantes, tais como qualidade, segurança, confidencialidade, controles internos, uso dos ativos de TI, ética e direitos de propriedade intelectual.
07 Avaliar e atualizar as políticas ao menos anualmente para acomodar mudanças no ambiente operacional ou de negócios.
08 Implementar e aplicar políticas de TI para todo o pessoal relevante, para que elas sejam incorporadas e sejam parte integrante das operações da organização.
09 Garantir que procedimentos estão implementados para acompanhar a conformidade com as políticas e definir as consequências de não conformidades.

Prática de Gestão	Entradas	Saídas		
<b>APO01.04 Comunicar objetivos e direcionadores de gerenciamento.</b> Conscientizar e comunicar o entendimento dos objetivos e do direcionamento de TI às partes interessadas e usuários apropriados em toda a organização.	De	Descrição	Descrição	Para
	EDM01.02	• Comunicação da governança corporativa	• Comunicação sobre os objetivos de TI	Todos APO Todos BAI Todos DSS Todos MEA
	EDM04.02	• Princípios para preservação de recursos		
	APO12.06	• Comunicação de impacto dos riscos		
	BAI08.01	• Comunicação sobre o valor do conhecimento		
	DSS04.01	• Políticas e objetivos para continuidade de negócios		
	DSS05.01	• Política de prevenção de software malicioso		
	DSS05.02	• Política de segurança de conectividade		
	DSS05.03	• Políticas de segurança para dispositivos endpoint		

Atividades
01 Comunicar continuamente os objetivos e o direcionamento de TI. Garantir que as comunicações são suportadas pela gerência executiva em ações e palavras, utilizando todos os canais disponíveis.
02 Garantir que a informação transmitida engloba uma missão claramente articulada, objetivos de serviço, segurança, controles internos, qualidade, código de ética/conduta, políticas e procedimentos, papéis e responsabilidades, etc. Transmitir a informação no nível de detalhe adequado à respectiva audiência na organização.
03 Fornecer recursos suficientes e qualificados para apoiar o processo de comunicação.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Alinhar, Planejar e Organizar

**APO01 Práticas de Processo, Entradas/Saídas e Atividades**

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO01.05 Otimizar o posicionamento da função de TI.</b> Posicionar a capacidade de TI na estrutura organizacional geral para refletir um modelo corporativo pertinente à importância da TI na organização, especificamente a sua criticidade para a estratégia da empresa e o grau de dependência operacional em TI. A linha de reporte do CIO deve ser proporcional à importância da TI na organização.	Externo ao COBIT	<ul style="list-style-type: none"> <li>Modelo operacional corporativo</li> <li>Estratégia corporativa</li> </ul>	<ul style="list-style-type: none"> <li>Avaliação das opções para a estrutura de TI</li> <li>Posição operacional definida para a TI</li> </ul>	APO03.02  APO03.02
<b>Atividades</b>				
01 Entender o contexto para o posicionamento da função de TI, incluindo uma análise da estratégia e modelo operacional corporativo (centralizado, federado, descentralizado, híbrido), importância da TI e situação e opções de terceirização.				
02 Identificar, avaliar e priorizar opções para modelos de posicionamento organizacional, de terceirização e de operação.				
03 Definir o posicionamento da função de TI e obter a aprovação.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO01.06 Definir a propriedade das informações (dados) e sistemas.</b> Definir e manter responsabilidades para a propriedade das informações (dados) e sistemas de informação. Garantir que os proprietários tomem decisões sobre a classificação de informações e sistemas e os protejam de acordo com essa classificação.			<ul style="list-style-type: none"> <li>Diretrizes de classificação de dados</li> <li>Diretrizes de segurança e controles</li> <li>Procedimentos para integridade de dados</li> </ul>	APO03.02 BAI02.01 DSS05.02 DSS06.01  BAI02.01  BAI02.01 DSS06.01
<b>Atividades</b>				
01 Fornecer políticas e diretrizes para garantir uma classificação da informação (dados) apropriada e consistente em toda a organização.				
02 Definir, manter e fornecer ferramentas, técnicas e diretrizes apropriadas para proporcionar segurança e controles eficazes sobre informações e sistemas de informação em apoio ao proprietário.				
03 Criar e manter um inventário de informações (sistemas e dados) que inclui uma lista dos proprietários, custodiantes e classificações. Incluir sistemas que são terceirizados e aqueles para os quais a propriedade deve estar com a organização.				
04 Definir e implementar procedimentos para garantir a integridade e consistência de todas as informações armazenadas eletronicamente, tais como bases de dados, data warehouses e arquivos de dados.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO01.07 Gerenciar o melhoramento contínuo de processos.</b> Analisa, planeja e executa o melhoramento contínuo de processos e sua maturidade para garantir que sejam capazes de entregar diante dos objetivos corporativos, de governança, de gestão, e de controle. Considerar o guia de implementação de processos do COBIT, padrões emergentes, requerimentos de conformidade, oportunidades de automação e o feedback de usuários do processo, da equipe de processos e de outras partes interessadas. Atualizar o processo e considerar os impactos nos habilitadores de processos.	EDM01.03	<ul style="list-style-type: none"> <li>Feedback sobre eficácia e desempenho da governança</li> </ul>	<ul style="list-style-type: none"> <li>Análise da capacidade dos processos</li> </ul>	MEA01.03
	MEA03.02	<ul style="list-style-type: none"> <li>Políticas, princípios, procedimentos e padrões atualizados</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidades de melhoria nos processos</li> <li>Objetivos e métricas de desempenho para rastreamento da melhoria de processos</li> </ul>	Todos APO Todos BAI Todos DSS Todos MEA  MEA01.02
<b>Atividades</b>				
01 Identificar os processos críticos de negócios por meio de direcionadores e de riscos relacionados ao desempenho e à conformidade. Avaliar a capacidade do processo e identificar objetivos para melhorias. Analisar falhas na capacidade e controle do processo. Identificar opções para melhoria e redesenho do processo. Priorizar iniciativas para melhoria do processo baseado nos potenciais benefícios e custos.				
02 Implementar melhorias acordadas, operar com práticas negócio adequadas e definir objetivos e métricas de desempenho para permitir o monitoramento de melhorias no processo.				
03 Considerar meios para melhorar a eficiência e a eficácia (ex: por meio de treinamentos, documentação, padronização e automação do processo).				
04 Aplicar práticas de gestão da qualidade para atualizar o processo.				
05 Aposentar processos, componentes de processos ou habilitadores obsoletos.				

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas			
	De	Descrição	Descrição	Para		
<b>APO01.08 Manter a conformidade com políticas e procedimentos.</b> Colocar em prática procedimentos para manter a conformidade e medir o desempenho de políticas e outros habilitadores do modelo de controle e reforçar as consequências de não conformidades ou desempenho inadequado. Acompanhar tendências e desempenho e considerá-los no desenho e melhoria futuros do modelo de controles.	DSS01.04	• Políticas ambientais	• Ações corretivas para não conformidades	MEA01.05		
	MEA03.02	• Políticas, princípios, procedimentos e padrões atualizados				
<b>Atividades</b>						
01 Acompanhar a conformidade com políticas e procedimentos.						
02 Analisar não conformidades e tomar as ações apropriadas (o que poderia incluir necessidade de mudanças).						
03 Integrar desempenho e conformidade nos objetivos de desempenho de cada membro da equipe.						
04 Avaliar regularmente o desempenho dos habilitadores do modelo e tomar as ações adequadas.						
05 Analisar tendências no desempenho e na conformidade e tomar as ações adequadas.						

## APO 01 Orientação Relacionada

ISO/IEC 20000	3.1 Responsabilidade da direção 4.4 Melhoria contínua
ISO/IEC 27002	06 Organizando a Segurança da Informação
ITIL V3 2011	Melhoria de Serviço Continuada, 4.1 O Processo de Melhoria de 7 passos

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO02 Gerenciar a Estratégia	Área: Gestão Domínio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b> <p>Prover uma visão holística dos ambientes atuais de negócios e de TI, a direção futura e as iniciativas necessárias para migrar para o ambiente futuro desejado. Alavancar os módulos e componentes da arquitetura corporativa, incluindo serviços prestados externamente e capacidades relacionadas, para permitir uma resposta ágil, confiável e eficiente aos objetivos estratégicos.</p>	
<b>Declaração de Propósito do Processo</b> <p>Alinhar os planos estratégicos de TI com os objetivos corporativos. Comunicar claramente os objetivos e obrigações de prestar contas relacionadas para que eles sejam compreendidos por todos, estando as opções estratégicas de TI identificadas, estruturadas e integradas com os planos de negócios.</p>	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de objetivos e requisitos estratégicos corporativos suportados por objetivos estratégicos de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio de programas e serviços planejado</li> <li>Percentual de direcionadores de valor de TI mapeados em função de direcionadores de valor de negócios</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de eventos disruptivos de negócios devido a incidentes em serviços de TI</li> <li>Percentual de partes interessadas da área de negócios satisfeitas que o serviço de TI prestado atende aos níveis de serviço definidos</li> <li>Percentual de usuários satisfeitos com a qualidade do serviço de TI prestado</li> </ul>
17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>Nível de consciência e entendimento dos executivos de negócios quanto às possibilidades de inovação de TI</li> <li>Nível de satisfação das partes interessadas com os níveis de expertise e ideias para inovação de TI</li> <li>Número de iniciativas aprovadas resultantes de ideias inovadoras de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Todos os aspectos da estratégia de TI estão alinhados com a estratégia corporativa.	<ul style="list-style-type: none"> <li>Percentual de objetivos na estratégia de TI que suportam a estratégia corporativa</li> <li>Percentual de objetivos corporativos endereçados na estratégia de TI</li> </ul>
02 A estratégia de TI é custo-efetiva, adequada, realista, realizável, focada na organização e balanceada.	<ul style="list-style-type: none"> <li>Percentual das iniciativas na estratégia de TI que são autofinanciáveis (benefícios financeiros acima dos custos)</li> <li>Tendências no ROI de iniciativas incluídas na estratégia de TI</li> <li>Nível da pesquisa de satisfação com partes interessadas da organização sobre a estratégia de TI</li> </ul>
03 Objetivos de curto prazo claros e concretos podem ser derivados e remetidos a iniciativas específicas de logo prazo e podem então ser traduzidos em planos operacionais.	<ul style="list-style-type: none"> <li>Percentual de projetos no portfólio de projetos de TI que podem ser remetidos diretamente à estratégia de TI</li> </ul>
04 TI é um direcionador de valor para a organização.	<ul style="list-style-type: none"> <li>Percentual de objetivos corporativos estratégicos obtidos como resultado de iniciativas estratégicas de TI</li> <li>Número de novas oportunidades corporativas percebidas por resultado direto de desenvolvimentos de TI</li> <li>Percentual de iniciativas/projetos de TI patrocinados por proprietários de negócios</li> </ul>
05 Há consciência da estratégia de TI e uma clara atribuição da obrigação de prestar de contas pela entrega.	<ul style="list-style-type: none"> <li>Realização de resultados mensuráveis da estratégia de TI como parte das metas de performance da equipe</li> <li>Frequência das atualizações no plano de comunicação da estratégia de TI</li> <li>Percentual de iniciativas estratégicas com obrigação de prestar de contas atribuída</li> </ul>

# COBIT® : HABILITANDO PROCESSOS

APO02 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escrítorio de Programas e Projetos (PMO)	Escrítorio de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Conformidade	Auditor	Diretor de TI (CIO)	Gerente de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>APO02.01</b> Compreender o direcionamento corporativo.	C C C A C C						C C		C			R	C R R				R R R								
<b>APO02.02</b> Analisa o ambiente, capacidade e desempenho atuais.	C C C R C C						C					C C A R R R	R	C C C C C C C C C C C C C C											
<b>APO02.03</b> Definir as capacidades de TI desejáveis.	A C C C I R	I				I	C	C			C C R C C C C C C C C C C C C C														
<b>APO02.04</b> Conduzir uma análise de falhas.		R R C					C				C R R A R R R R R R R R R R R C														
<b>APO02.05</b> Definir plano e roteiro estratégicos.	C I C C C		C	R	C		C C				C C A C C C C C C C C C C C C C C														
<b>APO02.06</b> Comunicar a estratégia e o direcionamento de TI.	I R I I R I A I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO02 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO02.01 Compreender o direcionamento corporativo.</b>  Considerar o ambiente corporativo e processos de negócios atuais, assim como a estratégia corporativa e objetivos futuros. Considerar também o ambiente externo da organização (direcionadores da indústria, regulamentações relevantes, bases para competição).	EDM04.01	• Princípios de orientação para alocação de recursos e capacidades	• Fontes e prioridades para mudanças	Interno
	APO04.02	• Oportunidades de inovação ligadas a direcionadores de negócio		
	Externo ao COBIT	• Análise corporativa de forças, fraquezas, oportunidades e ameaças (SWOT)		
Atividades				
01 Desenvolver e manter um entendimento da estratégia e objetivos corporativos, assim como do ambiente operacional e desafios corporativos atuais.				
02 Desenvolver e manter um entendimento do ambiente externo da organização.				
03 Identificar as principais partes interessadas e obter uma visão sobre suas necessidades.				
04 Identificar e analisar fontes de mudança na organização e em ambientes externos.				
05 Apurar prioridades para mudança estratégica.				
06 Entender a arquitetura corporativa atual e trabalhar com o processo de arquitetura corporativa para determinar qualquer potencial falha arquitetural.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO02 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO02.02 Analisar o ambiente, capacidade e desempenho atuais.</b> Analizar o desempenho atual da capacidade de negócios e da TI internamente, dos serviços externos de TI e desenvolver um entendimento da arquitetura corporativa em relação à TI. Identificar problemas sendo experimentados atualmente e desenvolver recomendações em áreas que poderiam se beneficiar das melhorias. Considerar diferenciais e opções do provedor de serviços, o impacto financeiro e potenciais custos e benefícios de usar serviços externos.	APO06.05	<ul style="list-style-type: none"> <li>Oportunidades de otimização de custos</li> </ul>	<ul style="list-style-type: none"> <li>Referência das capacidades atuais</li> </ul>	Interno
	APO08.05	<ul style="list-style-type: none"> <li>Definição de projetos de potencial melhoria</li> </ul>	<ul style="list-style-type: none"> <li>Falhas e riscos relacionados à capacidade atual</li> </ul>	APO12.01
	APO09.01	<ul style="list-style-type: none"> <li>Falhas identificadas em serviços de TI para o negócio</li> </ul>	<ul style="list-style-type: none"> <li>Análise de capacidade SWOT</li> </ul>	Interno
	APO09.04	<ul style="list-style-type: none"> <li>Planos de ação e remediations para melhoria</li> </ul>		
	APO12.01	<ul style="list-style-type: none"> <li>Questões e fatores de risco emergentes</li> </ul>		
	APO12.02	<ul style="list-style-type: none"> <li>Resultados das análises de risco</li> </ul>		
	APO12.03	<ul style="list-style-type: none"> <li>Perfil de risco agregado, incluindo o estado das ações de gerenciamento de risco</li> </ul>		
	APO12.05	<ul style="list-style-type: none"> <li>Propostas de projeto para reduzir o risco</li> </ul>		
	BAI04.03	<ul style="list-style-type: none"> <li>Planos de capacidade e de desempenho</li> <li>Melhorias priorizadas</li> </ul>		
	BAI04.05	<ul style="list-style-type: none"> <li>Ações corretivas</li> </ul>		
<b>Atividades</b>	BAI09.01	<ul style="list-style-type: none"> <li>Resultados da revisão de adequação para a finalidade</li> </ul>		
	BAI09.04	<ul style="list-style-type: none"> <li>Oportunidades para reduzir custos dos ativos ou aumentar valor</li> <li>Resultados das revisões de otimização de custos</li> </ul>		

01 Desenvolver uma referência do ambiente, capacidades e serviços atuais de TI e de negócios contra a qual requerimentos futuros possam ser comparados. Incluir o detalhe de alto nível relevante da arquitetura corporativa atual (negócios, informações, dados, aplicações e domínios de tecnologia), processos de negócios, processos e procedimentos de TI, estrutura organizacional de TI, provisão de serviços externos, governança de TI e habilidades e competências relacionadas a TI em toda a organização.

02 Identificar riscos das tecnologias atuais, potenciais e em declínio.

03 Identificar falhas entre as capacidades e serviços atuais de TI e de negócios e padrões de referência e boas práticas, capacidades de negócios e de TI dos competidores e benchmarks comparativos de boas práticas e provisão de serviços de TI emergentes.

04 Identificar problemas, pontos fortes, oportunidades e ameaças no ambiente, capacidades e serviços atuais para entender o desempenho atual. Identificar áreas para melhoria em termos de contribuição da TI para os objetivos corporativos.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO02.03 Definir as capacidades de TI desejáveis</b> Definir as capacidades de TI e de negócios desejáveis e os serviços de TI necessários. Isto deve ser baseado no conhecimento do ambiente e requisitos corporativos; na análise dos atuais processos de negócio e ambiente e problemas de TI; e consideração das referências em padrões, boas práticas e tecnologias emergentes ou propostas de inovação validadas.	APO04.05	<ul style="list-style-type: none"> <li>Análise de iniciativas rejeitadas</li> <li>Resultados e recomendações de iniciativas de prova de conceito</li> </ul>	<ul style="list-style-type: none"> <li>Objetivos de alto nível relacionados a TI</li> </ul>	Interno
			<ul style="list-style-type: none"> <li>Capacidades requeridas de negócios e de TI</li> </ul>	Interno
			<ul style="list-style-type: none"> <li>Mudanças na arquitetura corporativa propostas</li> </ul>	APO03.03



## : HABILITANDO PROCESSOS

**APO02 Práticas de Processo, Entradas/Saídas e Atividades.**

Atividades				
01 Considerar tecnologias emergentes ou ideias inovadoras validadas.				
02 Identificar ameaças de tecnologias em declínio, atuais e adquiridas recentemente.				
03 Definir objetivos/metas de alto nível para TI e como elas contribuirão para os objetivos de negócio da organização.				
04 Definir as capacidades requeridas e desejadas para os processos de negócios e de TI e para os serviços de TI e descrever as alterações da arquitetura corporativa em alto nível (negócios, informações, dados, aplicações e domínios de tecnologia), processos e procedimentos de negócios e de TI, a estrutura da organização de TI, provedores de serviço de TI, governança de TI e habilidades e competências de TI.				
05 Alinhar e combinar com o arquiteto corporativo as alterações propostas na arquitetura corporativa.				
06 Demonstrar rastreabilidade para a estratégia e requisitos corporativos.				

**Prática de Gestão****Entradas****Saídas**

Prática de Gestão	De	Descrição	Descrição	Para
<b>APO02.04 Conduzir uma análise de falhas.</b> Identificar falhas entre os ambientes atual e desejável e considerar o alinhamento dos ativos (as capacidades que suportam serviços) com os resultados de negócios para otimizar o investimento e a utilização da base de ativos interna e externa. Considerar os fatores críticos de sucesso para suportar a execução da estratégia.	EDM02.01	<ul style="list-style-type: none"> <li>Avaliação do alinhamento estratégico</li> </ul>	<ul style="list-style-type: none"> <li>Falhas e mudanças necessárias para realizar a capacidade desejada</li> </ul>	EDM04.01 APO13.02 BAI03.11  BAI03.11
	APO04.06	<ul style="list-style-type: none"> <li>Análise do uso de abordagens inovadoras</li> </ul>		
	APO05.02	<ul style="list-style-type: none"> <li>Expectativas de retorno dos investimentos</li> </ul>		
	BAI01.05	<ul style="list-style-type: none"> <li>Resultados do monitoramento do programa de realização de objetivos</li> </ul>		
	BAI01.06	<ul style="list-style-type: none"> <li>Resultados da revisão stage-gate</li> </ul>		
	BAI01.13	<ul style="list-style-type: none"> <li>Resultados da Revisão pós implementação</li> </ul>		

**Atividades**

01 Identificar todas as falhas e mudanças necessárias para realizar o ambiente desejado.
02 Considerar as implicações de alto nível de todos as falhas. Considerar o valor de potenciais mudanças para as capacidades de negócios e TI, serviços de TI e arquitetura corporativa e as implicações se nenhuma mudança for realizada.
03 Analisar o impacto de potenciais mudanças nos modelos operacionais de negócios e de TI, capacidades de pesquisa e desenvolvimento de TI e programas de investimento de TI.
04 Refinar a definição do ambiente desejado e preparar uma declaração de valor com os benefícios do ambiente desejado.

**Prática de Gestão****Entradas****Saídas**

Prática de Gestão	De	Descrição	Descrição	Para
<b>APO02.05 Definir plano e roteiro estratégicos.</b> Criar um plano estratégico que defina, em conjunto com as partes interessadas relevantes, como os objetivos relacionados a TI contribuirão com os objetivos estratégicos da organização. Abranger como TI suportará os programas de investimento, processos de negócios, serviços de TI e ativos de TI habilitados por TI. Orientar TI para definir as iniciativas necessárias para corrigir as falhas, a estratégia de terceirização e as medições que serão utilizadas para monitorar a realização de objetivos, e então priorizar as iniciativas e combina-las em um roteiro de alto nível.	EDM04.01	<ul style="list-style-type: none"> <li>Plano de recursos aprovado</li> </ul>	<ul style="list-style-type: none"> <li>Definição das iniciativas estratégicas</li> </ul>	APO05.01  APO05.01 APO12.01  EDM02.01 APO01.03 APO03.01 APO05.01 APO08.01
	EDM04.03	<ul style="list-style-type: none"> <li>Feedback sobre a alocação e eficácia dos recursos e capacidades</li> <li>Ações de remediação para endereçar desvios no gerenciamento de recursos</li> </ul>	<ul style="list-style-type: none"> <li>Iniciativas de análise de risco</li> </ul>	
	APO03.01	<ul style="list-style-type: none"> <li>Escopo de arquitetura definido</li> <li>Estudo de caso e proposição de valor do conceito de arquitetura</li> </ul>	<ul style="list-style-type: none"> <li>Roteiro estratégico</li> </ul>	
	APO03.02	<ul style="list-style-type: none"> <li>Modelo de arquitetura da informação</li> </ul>		
	APO03.03	<ul style="list-style-type: none"> <li>Arquiteturas de transição</li> <li>Estratégias de alto nível de implementação e migração</li> </ul>		
	APO05.01	<ul style="list-style-type: none"> <li>Feedback sobre estratégia</li> </ul>		

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO02 Práticas de Processo, Entradas/Saídas e Atividades.

		e objetivos		
APO05.02		• Opções de financiamento		
APO06.02		• Alocações de orçamento		
APO06.03		• Orçamento e plano de TI • Comunicações de orçamento		
APO13.02		• Estudos de caso de segurança da informação		
BAI09.05		• Plano de ação para ajustar números e alocações de licenças		
DSS04.02		• Opções estratégicas aprovadas		

## Atividades

- 01 Definir as iniciativas necessárias para corrigir falhas e migrar do ambiente atual para o desejado, incluindo orçamento de investimento/operacional, fontes de financiamento, estratégia de terceirização e estratégia de aquisição.
- 02 Identificar e endereçar adequadamente o risco, custos e implicações de mudanças organizacionais, evolução tecnológica, requerimentos regulatórios, reengenharia de processos, alocação de pessoal, oportunidades de internalização e terceirização, etc., no processo de planejamento.
- 03 Determinar dependências, sobreposições, sinergias e impactos entre iniciativas e priorizar as iniciativas.
- 04 Identificar requisitos de recursos, cronograma e orçamento de investimento/operacional para cada uma das iniciativas.
- 05 Criar um roteiro indicando a programação relativa e interdependências das iniciativas.
- 06 Traduzir os objetivos em medidas de resultado representadas por métricas (o quê) e objetivos (quanto) que podem ser relacionados com benefícios corporativos.
- 07 Obter suporte formal das partes interessadas e obter aprovação para o plano.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
APO02.06 Comunicar a estratégia e o direcionamento de TI. Criar consciência e compreensão dos objetivos e direcionamento de negócios e de TI, conforme assimilado na estratégia de TI, por meio da comunicação com as partes interessadas e usuários apropriados em toda a organização.	EDM04.02	Comunicação das estratégias de disponibilização de recursos	Plano de comunicação Pacote de comunicação	Interno Todos APO Todos BAI Todos DSS Todos MEA

## Atividades

- 01 Desenvolver e manter uma rede para endossar, apoiar e conduzir a estratégia de TI.
- 03 Desenvolver um plano de comunicação abrangendo as mensagens, público alvo, mecanismos/canais de comunicação e cronogramas requeridos.
- 03 Preparar um pacote de comunicação que entregue o plano efetivamente utilizando mídias e tecnologia disponíveis.
- 04 Obter feedback e atualizar o plano de comunicação e entregar conforme requerido.

## APO02 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	4.0 Planejamento e implementação do gerenciamento de serviço 5.0 Planejamento e implementação de serviços novos ou modificados
ITIL V3 2011	Estratégia de Serviço, 4.1 Gerenciamento da Estratégia para Serviços de TI

# COBIT® : HABILITANDO PROCESSOS

AP003 Gerenciar a Arquitetura Corporativa

Área: Gestão

Dominio: Alinhar, Planejar e Organizar

**Descrição do Processo**

Estabelecer uma arquitetura comum que consista de camadas de processos de negócio, informação, dados, aplicação e tecnologia para de forma eficiente e eficaz realizar as estratégias de TI e negócio por meio da criação de modelos e práticas chave que descrevam as arquiteturas básicas e desejadas. Definir requisitos para taxonomia, padrões, diretrizes procedimentos, modelos e ferramentas, e fornecer um relacionamento entre estes componentes. Aprimorar o alinhamento, aumentar a agilidade, aprimorar a qualidade da informação e gerar potenciais reduções de custos por meio de iniciativas tais como o reuso de componentes.

**Declaração de Propósito do Processo**

Representar os diferentes blocos que compõe a empresa e seus inter-relacionamentos bem como os princípios que guiam o seu desenho e evolução ao longo do tempo, permitindo uma entrega padronizada, responsável e eficiente dos objetivos estratégicos e operacionais.

**O processo suporta a realização de um conjunto primário de objetivos de TI:**

Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de objetivos e requisitos estratégicos de negócio suportados por objetivos estratégicos de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfolio planejado de programas e serviços</li> <li>Percentual de direcionadores de valor de TI mapeados com os direcionadores de valor de negócio</li> </ul>
09 Agilidade de TI	<ul style="list-style-type: none"> <li>Nível de satisfação dos executivos de negócio com a capacidade de resposta de TI para novos requisitos</li> <li>Número de processos críticos de negócio suportados por infraestrutura e aplicações atualizadas</li> <li>Tempo médio para traduzir objetivos estratégicos de TI em iniciativas acordadas e aprovadas</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência de avaliações sobre otimização de custos e maturidade das capacidades</li> <li>Tendência de resultados das avaliações</li> <li>Níveis de satisfação dos executivos de negócio e TI com os custos e capacidades de TI relacionadas</li> </ul>

**Objetivos e Métricas do Processo**

Objetivo do Processo	Métricas Relacionadas
01 A arquitetura e os padrões são efetivos no suporte à empresa	<ul style="list-style-type: none"> <li>Número de exceções aplicadas e concedidas nos padrões e bases da arquitetura</li> <li>Nível de feedback dos clientes de arquitetura</li> <li>Benefícios de projetos realizados e que podem ser relacionados com o envolvimento da arquitetura (ex. redução de custos por meio de reuso)</li> </ul>
2.Um portfolio de serviços de arquitetura empresarial suporta mudanças ágeis na empresa	<ul style="list-style-type: none"> <li>Percentual de projetos usando serviços de arquitetura corporativa</li> <li>Nível de feedback dos clientes de arquitetura</li> </ul>
3.Arquiteturas apropriadas e atualizadas de domínio e/ou federadas existem para prover informações confiáveis de arquitetura	<ul style="list-style-type: none"> <li>Data da última atualização das arquiteturas de domínio e/ou federadas</li> <li>Número de lacunas identificadas em modelos nos diversos domínios de arquitetura corporativa, como informação, dados, aplicação e tecnologia</li> <li>Nível de feedback dos clientes de arquitetura com relação à informação fornecida</li> </ul>
04 Uma estrutura comum e uma metodologia de arquitetura corporativa, bem como um repositório integrado de arquiteturas são usados para gerar eficiência com reuso por toda a empresa.	<ul style="list-style-type: none"> <li>Percentual de projetos que utilizam a estrutura e metodologia para reuso de componentes definidos</li> <li>Número de pessoas treinadas na metodologia e conjunto de ferramentas</li> <li>Número de exceções aplicadas e concedidas nos padrões e bases da arquitetura</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO03 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
APO03.01 Desenvolver a visão da arquitetura corporativa	A C C R C R								C R C C C C	C R R C C C												C				
Definir a arquitetura de referência	C C C R C R								C A C C C C	R R C C C C												C				
Selecionar oportunidades e soluções	A C C R C R								C R C C C C	C R R C C C												C				
Definir a implementação da arquitetura	A C R C C R								C R C C C C	C R R C C C												C				
Fornecer serviços de arquitetura corporativa	A C R C C R								C R C C C C	C R R C C C												C				

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO03 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO03.01 Desenvolver a visão da arquitetura corporativa</b>  A visão da arquitetura fornece uma descrição preliminar e de alto-nível das arquiteturas básica e desejada, cobrindo os domínios de negócio, informações, dados, aplicativos e tecnologias. A visão da arquitetura proporciona ao patrocinador com uma ferramenta chave para apresentar os benefícios das capacidades propostas para as partes interessadas da Organização. Adicionalmente, a visão da arquitetura descreve como as novas capacidades vão atender aos Objetivos Corporativos bem como seus objetivos estratégicos, e endereçar as preocupações das partes interessadas quando implementada.	EDM04.01	• Princípios orientadores para arquitetura corporativa	• Escopo da arquitetura definido	APO02.05
	APO02.05	• Roadmap estratégico	• Princípios da arquitetura	BAI02.01 BAI03.01 BAI03.02
	Referência externa ao COBIT	• Estratégia corporativa	• Business case conceitual e proposição de valor da arquitetura	APO02.05 APO05.03
Atividades				
01 Identificar as principais partes interessadas e suas preocupações/objetivos, e definir os principais requisitos corporativos a serem endereçados bem como as visões de arquitetura a serem desenvolvidas para satisfazer os diversos requisitos das partes interessadas.				
02 Identificar os Objetivos Corporativos e direcionadores estratégicos da organização e definir as restrições que devem ser tratadas, incluindo restrições em nível corporativo e restrições específicas de projeto (tempo, cronograma, recursos, etc.).				
03 Alinhar objetivos de arquitetura com as prioridades de programas estratégicos.				
04 Entender as capacidades e desejos do negócio, e então identificar as opções para realizar estas capacidades.				
05 Avaliar a preparação da empresa para mudanças.				
06 Definir o que está dentro e o que está fora do escopo da arquitetura básica e esforços da arquitetura desejada, entendendo que não há necessidade de descrevê-las no mesmo nível de detalhe.				
07 Confirmar e elaborar os princípios da arquitetura, incluindo princípios corporativos. Certificar que quaisquer definições existentes sejam atuais e esclarecer quaisquer áreas de ambiguidade.				

# COBIT<sup>®</sup> : HABILITANDO PROCESSOS

## APO03 Práticas de Processo, Entradas/Saídas e Atividades.

- 08 Entender as atuais metas e objetivos estratégicos corporativos e trabalhar com o processo de planejamento estratégico para garantir que oportunidades de arquitetura corporativa relacionadas a TI sejam alavancadas no desenvolvimento do plano estratégico.
- 09 Com base nas preocupações das partes interessadas, requisites de capacidade de negócio, escopo, restrições e princípios, criar a visão de arquitetura: uma visão de alto nível das arquiteturas básica e desejada.
- 10 Definir as proposições de valor, metas e métricas da arquitetura desejada.
- 11 Identificar os riscos de mudança corporativa associados com a visão de arquitetura, avaliar o nível iniciar de risco (ex. crítico, marginal ou desprezível), e desenvolver uma estratégia de mitigação para cada risco significativo.
- 12 Desenvolver um business case conceitual para a arquitetura corporativa, esboço dos planos e declaração do trabalho de arquitetura, e assegurar a aprovação para iniciar o projeto alinhado e integrado com a estratégia corporativa.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO03.02 Definir a arquitetura de referência</b> A arquitetura de referência descreve a arquitetura atual e a desejada para os domínios de negócio, informações, dados, aplicações e tecnologias.	APO01.01	<ul style="list-style-type: none"> <li>• Diretrizes operacionais corporativas</li> <li>• Definição da estrutura organizacional e funções</li> </ul>	<ul style="list-style-type: none"> <li>• Descrições dos domínios básicos e definição da arquitetura</li> </ul>	APO13.02 BAI02.01 BAI03.01 BAI03.02
	APO01.05	<ul style="list-style-type: none"> <li>• Definição do posicionamento operacional da função de TI</li> <li>• Avaliação das opções para a organização de TI</li> </ul>	<ul style="list-style-type: none"> <li>• Modelo de processo de arquitetura</li> </ul>	APO01.01
	APO01.06	<ul style="list-style-type: none"> <li>• Diretrizes para classificação de dados</li> </ul>	<ul style="list-style-type: none"> <li>• Modelo de arquitetura da informação</li> </ul>	APO02.05 BAI02.01 BAI03.02 DSS05.03 DSS05.04 DSS05.06
	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>• Estratégia corporativa</li> </ul>		

## Atividades

- 01 Manter um repositório de arquitetura contendo padrões, componentes reutilizáveis, artefatos de modelagem, relacionamentos, dependências e visões para permitir uniformidade na organização arquitetural e manutenção.
- 02 Selecionar pontos de vista de referência do repositório de arquitetura que permitirão ao arquiteto demonstrar como as preocupações das partes interessadas estão sendo endereçadas na arquitetura.
- 03 Para cada ponto de vista, selecionar modelos necessários para suportar a visão específica requerida, usando ferramentas ou métodos selecionados, e nível apropriado de decomposição.
- 04 Desenvolver descrições dos domínios da arquitetura básica, usando o escopo e nível de detalhe necessário para suportar a arquitetura desejada e, até onde possível, identificando os blocos de construção da arquitetura relevantes a partir do repositório.
- 05 Manter um modelo de processo de arquitetura como parte das descrições de domínio básicas e desejadas. Padronizar as descrições e documentação dos processos. Definir os papéis e responsabilidades dos tomadores de decisão do processo, donos do processo, usuários do processo, time do processo e outras partes interessadas que precisem ser envolvidas.
- 06 Manter um modelo de arquitetura de informação como parte das descrições de domínio básicas e desejadas, consistente com a estratégia corporativa, permitindo um uso otimizado da informação para tomada de decisões. Manter um dicionário de dados corporativo para promover um entendimento comum e um esquema de classificação que inclua detalhes sobre propriedade de dados, definição de níveis apropriados de segurança, e requisitos de retenção e destruição de dados.
- 07 Verificar os modelos de arquitetura para consistência e precisão internas, e realizar uma análise de lacunas entre situação básica e desejada. Priorizar as lacunas e definir componentes novos ou modificados que devem ser desenvolvidos para arquitetura desejada. Resolver potenciais impactos tais como incompatibilidades, inconsistências ou conflitos dentro da arquitetura visionada.
- 08 Conduzir uma revisão formal de partes interessadas por meio da checagem de arquitetura proposta em relação à motivação original para o projeto de arquitetura, e a declaração do trabalho de arquitetura.
- 09 Finalizar os domínios de arquitetura de negócio, informação, dados, aplicações e tecnologia, e criar um documento de definição da arquitetura.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO03.03 Selecionar oportunidades e soluções</b> Racionalizar as lacunas entre a arquitetura base e a desejada, levando em consideração tanto as perspectivas técnicas quanto de negócio, e agrupa-las de maneira lógica em pacotes de trabalho nos projetos. Integrar o projeto com programas de investimento de TI para garantir que as iniciativas de	APO02.03	<ul style="list-style-type: none"> <li>• Mudanças propostas na arquitetura corporativa</li> </ul>	<ul style="list-style-type: none"> <li>• Estratégia de alto nível de implementação e migração</li> </ul>	APO02.05
	Referência externa ao	<ul style="list-style-type: none"> <li>• Estratégias corporativas</li> <li>• Direcionadores</li> </ul>	<ul style="list-style-type: none"> <li>• Arquiteturas de transição</li> </ul>	APO02.05

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Alinhar, Planejar e Organizar

**APO03 Práticas de Processo, Entradas/Saídas e Atividades.**

arquitetura estejam alinhadas e fazer com que estas iniciativas sejam parte das mudanças gerais na empresa. Fazer deste processo em um esforço colaborativo com as principais partes interessadas de negócio e TI para avaliar a preparação para a transformação organizacional, e identificar oportunidades, soluções e todas as variáveis de implementação.	COBIT	corporativos	
---	-------	--------------	--

**Atividades**

- 01 Determinar e confirmar os principais atributos de mudança organizacional, incluindo a cultura organizacional e como esta impactará a implementação da arquitetura corporativa, bem como as capacidades de transição da empresa.
- 02 Identificar quaisquer direcionadores corporativos que possam restringir a sequência de implementação, incluindo a revisão dos planos estratégicos e de negócio, e consideração da maturidade atual da arquitetura corporativa.
- 03 Revisar e consolidar os resultados da análise de lacunas entre as arquiteturas básica e desejada, e avaliar suas implicações em relação às potenciais soluções/oportunidades, interdependências e alinhamento com os atuais programas de TI.
- 04 Avaliar os requisites, lacunas, soluções e fatores para identificar um conjunto mínimo de requisitos funcionais cujas integrações em pacotes de trabalho levariam a uma implementação mais eficiente e efetiva da arquitetura desejada.
- 05 Reconciliar os requisites consolidados com soluções potenciais.
- 06 Refinar as dependências iniciais, garantindo que quaisquer restrições no plano de implementação e migração sejam identificadas, e consolida-las em um relatório de análise de dependências.
- 07 Confirmar a preparação da organização para transformação, e o riscos associados a ela.
- 08 Formular uma estratégia alto nível de implementação e migração que guiará a implementação da arquitetura desejada, e estruturar as arquiteturas de transição alinhadas com os objetivos estratégicos da organização e os cronogramas associados.
- 09 Identificar e agrupar pacotes de trabalho em um conjunto coerente de programas e projetos, respeitando o direcionamento e a abordagem estratégica de implementação.
- 10 Desenvolver uma série de arquiteturas de transição quando necessário onde o escopo de mudança requerido para realizar a arquitetura desejada requeira uma abordagem incremental.

<b>Prática de Gestão</b>	<b>Entradas</b>		<b>Saídas</b>	
	<b>De</b>	<b>Descrição</b>	<b>Descrição</b>	<b>Para</b>
<b>APO03.04 Definir a implementação da arquitetura</b> Criar um plano de implementação e migração viável alinhado com os portfólios de programas e projetos. Certificar-se de que o plano seja coordenado de perto para garantir que o valor seja entregue e que os recursos requeridos estejam disponíveis para completar o trabalho necessário.			<ul style="list-style-type: none"> <li>• Requisitos de recursos BAIO1.02</li> <li>• Descrições de fases de implementação BAIO1.01 BAIO1.02</li> <li>• Requisitos de governança de arquitetura BAIO1.01</li> </ul>	

**Atividades**

- 01 Estabelecer o que o plano de implementação e migração deve incluir como parte do planejamento do programa e projeto, e garantir que esteja alinhado com os requisitos dos tomadores de decisão aplicáveis.
- 02 Confirmar incrementos e fases transitórias de arquitetura e atualizar o documento de definição de arquitetura.
- 03 Definir os requisitos de governança na implementação de arquitetura.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO03 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO03.05 Fornecer serviços de arquitetura corporativa</b> O fornecimento de serviços de arquitetura corporativa dentro da empresa inclui orientação e monitoramento na implementação de projetos, formalizando meios de se trabalhar por meio de contratos de arquitetura, e mensuração e comunicação do valor agregado da arquitetura e monitoramento de conformidade.			<ul style="list-style-type: none"> <li>Orientação para desenvolvimento de soluções</li> </ul>	BAI02.01 BAI02.02 BAI03.02
<b>Atividades</b>				
01 Confirmar o escopo e prioridades e fornecer direcionamento para desenvolvimento e implantação de soluções				
02 Gerenciar o portfólio de serviços de arquitetura corporativa para garantir o alinhamento com objetivos estratégicos e desenvolvimento de soluções				
03 Gerenciar os requisitos de arquitetura corporativa e suporte com princípios arquitetônicos, modelos e blocos de construção				
04 Identificar e alinhar as prioridades da arquitetura corporativa com os direcionadores de valor. Definir e coletar métricas de valor e medir e comunicar os valores da arquitetura corporativa.				
05 Estabelecer um fórum de tecnologia para fornecer diretrizes de arquitetura, aconselhamento em projetos e orientação na seleção de tecnologias. Mensurar a conformidade com estes padrões e diretrizes, incluindo conformidade com requisitos externos e sua relevância para o negócio.				

## APO03 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
TOGAF 9	No núcleo do TOGAF está o Método de Desenvolvimento de Arquitetura (ADM), que faz o mapeamento com as práticas do COBIT 5 de desenvolvimento da visão da arquitetura (ADM Fase A), definição das arquiteturas de referência (ADM Fases B, C, D), seleção de oportunidades e soluções (ADM Fase E), e definição de implementação da arquitetura (ADM Fases F, G). Um número de componentes do TOGAF é mapeado com a prática do COBIT 5 de fornecimento de serviços de arquitetura. Estes incluem Gestão de Requisitos, Princípios de Arquitetura, Gestão de Partes Interessadas, Avaliação da Preparação para Transformação de Negócio, Gestão de Riscos, Planejamento Baseado em Capacidade, Conformidade da Arquitetura e Contratos de Arquitetura.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO04 Gerenciar Inovação	Área: Gestão Domínio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b> Manter a conscientização sobre tendências em tecnologia e serviços relacionados, identificar oportunidades de inovação, e planejar como obter benefícios destas inovações em relação ao negócio. Analisar quais oportunidades para a inovação ou melhorias podem ser criadas a partir de tecnologias emergentes, inovações nos serviços ou processos de TI, bem como por meio de tecnologias estabelecidas existentes, e por inovação nos processos de negócio.	
<b>Declaração de Propósito do Processo</b> Alcançar vantagens competitivas, inovação de negócios, e eficiência e eficácia operacional aprimorada, por meio da exploração de desenvolvimentos em tecnologia da informação.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	<ul style="list-style-type: none"> <li>Percentual de investimentos relacionados à TI onde a realização de benefícios é monitorada durante todo seu ciclo de vida econômico</li> <li>Percentual de serviços de TI onde os benefícios esperados são realizados</li> <li>Percentual de investimentos relacionados à TI onde os benefícios planejados são atingidos ou superados</li> </ul>
08 Uso adequado de aplicativos, informações e soluções tecnológicas	<ul style="list-style-type: none"> <li>Percentual de donos dos processos de negócio satisfeitos com os produtos e serviços de TI que os suportam</li> <li>Nível de entendimento dos usuários de negócio sobre como as soluções tecnológicas suportam seus processos</li> <li>Nível de satisfação dos usuários de negócio com treinamento e manuais de usuários</li> <li>Valor presente líquido (NPV) mostrando o nível de satisfação do negócio com a qualidade e utilidade das soluções tecnológicas</li> </ul>
09 Agilidade de TI	<ul style="list-style-type: none"> <li>Nível de satisfação dos executivos de negócio com o tempo de resposta de TI sobre novos requisitos.</li> <li>Número de processos críticos de negócio suportado por aplicações e infraestrutura atualizadas.</li> <li>Tempo médio para traduzir objetivos estratégicos de TI em iniciativas acordadas e aprovadas</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência de avaliações de maturidade e de otimização de custos</li> <li>Tendências nos resultados das avaliações</li> <li>Níveis de satisfação dos executivos de TI e negócios com os custos e capacidades relacionadas à TI</li> </ul>
17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>Nível de conscientização e entendimento dos executivos de negócio com as possibilidades de inovação de TI</li> <li>Nível de satisfação das partes interessadas com o nível de especialização e ideias relacionadas com inovação de TI</li> <li>Número de iniciativas aprovadas resultante de ideias inovadoras</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Valor ao negócio é criado por meio de qualificação e seleção dos mais apropriados avanços e inovações em tecnologia, métodos e soluções de TI	<ul style="list-style-type: none"> <li>Aumento em participação de mercado ou competitividade por meio de inovações</li> <li>Percepção e feedback das partes interessadas da empresa sobre inovação de TI</li> </ul>
02 Objetivos corporativos são alcançados com benefícios qualitativos aprimorados e/ou redução de custos como resultado da identificação e implementação de soluções inovadoras	<ul style="list-style-type: none"> <li>Percentual de iniciativas implementadas que realizam os benefícios esperados</li> <li>Percentual de iniciativas implementadas com claro relacionamento a um objetivo corporativo</li> </ul>
03 Inovação é promovida e proporcionada, e é parte da cultura da empresa	<ul style="list-style-type: none"> <li>Inclusão de objetivos relacionados à inovação ou tecnologias emergentes nas metas de desempenho das equipes</li> <li>Feedback de partes interessadas e pesquisas</li> </ul>

# COBIT® : HABILITANDO PROCESSOS

APO04 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Conselho de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
APO04.01 Criar um ambiente favorável à inovação	<b>A</b>		<b>R</b>	<b>R</b>	<b>R</b>									<b>R</b>				<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>		
APO04.02 Manter um entendimento sobre o ambiente corporativo		<b>A</b>	<b>R</b>	<b>R</b>	<b>C</b>													<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>					
APO04.03 Monitorar e analisar o ambiente de tecnologia																			<b>A</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	
APO04.04 Avaliar o potencial de tecnologias emergentes e ideias inovadoras	I	I	C	C	C				<b>C</b>									<b>A</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>		
APO04.05 Recomendar ações adicionais futuras			I	R	R	A						<b>C</b>						<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>		
APO04.06 Monitorar a implementação e o uso da inovação				<b>C</b>	<b>C</b>	<b>A</b>					<b>C</b>				<b>C</b>			<b>R</b>	<b>C</b>	<b>C</b>	<b>C</b>	<b>C</b>	<b>C</b>	<b>C</b>		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO04 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO04.01 Criar um ambiente favorável à inovação</b> Criar um ambiente que propicie a inovação, levando em consideração questões como a cultura, premiação, colaboração, fóruns de tecnologia, e com mecanismos para promover e absorver ideias dos colaboradores			<ul style="list-style-type: none"> <li>• Plano de inovação</li> <li>• Programa de reconhecimento e premiação</li> </ul>	Interno APO07.04
<b>Atividades</b>				
01. Criar um plano de inovação que inclua o apetite a riscos, o orçamento reservado para gastos com iniciativas de inovação, e objetivos da inovação.				
02 Prover infraestrutura que possa ser um habilitador de inovação, como ferramentas de colaboração para aprimorar o trabalho entre localidades geográficas e divisões.				
03 Criar um ambiente que seja favorável à inovação por meio de iniciativas de RH relevantes, tais como programas de reconhecimento e premiação por inovação, apropriada rotação entre funções, e tempo discricionário para experimentação.				
04 Manter um programa que possibilite às equipes a submissão de ideias inovadoras e criar uma estrutura apropriada para tomada de decisões para avaliar estas ideias e leva-las adiante.				
05 Encorajar ideias inovadoras de clientes, fornecedores e parceiros de negócios.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	De
<b>APO04.02 Manter um entendimento sobre o ambiente corporativo</b> Trabalhar com as partes interessadas em TI para entender seus respectivos desafios. Manter um entendimento adequado sobre a estratégia corporativa, sobre o ambiente competitivo e outras restrições, de forma que oportunidades geradas por novas tecnologias possam ser identificadas.	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>• Estratégia corporativa e análise SWOT da empresa</li> </ul>	<ul style="list-style-type: none"> <li>• Oportunidade de inovação relacionadas com direcionadores de negócio</li> </ul>	APO02.01

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Alinhar, Planejar e Organizar

**APO04 Práticas de Processo, Entradas/Saídas e Atividades**

Atividades				
Prática de Gestão	Entradas		Saídas	
De	Descrição	Descrição	Para	
<b>APO04.03 Monitorar e analisar o ambiente de tecnologia</b> Realizar monitoramento sistemático e análise sobre o ambiente externo do Banco para identificar tecnologias emergentes que têm o potencial para a criação de valor (ex. realização da estratégia corporativa, otimização de custos, redução na obsolescência de equipamentos, e melhor implementação de processos de negócio e de TI). Monitorar o mercado, cenário competitivo, os setores industriais, tendências legais e regulatórias, de forma a analisar as tecnologias emergentes ou ideias inovadoras no contexto corporativo	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>Tecnologias emergentes</li> </ul>	<ul style="list-style-type: none"> <li>Análises das pesquisas sobre possibilidades de inovação</li> </ul>	BAI03.01
Atividades				
01 Entender o interesse e potencial da empresa para adoção de novas inovações tecnológicas e focar os esforços de conscientização nas tecnologias que trazem maior oportunidade.				
02 Realizar pesquisas e exploração do ambiente externo, incluindo sítios de internet apropriados, periódicos e conferências, para identificar tecnologias emergentes.				
03 Consultar especialistas terceirizados quando necessário para confirmar as descobertas das pesquisas ou como fonte de informação em tecnologias emergentes.				
04 Capturar ideias inovadoras dos membros das equipes de TI e analisá-las pelo potencial de implementação.				
Prática de Gestão	Entradas		Saídas	
De	Descrição	Descrição	Para	
<b>APO04.04 Avaliar o potencial de tecnologias emergentes e ideias inovadoras</b> Analisa tecnologias emergentes identificadas e/ou outras sugestões de inovação em TI. Trabalhar com as partes interessadas para validar premissas sobre o potencial de novas tecnologias e inovações.		<ul style="list-style-type: none"> <li>Avaliação de ideias inovadoras</li> <li>Escopo da prova de conceito e esboço do business case</li> <li>Resultados dos testes obtidos por meio das iniciativas de prova de conceito</li> </ul>	<ul style="list-style-type: none"> <li>BAI03.01</li> <li>APO05.03</li> <li>APO06.02</li> <li>Interno</li> </ul>	
Atividades				
01 Avaliar as tecnologias identificadas, avaliando aspectos como tempo para atingir a maturidade, risco inerente de novas tecnologias (incluindo potenciais implicações legais), aderência com a arquitetura corporativa, e potencial para fornecer valor adicional.				
02 Identificar eventuais questões que necessitem serem resolvidas ou comprovadas por meio de uma iniciativa de prova de conceito.				
03 Definir o escopo da iniciativa de prova de conceito, incluindo resultados desejados, orçamento necessário, cronograma e responsabilidades.				
04 Obter aprovação para conduzir a iniciativa de prova de conceito.				
05 Conduzir iniciativas de prova de conceito para testar tecnologias emergentes ou outras ideias inovadoras, identificar questões a serem resolvidas, e determinar se implementações adicionais devam ser consideradas com base na viabilidade e potencial retorno de investimento (ROI).				
Prática de Gestão	Entradas		Saídas	
De	Descrição	Descrição	Para	
<b>APO04.05 Recomendar ações adicionais futuras</b> Avaliar e monitorar os resultados das Provas de Conceito e, se favoráveis, gerar recomendações para ações adicionais, e obter apoio das partes interessadas.		<ul style="list-style-type: none"> <li>Resultados e recomendações geradas pelas iniciativas de provas de conceito</li> <li>Análise das iniciativas rejeitadas</li> </ul>	<ul style="list-style-type: none"> <li>APO02.03</li> <li>BAI03.09</li> <li>APO02.03</li> <li>BAI03.08</li> </ul>	

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO04 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
Prática de Gestão	Entradas	Saídas		
	De	Descrição	Descrição	Para
<b>APO04.06 Monitorar a implementação e o uso da inovação</b> Monitorar a implementação e uso de tecnologias emergentes e inovações durante sua integração e adoção, e por todo seu ciclo de vida econômico para garantir que os benefícios planejados sejam realizados, e para identificar lições aprendidas.		<ul style="list-style-type: none"> <li>• Avaliações sobre o uso de abordagens inovadoras</li> <li>• Avaliação dos benefícios da inovação</li> <li>• Planos de inovação ajustados</li> </ul>	APO02.04 BAI03.02 APO05.04	Interno
Atividades				
01 Avaliar a implementação de novas tecnologias ou inovações de TI adotadas como parte da estratégia de TI e desenvolvimentos da arquitetura corporativa, e sua realização a gestão de iniciativas do programa.				
02 Capturar lições aprendidas e oportunidades para aprimoramento.				
03 Ajustar o plano de inovação, se necessário.				
04 Identificar e avaliar o valor potencial a ser realizado por meio do uso de inovação.				

## APO04 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
Nenhum	

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Alinhar, Planejar e Organizar

APO05 Gerenciar Portfólio	Área: Gestão Dominio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b>	
Executar o direcionamento estratégico definido para os investimentos, em linha com a visão da arquitetura empresarial e as características desejadas para os portfólios de investimentos e serviços, e considerar as diferentes categorias de investimentos e limitações de recursos e fontes de financiamento. Avaliar, priorizar e manter o equilíbrio nos programas e serviços, gerenciando as demandas e considerando as restrições de recursos e fontes de financiamento, com base no seu alinhamento com os objetivos estratégicos, valor para a Organização e riscos. Movimentar os programas de investimentos selecionados para o portfólio de serviços ativo para execução. Monitorar o desempenho da carteira global de serviços e programas propondo os ajustes necessários de acordo com o desempenho dos mesmos ou se as prioridades corporativas forem alteradas/ajustadas.	
<b>Declaração de Propósito do Processo</b>	
Otimizar o desempenho do portfólio global de programas considerando o desempenho dos programas e dos serviços além de mudanças de prioridades e demandas da Organização.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de metas e requisitos estratégicos corporativos suportados por metas estratégicas de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio planejado de programas e serviços</li> <li>Percentual de direcionadores de valor de TI mapeados a direcionadores de valor de negócio</li> </ul>
05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	<ul style="list-style-type: none"> <li>Percentual de investimentos de TI onde a realização de benefícios é monitorada por todo seu ciclo de vida econômico</li> <li>Percentual de serviços de TI onde os benefícios esperados são realizados</li> <li>Percentual de investimento de TI onde os benefícios planejados são atingidos ou excedidos</li> </ul>
13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	<ul style="list-style-type: none"> <li>Número de programas/projetos dentro do cronograma e do orçamento planejado</li> <li>Percentual de partes interessadas satisfeitas com a qualidade do programa/projeto</li> <li>Número de programas com necessidade significativa de retrabalho devido a defeitos de qualidade</li> <li>Custo com manutenção de aplicações vs. custo geral de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Uma combinação apropriada de investimentos está definida e alinhada com a estratégia corporativa	<ul style="list-style-type: none"> <li>Percentual de investimentos de TI que possuem rastreabilidade com a estratégia corporativa</li> <li>Grau de satisfação dos gestores da empresa com a contribuição de TI na estratégia corporativa</li> </ul>
02 Fontes de investimento estão identificadas e disponíveis	<ul style="list-style-type: none"> <li>Relação entre os fundos alocados e os fundos usados</li> <li>Relação entre os fundos disponíveis e os fundos alocados</li> </ul>
03 Business cases dos programas são avaliados e priorizados antes dos fundos serem alocados	Percentual de unidades de negócios envolvidas no processo de avaliação e priorização
04 Uma visão abrangente e precisa do desempenho do portfolio de investimentos existe.	Nível de satisfação com os relatórios de monitoramento do portfolio
05 Mudanças no programa de investimentos são refletidas nos portfólios de serviços, recursos e ativos de TI	Percentual de mudanças provenientes do programa de investimentos e que foram refletidas no portfólio de TI
06 Benefícios são realizados por meio de monitoramento de benefícios	Percentual de investimentos nos quais os benefícios realizados foram mensurados e comparados com o business case

# COBIT® : HABILITANDO PROCESSOS

APO05 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Conselho de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
APO05.01 Estabelecer a combinação de investimentos desejada	A	R	R		C					I	C	C				C	C	C	C							
APO05.02 Determinar a disponibilidade e as fontes de investimentos	C	A		R					C								R									
APO05.03 Avaliar e selecionar os programas para investimento	C	A	R		R	R		R										R	C							
APO05.04 Monitorar, otimizar e reportar o desempenho do portfólio de investimentos	I	C	C	C	C	C	R		A							C	C	C	C					C		
APO05.05 Manter os portfólios		I	I	R	C	A	R										R	C	C	C						
APO05.06 Gerenciar o alcance aos benefícios	C	C	C	A	R	I	R	I								C	C	R	C					C		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO05 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas							
	De	Descrição	Descrição	Para						
APO05.01 Estabelecer a combinação de investimentos desejada  Revisar e garantir clareza nas estratégias de TI e de negócios, bem como nos atuais serviços fornecidos por TI. Definir uma combinação de investimentos apropriados com base no custo, no alinhamento com a estratégia e métricas financeiras, tais como custos e retorno sobre o investimento, grau de risco e o tipo de benefício para os programas existentes no portfólio. Ajustar as estratégias de TI e da Organização quando necessário	EDM02.02	• Tipos e critérios de Investimentos	• Mix de investimentos definido	Interno						
	APO02.05	• Roadmap estratégico • Iniciativas de gestão de risco • Definição de iniciativas estratégicas	• Recursos e capacidades identificadas para suportar a estratégia.	Interno						
	APO06.02	• Ranking e priorização das iniciativas de TI	• Feedback quanto a estratégia e objetivos	APO02.05						
	APO09.01	• Definição dos serviços padrão								
	BAI03.11	• Definições de serviços								
	Atividades									
01 Validar se os investimentos de TI e atuais serviços de TI estão alinhados com a visão corporativa, os princípios corporativos, metas e objetivos estratégicos, visão da arquitetura corporativa, e prioridades.										
02 Obter um entendimento comum entre TI e outras funções de negócio sobre potenciais oportunidades para TI direcionar e suportar a estratégia corporativa.										
03 Criar uma combinação de investimentos que alcancem o balanço correto entre um número de dimensões, incluindo um balanço apropriado entre retornos de curto e longo prazos, benefícios financeiros e não financeiros, e investimentos de alto e baixo risco.										
04 Identificar as categorias amplas de sistemas de informação, aplicações, dados, serviços de TI, infraestrutura, ativos de TI, recursos, habilidades, práticas, controles e relacionamentos necessários para suportar a estratégia corporativa.										
05 Definir um acordo sobre a estratégia e metas de TI, levando em consideração os inter-relacionamentos entre a estratégia corporativa e os serviços, ativos e outros recursos de TI. Identificar e alavancar sinergias que possam ser alcançadas.										

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO05 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
APO05.02 Determinar a disponibilidade e as fontes de investimentos Verificar potenciais fontes de investimentos, diferentes opções de financiamento e as implicações destas fontes nas expectativas de retorno da Organização			<ul style="list-style-type: none"> <li>• Opções de Financiamento</li> <li>• Expectativas de retorno de investimento</li> </ul>	APO02.05  EDM02.01 APO02.04 APO06.02 BAI01.06

## Atividades

- 01 Entender a atual disponibilidade e comprometimento de fundos, o atuais gastos aprovados, e o total gasto até o momento.  
 02 Identificar opções para obtenção de fundos adicionais para os investimentos de TI, seja internamente ou por meio de fontes externas.  
 03 Determinar as implicações das fontes de financiamento nas expectativas de retorno de investimento.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO05.03 Avaliar e selecionar os programas para investimento</b> Com base nos requisitos gerais para gestão do portfólio de investimentos, avaliar e priorizar os business cases dos programas e decidir sobre as propostas de investimento. Alocar recursos e iniciar esses programas.	EDM02.01	<ul style="list-style-type: none"> <li>• Avaliação dos portfólios de investimento e serviços</li> <li>• Avaliação do alinhamento estratégico</li> </ul>	<ul style="list-style-type: none"> <li>• Business case do programa</li> </ul>	APO06.02 BAI01.02
	EDM02.02	<ul style="list-style-type: none"> <li>• Tipos e critérios de investimento</li> </ul>	<ul style="list-style-type: none"> <li>• Avaliações sobre o business case</li> </ul>	APO06.02 BAI01.06
	APO03.01	<ul style="list-style-type: none"> <li>• Business case conceitual da arquitetura e proposição de valor</li> </ul>	<ul style="list-style-type: none"> <li>• Programas selecionados com os pontos de controle sobre o retorno de investimento (ROI)</li> </ul>	EDM02.01 BAI01.04
	APO04.04	<ul style="list-style-type: none"> <li>• Escopo da prova de conceito e esboço do business case</li> </ul>		
	APO06.02	<ul style="list-style-type: none"> <li>• Alocações de orçamento</li> </ul>		
	APO06.03	<ul style="list-style-type: none"> <li>• Comunicações sobre o orçamento</li> <li>• Plano e orçamento de TI</li> </ul>		
	APO09.01	<ul style="list-style-type: none"> <li>• Lacunas(Gaps) identificadas nos serviços de TI para o negócio</li> </ul>		
	APO09.03	<ul style="list-style-type: none"> <li>• Acordos de Nível de Serviço (SLAs)</li> </ul>		
	BAI01.02	<ul style="list-style-type: none"> <li>• Plano de realização dos benefícios do programa</li> <li>• Resumo e objetivo do programa</li> <li>• Business case conceitual do programa</li> </ul>		

## Atividades

- 01 Reconhecer oportunidades de investimento e classifica-las em linha com as categorias do portfólio de investimento. Especificar o(s) resultado(s) corporativo(s) esperado(s), todas as iniciativas requeridas para atingir aos resultados esperados, custos, dependências e riscos, e como estes indicadores serão mensuradas.  
 02 Realizar avaliações detalhadas sobre os business cases de todos os programas, avaliando o alinhamento estratégico, benefícios para a empresa, riscos e disponibilidade de recursos.  
 03 Avaliar o impacto no portfólio geral de investimentos com a adição de programas candidatos, incluindo quaisquer mudanças que possam ser necessárias em outros programas.  
 04 Decidir quais programas candidatos deverão ser movidos para o portfólio ativo de investimentos. Decidir se os programas rejeitados devem ser reservados para consideração no futuro ou alimentados com financiamento inicial para determinar se o business case pode ser aprimorado ou descartado.  
 05 Determinar os pontos de controle requeridos para o ciclo de vida econômico de cada um dos programas selecionados. Alocar e reservar o financiamento total por ponto de controle. Mover o programa para o portfólio ativo de investimentos.  
 06 Estabelecer procedimentos para comunicar os aspectos relacionados a custos, benefícios e riscos destes portfólios para os processos de priorização de orçamento, gestão de custos e gestão de benefícios.

# COBIT® : HABILITANDO PROCESSOS

## APO05 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO05.04 Monitorar, otimizar e reportar o desempenho do portfólio de investimentos</b> Monitorar e otimizar o desempenho do portfólio de investimentos, e de programas individuais de forma periódica por todo o ciclo de vida desses investimentos.	EDM02.01	• Avaliação do portfólio de investimentos e serviços	• Relatórios de desempenho sobre o desempenho do portfólio	EDM02.03
	EDM02.03	• Ações para aprimorar a entrega de valor • Feedback sobre o desempenho do portfólio e programa		APO09.04 BAI01.06 MEA01.03
	APO04.06	• Avaliação dos benefícios da inovação		
	BAI01.06	• Resultados das revisões realizadas nos pontos de controle		

### Atividades

02 Revisar periódica o portfólio para identificar e explorar sinergias, eliminar duplicação entre os programas, e identificar e mitigar riscos.
02 Quando mudanças ocorrerem, reavaliar e redefinir prioridades do portfólio para garantir que este esteja alinhado com a estratégia de negócios, e a combinação desejada de investimentos seja mantida de forma que o portfólio esteja otimizando o valor geral entregue. Esta ação pode requerer que programas sejam alterados, deferidos ou retirados, e novos programas sejam iniciados.
03 Ajustar os Objetivos Corporativos, previsões, orçamentos e, se necessário, o grau de monitoramento para refletir os gastos a serem incorridos e os benefícios corporativos a serem realizados pelos programas no portfólio ativo de investimentos. Incorporar gastos dos programas nos mecanismos de chargeback.
04 Fornecer uma visão precisa sobre o desempenho do portfólio de investimentos a todas as partes interessadas.
05 Fornecer relatórios de gestão para revisão dos executivos sêniores sobre o progresso da empresa em direção às metas identificadas, apontando o que ainda precisa ser gasto e alcançado de acordo com o cronograma.
06 Incluir no monitoramento periódico de desempenho informações sobre a extensão na qual os objetivos planejados foram alcançados, os riscos mitigados, as capacidades criadas, o entregáveis alcançados e as metas de desempenho atingidas.
07 Identificar desvios em: Controle orçamentário entre o realizado e o planejado Gestão de benefícios: Realizado vs planejado para investimentos em soluções, possivelmente expresso em termos de Retorno de Investimento (ROI), Valor Presente Líquido (NPV) ou Taxa Interna de Retorno (IRR) A tendência atual dos custos do portfólio de serviços para entrega das melhorias de produtividade nos serviços
08 Desenvolver métricas para mensuração da contribuição de TI para a empresa, e estabelecer metas apropriadas de desempenho refletindo as metas requeridas de capacidades de TI e corporativas. Usar orientação de especialistas externos e dados de benchmark para desenvolver métricas.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO05.05 Manter os portfólios</b> Manter os portfólios de programas e projetos de investimento, assim como de serviços e ativos de TI	BAI01.14	• Comunicação sobre a descontinuação do programa e responsabilidades contínuas	• Portfolio de programas, serviços e ativos atualizados	APO09.02 BAI01.01
	BAI03.11	• Portfolio de serviços atualizado		

### Atividades

01 Criar e manter portfólios de programas de investimento em TI, serviços de TI e ativos de TI, que formam a base para o orçamento atual de TI e suportam os planos estratégico e tático de TI.
02 Trabalhar com os gerentes de entrega de serviços para manter os portfólios de serviços, e com os gerentes de operações e arquitetos para manter os portfólios de ativos. Priorizar os portfólios para suportar as decisões de investimento.
03 Remover o programa do portfólio de investimentos ativos quando os benefícios desejados pela empresa tenham sido atingidos ou quando claramente os benefícios não serão atingidos dentro dos critérios de valor definidos no programa.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO05 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO05.06 Gerenciar o alcance aos benefícios</b> Monitorar os benefícios provenientes da prestação de serviços apropriados e manutenção de recursos de TI, utilizando como base business case acordado entre as partes envolvidas	BAI01.04	• Registro do orçamento e benefícios do programa	• Resultados dos benefícios e comunicações relacionadas	EDM02.01 APO09.04 BAI01.06
	BAI01.05	• Resultados do monitoramento sobre a realização dos benefícios	• Ações corretivas para aprimorar a realização dos benefícios	APO09.04 BAI01.06
<b>Atividades</b>				
<p>01 Usar a métricas acordadas e rastrear como os benefícios serão alcançados, como eles evoluem ao longo do ciclo de vida de programas e projetos, como eles estão sendo entregues pelos serviços de TI, e como eles se comparam com benchmarks internos e da indústria. Comunicar os resultados para as partes interessadas.</p> <p>02 Implementar ações corretivas quando os benefícios atingidos desviam significativamente dos benefícios esperados. Atualizar o business case para novas iniciativas e implementar processos de negócio e aprimoramentos de serviço quando requerido.</p> <p>03 Considerar a obtenção de orientação de especialistas externos, líderes de indústria e dados comparativos de benchmarking para testar e aprimorar as métricas e metas.</p>				

## APO05 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	3.1 Responsabilidade dos gestores Planejamento e implementação da gestão de serviços Planejamento e implementação de serviços novos ou alterados
ITIL V3 2011	Estratégia de Serviços, 4.2 Gestão do Portfólio de Serviços
Skills Framework for the Information Age (SFIA)	

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

APO06 Gerenciar Orçamento e Custos	Área: Gestão Domínio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b> Gerenciar as atividades financeiras relacionadas à tecnologia, tanto nas áreas de negócios quanto em TI, abrangendo orçamento, custos, investimentos, despesas e benefícios. Adicionalmente, realizar priorização dos gastos por meio do uso de práticas formais de orçamento, e de um sistema justo de alocação de custos. Consultar as partes interessadas para identificar, controlar os custos totais e benefícios no contexto dos planos estratégicos e táticos de TI, e iniciar ações corretivas quando necessário.	
<b>Declaração de Propósito do Processo</b> Adotar parceria entre TI e as partes interessadas da Organização para permitir o uso eficaz e eficiente dos recursos de TI, e permitir transparência e prestação de contas sobre custo e valor gerado pelas soluções e serviços ao negócio. Possibilitar à Organização a tomada de decisões utilizando informações reais e úteis sobre o uso de soluções e serviços de TI.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	<ul style="list-style-type: none"> <li>Percentual de investimentos de TI onde a realização de benefícios é monitorada por todo seu ciclo de vida econômico</li> <li>Percentual de serviços de TI onde os benefícios esperados são realizados</li> <li>Percentual de investimento de TI onde os benefícios planejados são atingidos ou excedidos</li> </ul>
06 Transparência dos custos, benefícios e riscos de TI	<ul style="list-style-type: none"> <li>Percentual de business cases de investimento com definição e aprovação clara dos custos e benefícios relacionados com TI</li> <li>Percentual de serviços de TI com custos operacionais e benefícios esperados claramente definidos e aprovados</li> <li>Pesquisa de Satisfação com principais partes interessadas com relação ao nível de transparência, entendimento e precisão das informações financeiras de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Um orçamento completo e transparente para TI reflete de forma precisa os gastos planejados	<ul style="list-style-type: none"> <li>Número de mudanças no orçamento devido a omissões e erros</li> <li>Número de desvios entre as categorias de orçamento planejadas e reais</li> </ul>
02 A alocação de recursos de TI para iniciativas de TI é priorizada com base nas necessidades da empresa	<ul style="list-style-type: none"> <li>Percentual de alinhamento dos recursos de TI com iniciativas altamente prioritárias</li> <li>Número de problemas de alocação de recursos escalados</li> </ul>
03 Os custos para os serviços são alocados de forma equitativa	<ul style="list-style-type: none"> <li>Percentual de custos gerais de TI que são alocados de acordo com os modelos de custos acordados</li> </ul>
04 Os orçamentos podem ser comparados de forma precisa com os custos reais	<ul style="list-style-type: none"> <li>Percentual de variação entre orçamentos, previsões e custos reais</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO06 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Dir. de Riscos (CRO)	Dir. de Segurança da Informação (CSO)	Conselho de Arquitetura	Conformidade	Auditor	Dir. de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade		
APO06.01 Gerenciar finanças e contabilidade		A	C	C					C	R				C	C					A	I	C	C	R	C	C
APO06.02 Priorizar a alocação de Recursos	I	R		C	C	C	I	C	C	I										A	I	C	C	R	C	C
APO06.03 Criar e manter orçamentos	I	A		C	C	C	C	C	C											R	C	C	C	R	C	C
APO06.04 Modelar e alocar custos		C		C	C	C	C	C	C										A	C	C	C	R	C	C	
APO06.05 Gerenciar custos		R		C	C	C	C	C	C										A	C	C	C	R	C	C	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO06 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO06.01 Gerenciar finanças e contabilidade</b> Estabelecer e manter um método para contabilizar todos os custos, investimentos e depreciações relacionados a TI, como parte integral do sistema financeiro corporativo e plano de contas, permitindo a gestão dos custos e investimentos de TI. Capturar e alocar os custos reais, analisar as variações entre as previsões e as realizações, e realizar o reporte utilizando os sistemas de acompanhamento financeiro da empresa.	BAI09.01	• Registro do ativo	<ul style="list-style-type: none"> <li>• Processos contábeis</li> <li>• Modelo de classificação dos custos de TI</li> <li>• Práticas de planejamento financeiro</li> </ul>	Interno Interno Interno
<b>Atividades</b>				
01 Definir processos, entradas e saídas, e responsabilidades em alinhamento com as políticas e abordagem corporativas de definição de orçamento e alocação de custos, para direcionar de forma sistemática o orçamento e os custos de TI; possibilitar uma estimativa dos custos e benefícios de TI justa, transparente, repetitiva e comparável para servir de insumo ao portfólio de programas de negócio habilitados por TI; e garantir que os orçamentos e custos sejam mantidos no portfólio de ativos e serviços de TI. 02 Definir um esquema de classificação para identificar todos os elementos de custos relacionados a TI, como eles são alocados entre os orçamentos e serviços, e como eles são capturados. 03 Usar informação financeira e do portfólio para fornecer insumos aos business cases para novos investimentos em ativos e serviços de TI. 04 Definir como analisar, reportar (a quem e como), e usar os processos de controle de orçamento e gestão de benefícios. 05 Estabelecer e manter práticas para planejamento financeiro, gestão de investimentos e tomada de decisões, e otimização de custos operacionais recorrentes para entregar o máximo de valor para a empresa ao mesmo tempo em que gera menores gastos.				

# COBIT® : HABILITANDO PROCESSOS

## APO06 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO06.02 Priorizar a Alocação de Recursos</b> Implementar um processo de tomada de decisões para priorizar a alocação de recursos, e estabelecer regras para a realização de investimentos arbitrários pelas unidades de negócios. Incluir o uso potencial de prestadores de serviços externos e considerar as opções de comprar, desenvolver internamente ou alugar recursos	EDM02.01	• Avaliação dos portfólios de investimentos e serviços	• Priorização e classificação de iniciativas de TI	APO05.01
	EDM02.03	• Ações para aprimorar a entrega de valor	• Alocações de orçamento	APO02.05
	APO04.04	• Escopo da prova de conceito e esboço do business case		APO05.03
	APO05.02	• Expectativas sobre o retorno de investimentos		APO07.05
	APO05.03	• Avaliações do business case • Business case do programa		BAI03.11

### Atividades

- 01 Estabelecer um órgão de decisão para a priorização de recursos de negócios e de TI, incluindo o uso de prestadores de serviços externos no âmbito de alocações orçamentárias de alto nível para os programas de ativação da TI, serviços de TI e ativos de TI, conforme estabelecido pelos planos estratégicos e táticos. Considere as opções para a compra ou o desenvolvimento de ativos capitalizados e serviços versus ativos utilizados externamente e serviços baseados em pagamento por utilização.
- 02 Classifique todas as iniciativas de TI baseando em casos de negócios e planos estratégicos e táticos, e em procedimentos estabelecidos para determinar as alocações orçamentárias e de corte. Estabelecer um procedimento para comunicar as decisões orçamentárias e revisar com os responsáveis pelo orçamento da unidade de negócios.
- 03 Identificar, comunicar e resolver impactos significativos das decisões orçamentárias sobre casos de negócios, carteiras e dos planos estratégicos (por exemplo, quando os orçamentos podem requerer a revisão devido a mudanças da situação econômica da empresa, quando elas não são suficientes para apoiar os objetivos estratégicos ou objetivos de negócios).
- 04 Obter a ratificação do comitê executivo para todas as mudanças do orçamento de TI que impactam negativamente nos planos estratégicos ou táticos da organização e oferecer ações para resolver os respectivos impactos.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 06.03 Criar e manter orçamentos.</b> Preparar um orçamento, que reflete as prioridades de investimento que apoiam os objetivos estratégicos, baseado no portfólio de TI, programas aprovados e serviços de TI.			• Orçamento de TI plano	APO02.05
			• Comunicações de orçamento	APO05.03 APO07.01 BAI03.11

### Atividades

- 01 Implementar um orçamento de TI formal, incluindo todos os programas aprovados, custos de TI, serviços de TI e ativos de TI direcionados pela estratégia, programas e portfólios.
- 02 Quando criar o orçamento, considere os seguintes componentes:  
 Alinhamento com o negócio  
 Alinhamento com a estratégia de suprimentos  
 Fontes autorizadas de financiamento  
 Custos de recursos internos, incluindo quadro de funcionários, ativos de informação e acomodações  
 Custos de terceiros, incluindo contratos de outsourcing, consultores e prestadores de serviço  
 Despesas de capital e operacional  
 Elementos de custos que dependem da carga de trabalho
- 03 Formalizar os motivos para justificar as contingências e revisá-los regularmente.
- 04 Processo de instruções, serviços e programas proprietários, bem como gerentes de projeto e de ativos, para planejamento de orçamentos.
- 05 Revisar os planos de orçamento e tomadas de decisões sobre as alocações de orçamento. Consolidar e ajustar o orçamento com base na evolução das necessidades da empresa e considerações financeiras.
- 06 Registrar, manter e comunicar o orçamento de TI atual, incluindo as despesas aprovadas, as despesas atuais, considerando projetos de TI registrados nos portfólios de investimento de TI, na operação e manutenção do portfólio dos ativos e serviços.
- 07 Monitorar a eficácia dos diferentes aspectos do orçamento e utilização dos resultados para implementar melhorias para garantir que os futuros orçamentos sejam mais precisos, confiáveis e de baixo custo.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO06 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 06.04 Modelo e alocação de custos.</b> Estabelecer e utilizar um modelo de custos de TI baseado na definição de serviço de custeio, garantindo que a alocação dos custos de serviços seja identificável, mensurável e previsível, para incentivar o uso responsável dos recursos incluindo os fornecidos pelos prestadores de serviços. Regularmente, revisar e aferir a adequação do modelo de custo/estorno para manter sua relevância e adequação à evolução das atividades de negócios e de TI.			<ul style="list-style-type: none"> <li>Custos de TI categorizados</li> <li>Modelo de alocação de custos</li> <li>Comunicações de alocação de custo</li> <li>Procedimentos operacionais</li> </ul>	Interno Interno Interno Interno
<b>Atividades</b>				

- 01 Categorizar todos os custos de TI de forma adequada, incluindo os custos relacionados aos prestadores de serviços, de acordo com as práticas de contabilidade de gestão empresarial.
- 02 Analisar os catálogos de serviços para identificar serviços que estão sujeitos a estorno do usuário e aqueles que são serviços compartilhados.
- 03 Definir e aprovar um modelo que:  
 Suporte o cálculo das taxas de estorno por serviço  
 Defina como os custos de TI serão calculados / cobrados  
 Seja caracterizada, onde e quando for o caso  
 Que está alinhado com o orçamento de TI
- 04 Criar um modelo de custo para ser transparente e suficiente e permitir que os usuários identifiquem a sua utilização e encargos efetivos, e para permitir uma melhor previsibilidade dos custos de TI e utilização eficiente e eficaz dos recursos de TI.
- 05 Após revisão com os usuários dos departamentos, obter aprovação e comunicar as entradas e saídas do modelo de custeio de TI para gestão de usuários dos departamentos.
- 06 Comunique as mudanças no modelo de custo/estorno com os donos dos processos corporativos.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 06.05 Gerenciar custos.</b> Implementar um processo de gestão de custos comparando os custos atuais com o orçamento. Os custos devem ser monitorizados e reportados e, no caso de desvios, o seu impacto, sobre os processos e serviços avaliados, deve ser identificado em tempo hábil.	EDM02.03	<ul style="list-style-type: none"> <li>Feedback sobre carteira e programa de desempenho</li> </ul>	<ul style="list-style-type: none"> <li>Método de coleta dos custos de dados</li> </ul>	Interno
	BAI01.02	<ul style="list-style-type: none"> <li>Plano do programa de compreensão do benefício</li> </ul>	<ul style="list-style-type: none"> <li>Método de consolidação de custos</li> </ul>	Interno
	BAI01.04	<ul style="list-style-type: none"> <li>Registro do programa de orçamento e benefícios</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidades de otimização de custos</li> </ul>	APO02.02
	BAI01.05	<ul style="list-style-type: none"> <li>Monitoramento dos resultados da compreensão do benefício</li> </ul>		
<b>Atividades</b>				

- 01 Assegurar a devida autoridade e independência entre os donos do orçamento de TI e as pessoas que capturaram, analisam e reportam as informações financeiras.
- 02 Estabelecer prazos para o funcionamento do processo de gestão de custos em linha com os requisitos de orçamento e contabilidade.
- 03 Definir um método para levantamento dos dados relevantes para identificar desvios para:  
 • Controle de orçamento entre o real e o orçamento  
 • Gestão de benefícios de:  
 - Metas versus realizado para investimentos em soluções; possivelmente, expressa em termos de ROI, NPV ou IRR  
 - A tendência real do custo do serviço para otimização de custo dos serviços (por exemplo, definida como custo por usuário)  
 - Orçamento versus realizado para resposta e previsibilidade de melhorias de entrega de soluções  
 • Distribuição de custos entre custos diretos e indiretos (absorvida e não absorvida)
- 04 Definir como os custos são consolidados para os níveis adequados na organização e como eles serão apresentados para as partes interessadas. Os relatórios fornecem informações que permitem identificação tempestiva de ações corretivas necessárias.
- 05 Instruir os responsáveis pela gestão de custos para captar, recolher e consolidar os dados, e relatar os dados para os donos do orçamento. Em conjunto, analistas e donos de orçamento devem analisar desvios e comparar o desempenho de benchmarks internos e da indústria. O resultado da análise fornece uma explicação de desvios significativos e as ações de correção.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO06 Práticas de Processo, Entradas/Saídas e Atividades

- 06 Certificar que os responsáveis pela gestão revisam os resultados da análise e aprovam as ações corretivas sugeridas.
- 07 Alinhar os orçamentos e serviços de TI à infraestrutura de TI, processos corporativos e os donos que as utilizam.
- 08 Certificar que as mudanças na estrutura de custos e necessidades da organização são identificadas e orçamentos e previsões são revistos, conforme necessário.
- 09 Em intervalos regulares, e especialmente quando os orçamentos são cortados devido a restrições financeiras, identificar métodos de otimização de custos e introduzir ganhos de eficiência, sem comprometer os serviços.

## APO06 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	6.4 Orçamento e contabilização para serviços de TI
ITIL V3 2011	Estratégia de Serviços, 4.3 Gestão Financeira de serviços de TI

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

AP007 Gerenciar Recursos Humanos	Área: Gestão Dominio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b>	
Proporcionar uma abordagem estruturada para garantir a estruturação ideal, colocação, direitos de decisão e as competências dos recursos humanos. Isso inclui a comunicação dos papéis e responsabilidades definidas, aprendizagem e crescimento dos planos e expectativas de desempenho, suportado por pessoas competentes e motivadas.	
<b>Declaração de Propósito do Processo</b>	
Otimizar as capacidades dos recursos humanos para atender os objetivos da organização.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alineamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>• Porcentagem dos objetivos e necessidades estratégicas da organização suportada por metas estratégicas de TI</li> <li>• Nível de satisfação das partes interessadas com o escopo do portfólio planejado de programas e serviços</li> <li>• Porcentagem de direcionadores do valor da TI mapeada para os direcionadores do valor do negócio</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>• Frequência da maturidade da capacidade e de avaliações de otimização de custo</li> <li>• Tendência dos resultados da avaliação</li> <li>• Os níveis de satisfação dos executivos negócios e de TI estão relacionados com os custos e capacidades da TI</li> </ul>
13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	<ul style="list-style-type: none"> <li>• Número de programas/projetos no prazo e dentro do orçamento</li> <li>• Porcentagem de partes interessadas satisfeitas com a qualidade do programa/projeto</li> <li>• Número de programas que necessitam de retrabalho devido a problemas de qualidade</li> <li>• Custo de manutenção da aplicação versus custo global de TI</li> </ul>
16 Equipes de TI e de negócios motivadas e qualificadas	<ul style="list-style-type: none"> <li>• Porcentagem de funcionários cujas atuais habilidades relacionadas a TI sejam suficientes para exercer o seu papel</li> <li>• Porcentagem de funcionários satisfeitos com as suas funções relacionadas a TI</li> <li>• Número de horas de treinamento/formação, por funcionário</li> </ul>
17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>• Nível de sensibilização dos executivos de negócio e compreensão das possibilidades de inovação da TI</li> <li>• Nível de satisfação das partes interessadas, com os níveis de especialização inovação e ideias da TI</li> <li>• Número de ações aprovadas resultantes de ideias inovadoras de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 A estrutura organizacional de TI e os relacionamentos são flexíveis e responsivos.	<ul style="list-style-type: none"> <li>• Número de definições de serviço e catálogos de serviços</li> <li>• Nível de satisfação executiva com a gestão de tomada de decisões</li> <li>• Número de decisões que não pôde ser resolvida no âmbito das estruturas de gestão e foram escalonados para estruturas de governança</li> </ul>
02 Recursos humanos são eficazes e eficientemente gerenciados.	<ul style="list-style-type: none"> <li>• Porcentagem de rotatividade de funcionários</li> <li>• Duração média de vagas</li> <li>• Porcentagem de posições vagas</li> </ul>

# COBIT® : HABILITANDO PROCESSOS

APO07 Tabela RACI

Prática de Gestão	Conselho de Administração	Director Executivo (Presidente) (CEO)	Director Financeiro (CFO)	Director de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês: Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Director de Riscos (CRO)	Director de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Director de TI (CIO)	Gerente de Arquitetura	Gerente de Desenvolvimento	Gerente de Operações de TI	Gerente de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
APO07.01 Manter pessoal adequado e apropriado.						R		I							R			A	R	R	R	R	R	R	R	
APO07.02 Identificar pessoal-chave de TI.						R								R			A	R	R	R	R	R	R	R	R	
APO07.03 Manter as habilidades e competências do pessoal.						R								R			A	R	R	R	R	R	R	R	R	
APO07.04 Avaliar o desempenho do colaborador.						R								R			A	R	R	R	R	R	R	R	R	
APO07.05 Planejar e controlar o uso da TI e de recursos humanos do negócio.					R C A R R									I			R	R	R	R	R	R	R	R	R	
APO07.06 Gerenciar equipe contrato.						R								R			A	R	R	R	R	R	R	R	R	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO07 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
APO 07.01 Manter pessoal adequado e apropriado.  Avaliar as necessidades de pessoal em uma base regular ou em grandes mudanças operacionais, da empresa ou dos ambientes de TI para garantir que a empresa possua recursos humanos suficientes para apoiar as metas e objetivos. O quadro de pessoal deve incluir tanto recursos internos e externos.	EDM04.01	<ul style="list-style-type: none"> <li>Plano de recursos aprovados</li> <li>Guia de princípios para a alocação de recursos e capacidades</li> </ul>	<ul style="list-style-type: none"> <li>Avaliações de requisitos de pessoal</li> </ul>	Interno
	EDM04.03	<ul style="list-style-type: none"> <li>Ações corretivas para resolver os desvios de gestão de recursos</li> </ul>	<ul style="list-style-type: none"> <li>Planos de desenvolvimento de competências e de carreira</li> </ul>	Interno
	APO01.02	<ul style="list-style-type: none"> <li>Definição de práticas de supervisão</li> </ul>	<ul style="list-style-type: none"> <li>Planos de suprimento pessoal</li> </ul>	Interno
	APO06.03	<ul style="list-style-type: none"> <li>Comunicações</li> <li>Orçamento</li> <li>Plano e orçamento de TI</li> </ul>		
	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>Metas e objetivos da organização</li> <li>Políticas e procedimentos da área de RH</li> </ul>		

#### Atividades

01 Avaliar as necessidades de funcionários em uma base regular ou a grandes mudanças para garantir que a:

- A função de TI possua recursos suficientes para suportar adequadamente e de forma apropriada as metas e objetivos da empresa
- A organização possui recursos suficientes para suportar adequadamente e de forma apropriada os processos de negócios e controles e iniciativas habilitadas de TI

02 Manter o processo de recrutamento e retenção de funcionários de negócios e de TI em linha com as políticas e procedimentos de recursos humanos da organização.

03 Incluir análise de antecedentes no processo de recrutamento de TI para funcionários, contratados e fornecedores. A extensão e

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**APO07 Práticas de Processo, Entradas/Saídas e Atividades.**

frequência dos controles devem depender da sensibilidade e/ou criticidade da função.

**04** Estabelecer mecanismos de recursos flexíveis para suportar mudanças das necessidades de negócios, tais como o uso de transferências, contratações externas e combinação de serviços de terceiros.

**05** Certificar a ocorrência de treinamento cruzado e existência de backup para o pessoal-chave e reduzir o risco de dependência de uma única pessoa.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 07.02 Identificar pessoas chave de TI.</b> Identificar pessoas chave de TI, minimizando a dependência de um único funcionário que exerce uma função de trabalho crítica através da captura de conhecimento (documentação), o compartilhamento de conhecimento, planejamento de sucessão e backup pessoal.			• Lista de pessoal-chave	Interno

**Atividades**

**01** Minimizar a dependência em um único indivíduo que executa uma função de trabalho crítica através da captura de conhecimento (documentação), a compartilhamento de conhecimento, planejamento de sucessão, backup do pessoal, treinamento cruzado e iniciativas de rotação de trabalho.

**02** Como medida de segurança, fornecer orientações sobre um tempo mínimo de férias anuais a serem tomadas pelos indivíduos-chave.

**03** Tomar medidas adequadas em relação às mudanças de emprego, especialmente em conclusões de trabalho.

**04** Testar regularmente os planos de backup do pessoal.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 07.03 Manter as habilidades e competências do pessoal.</b> Definir e gerenciar as habilidades e competências necessárias do pessoal. Regularmente verificar se o pessoal possui as competências para cumprir as suas funções com base em sua educação, formação e/ou experiência, e verificar se essas competências estão sendo mantidas, usando a qualificação e programas de certificação, quando apropriado. Fornecer aos funcionários a aprendizagem e oportunidades para manter seus conhecimentos, habilidades e competências a um nível necessário para atingir os objetivos empresariais em curso.	EDM01.02	• Abordagem do sistema de recompensa	• Matriz de habilidades e competências	AP001.02 BAI01.02 BAI01.04
	EDM04.03	• Ações corretivas para resolver os desvios de gestão de recursos	• Planos de desenvolvimento de competências	EDM04.01 AP001.02
	BAI08.03	• Repositórios de conhecimento publicados	• Relatórios de avaliação	Interno
	BAI08.04	• Conscientização do conhecimento e programa de treinamento		
	DSS04.06	• Resultados de monitoramento de habilidades e competências • Requisitos de treinamento		
	Referência externa ao COBIT	• Metas e objetivos corporativos		

**Atividades**

**01** Definir as habilidades e competências dos recursos internos e externos necessários e disponíveis atualmente para alcançar as metas da organização, processo e de TI.

**02** Fornecer plano de carreira formalizada e desenvolvimento profissional para incentivar o desenvolvimento de competências, oportunidades de desenvolvimento pessoal e redução da dependência de pessoal-chave.

**03** Proporcionar acesso a bases de conhecimento para apoiar o desenvolvimento de habilidades e competências.

**04** Identificar lacunas entre as competências necessárias e disponíveis e desenvolver planos de ação para resolvê-las de forma individualizada e coletiva, tais como a formação (competências técnicas e comportamentais), recrutamento, readaptação e mudança estratégica de suprimentos.

**05** Desenvolver e implementar programas de formação com base em requisitos organizacionais e de processos, incluindo os requisitos para o conhecimento da organização, controles internos, conduta ética e segurança.

**06** Realizar revisões periódicas para avaliar a evolução das habilidades e competências dos recursos internos e externos. Revisar o planejamento de sucessão.

**07** Revisar materiais de treinamento e programas em uma base regular para assegurar a adequação em relação às mudanças por necessidades da organização e seu impacto sobre o conhecimento necessário, competências e habilidades.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

**APO07 Práticas de Processo, Entradas/Saídas e Atividades.**

**APO07 Práticas de Processo, Entradas/Saídas e Atividades.**

<b>Prática de Gestão</b>	<b>Entradas</b>		<b>Saídas</b>	
	<b>De</b>	<b>Descrição</b>	<b>Descrição</b>	<b>Para</b>
<b>APO 07.04 Avaliar o desempenho do empregado.</b> Realizar avaliações de desempenho em tempo hábil em uma base regular em relação aos objetivos individuais conforme os objetivos da organização, as normas estabelecidas, responsabilidades de trabalho, e as habilidades e quadro de competências. Os funcionários devem receber treinamento sobre o desempenho e conduzir, sempre que apropriado.	EDM01.02	• Abordagem sistema de recompensa	• Metas pessoais	Interno
	APO04.01	• Programa de reconhecimento e recompensa	• Avaliações de desempenho	
	BAI05.04	• Alinhamento dos objetivos de desempenho de RH	• Planos de melhoria	
	BAI05.06	• Resultados de avaliação de desempenho de RH		
	DSS06.03	• Atribuição dos direitos de acesso		
<b>Atividades</b>				
01 Considerar os objetivos funcionais/organização como contexto para a definição dos objetivos individuais.				
02 Estabelecer metas individuais alinhadas com os objetivos relevantes, de modo que haja uma clara contribuição para os objetivos de TI e da organização. Baseie as metas em objetivos SMART (específicos, mensuráveis, alcançáveis, relevantes e tempo limite) que refletem as competências essenciais, os valores corporativos e habilidades exigidas para o papel(is).				
03 Consolidar os resultados da avaliação de desempenho 360 graus.				
04 Implementar e comunicar um processo disciplinar.				
05 Fornecer instruções específicas para o uso e armazenamento de informações pessoais no processo de avaliação, em conformidade com os dados pessoais aplicáveis e legislação trabalhista.				
06 Fornecer feedback em tempo hábil sobre o desempenho em relação às metas do colaborador.				
07 Implementar um processo de remuneração/reconhecimento de que recompensa o comprometimento adequado, o desenvolvimento de competências e a realização bem sucedida de metas de desempenho. Certificar que o processo é aplicado de forma consistente e em linha com as políticas organizacionais.				
08 Desenvolver planos de melhoria de desempenho, com base nos resultados do processo de avaliação e identificar as necessidades de formação e desenvolvimento de competências.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO07 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 07.05 Planejar e controlar o uso da TI e recursos humanos de negócios.</b> Compreender e acompanhar a demanda atual e futura de recursos humanos de negócios e de TI com responsabilidades na TI corporativa. Identificar as deficiências e contribuir em planos de fornecimento, planos de contratação de empresas e recursos de TI e de processos de recrutamento do negócio e TI.	EDM04.02	• Comunicação de estratégias de obtenção de recursos	• Inventário de recursos humanos de negócios e TI	BAI01.04 BAI01.06 BAI01.06
	EDM04.03	• Comentários sobre alocação e eficácia dos recursos e capacidades	• Análise do déficit de suprimentos	
	APO06.02	• Alocações orçamentárias	• Registros de utilização de recursos	
	BAI01.04	• Necessidades de recursos e funções		
	BAI01.12	• Requisitos de recursos do projeto		
	Referência externa ao COBIT	• Estrutura de organização empresarial		

## Atividades

- 01 Criar e manter um inventário dos recursos humanos de negócios e de TI.
- 02 Compreender a demanda atual e futura de recursos humanos para apoiar a realização dos objetivos de TI e fornecer serviços e soluções baseados na carteira de atual de iniciativas relacionadas com a TI, às futuras necessidades operacionais carteira de investimentos e do dia-a-dia.
- 03 Identificar lacunas e contribuir para manter o plano, bem como a organização e processo de recrutamento de TI. Criar e rever o plano de pessoal, mantendo o controle de uso real.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 07.06 Gerenciar colaboradores contratados.</b> Certificar de que os consultores e pessoal contratado que apoia a empresa possuam habilidades e conhecimento de TI e respeita as políticas da organização e concordou com as exigências contratuais.	BAI01.04	• Necessidades de recursos e funções	• Políticas de pessoal contrato	Interno
	BAI01.12	• Requisitos de recursos do projeto	• Acordos contratuais	
	BAI01.14	• Comunicação do programa de aposentadoria e prestação de contas em curso	• Revisões do contrato	

## Atividades

- 01 Implementar políticas e procedimentos que descrevem quando, como e que tipo de trabalho pode ser realizado ou acrescentado por consultores e/ou contratados, de acordo com a política de compras e a estrutura de gestão de TI.
- 02 Obter acordo formal dos fornecedores no inicio do contrato que eles são obrigados a cumprir com a estrutura de gestão de TI da organização, tais como políticas de segurança, física e controle de acesso lógico, uso de instalações, os requisitos de confidencialidade da informação, e acordos de não divulgação.
- 03 Os contratantes informam que a gestão reserva-se o direito de monitorar e fiscalizar todo o uso dos recursos de TI, incluindo e-mail, comunicações de voz, e todos os programas e arquivos de dados.
- 04 Prover aos fornecedores uma definição clara de seus papéis e responsabilidades, como parte de seus contratos, incluindo os requisitos explícitos para documentar o seu trabalho de acordo com padrões e formatos.
- 05 Revisar contratos de trabalho e basear a aprovação de pagamentos sobre os resultados.
- 06 Definir todo o trabalho realizado por terceiros em contratos formais e não ambíguos.
- 07 Realizar revisões periódicas para garantir que o pessoal contratado assinou e concordou com todos os acordos necessários.
- 08 Conduzir revisões periódicas para garantir que os papéis dos contratados e direitos de acesso são adequados e em conformidade com os acordos.

## APO07 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 27002	08 Recursos Humanos de Segurança
SFIA	Referência de habilidades

# COBIT® 5 : HABILITANDO PROCESSOS

APO08 Gerenciar Relacionamentos	Área: Gestão Dominio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b>	
Gerenciar o relacionamento entre o negócio e TI de uma maneira formal e transparente, que garanta um foco em alcançar um objetivo comum e compartilhado dos resultados corporativos bem-sucedidos em apoio de metas estratégicas e dentro da limitação de orçamentos e tolerância ao risco. Basear as relações na confiança mútua, usando termos abertos e comprehensíveis e de linguagem comum e com propriedade e responsabilidade para decisões fundamentais.	
<b>Declaração de Propósito do Processo</b>	
Optimizar as capacidades dos recursos humanos para atenderem os objetivos da organização.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Ainhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>• Porcentagem de requisitos e metas estratégicas da organização apoiada por metas estratégicas de TI</li> <li>• Nível de satisfação das partes interessadas com o escopo do portfólio planejado de programas e serviços</li> <li>• Porcentagem de direcionadores de valor de TI mapeada para direcionadores de valor de negócios</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>• Número de interrupções no negócio devido aos incidentes de serviço de TI</li> <li>• Porcentagem de partes interessadas do negócio satisfeita onde a entrega de serviços atende os níveis de serviço acordados</li> <li>• Porcentagem de usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
12 Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia	<ul style="list-style-type: none"> <li>• Número de incidentes de processamento do negócio causado por erros de integração de tecnologia</li> <li>• Número de mudanças do processo de negócio que precisam ser atrasadas ou reformuladas por causa de problemas de integração de tecnologia</li> <li>• Número de programas de negócios atrasados ou ocorrência de custos adicionais devido a questões de integração tecnológica</li> <li>• Número de pedidos de infraestrutura crítica que operam em silos e não integrado</li> </ul>
17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>• Nível de conscientização executiva de negócios e compreensão da TI possibilite a inovação</li> <li>• Nível de satisfação das partes interessadas com os níveis de especialização da inovação e de ideias de TI</li> <li>• Número de iniciativas aprovadas resultantes de ideias inovadoras de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Estratégias de negócios, planos e requisitos são bem compreendidos, documentadas e aprovadas.	<ul style="list-style-type: none"> <li>• Porcentagem de alinhamento dos serviços de TI com requisitos de negócios da organização</li> </ul>
02 Existência de boas relações entre a organização e TI.	<ul style="list-style-type: none"> <li>• As pesquisas de satisfação classificam os usuários e o pessoal de TI</li> </ul>
03 As partes interessadas de negócio estão cientes das oportunidades habilitadas por tecnologia.	<ul style="list-style-type: none"> <li>• Pesquisa de conscientização do nível tecnológico das partes interessadas de negócio</li> <li>• Taxa de Inclusão de oportunidades tecnológicas em propostas de investimento</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO08 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escrítorio de Programas e Projetos (PMO)	Escrítorio de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Contabilidade dos Negócios	Oficial de Privacidade
<b>APO 08.01</b> Compreender as expectativas de negócios.	C C C C C R C						C	C					C C A C	R R R	C R R R											
<b>APO 08.02</b> Identificar oportunidades, riscos e limitações para a TI para melhorar o negócio.	I I I R R R							C				I	C C A R	R R R	R											
<b>APO 08.03</b> Administrar o relacionamento comercial.	C C C R R I															A R R R										
<b>APO 08.04</b> Coordenar e comunicar.	R I R R R I															A R R R										
<b>APO 08.05</b> Contribuir para a melhoria contínua dos serviços.	C I C R I						C						C C A C	R R	R C C C											

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO08 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO08.01 Entender expectativas de negócios.</b> Compreende questões de negócios atuais e objetivos e expectativas de negócios para TI. Assegura que requisitos foram compreendidos, geridos e comunicados, e seu status acordado e aprovado.	APO02.05	• Roteiro Estratégico	• Expectativas de negócios esclarecidas e Interno acordadas	
<b>Atividades</b>				
01 Identificar as partes interessadas do negócio, seus interesses e das suas responsabilidades.				
02 Rever o atual direcionamento da empresa, problemas, objetivos estratégicos e alinhamento com arquitetura corporativa.				
03 Manter uma tomada de consciência de processos de negócios e atividades conexas e compreender os padrões de demanda que se relacionam com volumes e uso de serviço.				
04 Clarificar as expectativas de negócios para soluções e serviços de TI e assegurar que os requisitos são definidos com critérios de aceitação de negócios associados e métricas.				
05 Confirmar expectativa do acordo de negócios, os critérios de aceitação e métricas em partes relevantes para IT por todas as partes interessadas.				
06 Gerencie expectativas, garantindo que as unidades de negócios entendem as prioridades, as dependências, as restrições financeiras e a necessidade de agendar requisições.				
07 Compreender o ambiente de negócios atual, restrições de processo ou questões, expansão geográfica ou contração e direcionadores de indústria/normativos.				

# COBIT® : HABILITANDO PROCESSOS

## APO08 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO08.02 identificar oportunidades, riscos e restrições em IT para que possa melhorar o negócio.</b> Identificar oportunidades para que seja um habilitador do de avançado desempenho empresarial.	APO09.01	<ul style="list-style-type: none"> <li>Identificação de gaps em serviços de TI para o negócio</li> </ul>	<ul style="list-style-type: none"> <li>Próximos passos e planos de ação acordados</li> </ul>	Interno
	APO09.04	<ul style="list-style-type: none"> <li>Melhoria em planos de ação e remediações</li> <li>Relatórios de desempenho de nível de serviço</li> </ul>		
	APO11.05	<ul style="list-style-type: none"> <li>Causas de falhas de entrega de qualidade</li> </ul>		

### Atividades

- Compreender as tendências de tecnologia e novas tecnologias e como estas podem ser aplicadas de forma inovadora para melhorar o desempenho do processo de negócios.
- Desempenhar um papel proativo na identificação e comunicando-se com as principais partes interessadas em oportunidades, riscos e restrições. Isso inclui tecnologias atuais e emergentes, serviços e modelos de processo de negócios.
- Colaborar em concordar sobre os passos seguintes para grandes novas iniciativas em conjunto com gestão de portfólio, incluindo desenvolvimento de casos de negócio (business cases).
- Certificar-se que a empresa e a TI entendem e apreciam os objetivos estratégicos e a visão da arquitetura corporativa.
- Coordenar ao planejar novas iniciativas para garantir a integração e o alinhamento com a arquitetura corporativa

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO08.03 Gerenciar a relação de negócios, Gerenciar o relacionamento com clientes (representantes comerciais).</b> Assegurar que papéis de relacionamento e suas responsabilidades são definidas e atribuídas e a comunicação é facilitada.	DSS02.02	<ul style="list-style-type: none"> <li>Incidentes e solicitações de serviço classificados e hierarquizados</li> </ul>	<ul style="list-style-type: none"> <li>Decisões chave alinhadas</li> </ul>	Interno
	DSS02.06	<ul style="list-style-type: none"> <li>Confirmação de usuários de cumprimento ou resolução satisfatórios</li> <li>Incidentes e requisição de serviços fechados</li> </ul>		
	DSS02.07	<ul style="list-style-type: none"> <li>Request fulfilment status and trends report</li> <li>Relatório de tendências e status de incidente</li> </ul>		

### Atividades

- Atribuir um gerente de relacionamento como um único ponto de contato para cada unidade de negócios significativa. Certifique-se que uma única contraparte é identificada na organização empresarial e a contraparte tem compreensão do negócio, suficiente consciência da tecnologia e o nível apropriado de autoridade.
- Gerenciar a relação de maneira formalizada e transparente que garante foco em atingir um objetivo comum e compartilhado dos resultados de sucesso empresarial para apoiar os objetivos estratégicos e dentro da restrição de orçamentos e tolerância ao risco.
- Definir e comunicar um procedimento de reclamações e escalonamento para resolver quaisquer problemas de relacionamento.
- Planejar interações específicas e horários com base em objetivos mutuamente acordados e linguagem comum (reuniões de revisão de serviço e desempenho, revisão de novas estratégias ou planos, etc.).
- Garantir que decisões chave sejam alinhadas em e aprovadas pelas partes interessadas responsáveis.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO08.04 coordenar e comunicar.</b> Trabalhar com as partes interessadas e coordenar entrega de serviços de TI ponta a ponta e soluções fornecidas para os negócios	APO09.03	<ul style="list-style-type: none"> <li>SLAs</li> </ul>	<ul style="list-style-type: none"> <li>Plano de Comunicação</li> </ul>	Interno
	APO12.06	<ul style="list-style-type: none"> <li>Comunicação de impacto de risco</li> </ul>		
	BAI05.05	<ul style="list-style-type: none"> <li>Plano de uso e operação</li> </ul>		
	BAI07.07	<ul style="list-style-type: none"> <li>Plano de suporte suplementar</li> </ul>		
	BAI09.02	<ul style="list-style-type: none"> <li>Comunicações de inatividade de manutenção planejada</li> </ul>		
	DSS03.04	<ul style="list-style-type: none"> <li>Comunicação do conhecimento aprendido</li> </ul>		

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO08 Práticas de Processo, Entradas/Saídas e Atividades.

Atividades			
01 Coordenar e comunicar alterações e atividades como projetos de transição ou mudança de planos, horários, condições de lançamento, erros de versão conhecidos e treinamento de conscientização.			
02 Coordenar e comunicar as atividades operacionais, funções e responsabilidades, incluindo a definição dos tipos de solicitação, escalonamento hierárquico, grandes paralisações (planejados e não planejados) e conteúdo e a frequência dos relatórios de serviço.			
03 Apropriar-se da resposta ao negócio para grandes eventos que possam influenciar a relação com o negócio. Providenciar Apoio direto se necessário.			
04 Manter um plano de comunicação ponta a ponta que define o conteúdo, frequência e os destinatários das informações de entrega do serviço, incluindo o status de valor entregado e qualquer risco identificado.			

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO08.05 Fornecer a entrada para a melhoria contínua dos serviços.</b> <i>Continually improve and evolve IT-enabled services and service delivery to the enterprise to align with changing enterprise and technology requirements.</i>	APO09.02	Catálogo de serviço	Análises de satisfação	APO09.04
	APO11.03	<ul style="list-style-type: none"> <li>Resultados de avaliação da qualidade do serviço, incluindo o feedback dos clientes</li> <li>Exigências do cliente para gestão da qualidade</li> </ul>	<ul style="list-style-type: none"> <li>Definição de potenciais projetos de melhoria</li> </ul>	APO02.02 BAI03.11
	APO11.04	<ul style="list-style-type: none"> <li>Resultados de avaliações de qualidade e auditorias</li> </ul>		
	APO11.05	<ul style="list-style-type: none"> <li>Resultados da solução e monitoramento da qualidade de entrega do serviço</li> </ul>		
	BAI03.10	<ul style="list-style-type: none"> <li>Plano de manutenção</li> </ul>		
	BAI05.05	<ul style="list-style-type: none"> <li>Resultados e medidas de sucesso</li> </ul>		
	BAI07.07	<ul style="list-style-type: none"> <li>Plano de suporte suplementar</li> </ul>		

## Atividades

01 Realizar análise de satisfação do cliente e fornecedor. Certificar que questões são açãoadas e relatam os resultados e o status.
02 Trabalhar em conjunto para identificar, comunicar e implementar iniciativas de melhoria.
03 Trabalhar com gestão de serviços e processo proprietários para assegurar que os serviços habilitados e processos de gestão de serviços são continuamente melhorados e as causas de problemas são identificadas e resolvidas.

## APO08 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	7.2 Gestão de relacionamento de negócios
ITIL V3 2011	Estratégia de serviço, 4.4 Gerenciamento da demanda Estratégia de serviço, 4.5 Gestão de relacionamento de negócios

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

APO09 Gerenciar Contratos de Prestação de Serviços		Área: Gestão Domínio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b> Alinhar serviços de TI e níveis de serviço com a empresa às necessidades e expectativas, incluindo identificação, especificação, projeto, publicação, acordo e monitoramento de serviços de TI, os níveis de serviço e indicadores de desempenho.		
<b>Declaração de Propósito do Processo</b> Assegurar que os serviços de TI e os níveis de serviço se adequem às demandas atuais e futuras da empresa.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
<b>Objetivos de TI</b>		<b>Métricas Relacionadas</b>
<b>07</b> Prestação de serviços de TI em consonância com os requisitos de negócio		<ul style="list-style-type: none"> <li>• Número de interrupções de negócios devido a incidentes de serviço</li> <li>• % De partes interessadas satisfeitas que entrega de serviços atende os níveis de serviço acordado</li> <li>• % De usuários satisfeitos com a qualidade da prestação de serviços IT</li> </ul>
<b>14</b> Disponibilidade de informações úteis e confiáveis para a tomada de decisão		<ul style="list-style-type: none"> <li>• Nível de satisfação dos usuários de negócios com qualidade e pontualidade</li> <li>• (ou disponibilidade) de informações de gestão</li> <li>• Número de incidentes de processo de negócio causadas pela não disponibilidade de informações</li> <li>• Proporção e extensão das decisões errôneas negócios onde informações erradas ou indisponíveis foi fator-chave</li> </ul>
<b>Objetivos e Métricas do Processo</b>		
<b>Objetivo do Processo</b>		<b>Métricas Relacionadas</b>
<b>01</b> A empresa poderá efetivamente utilizar serviços conforme definido em um catálogo.		<ul style="list-style-type: none"> <li>• Número de processos de negócios com contratos de serviço indefinido</li> </ul>
<b>02</b> Acordos de serviço refletem as necessidades da empresa e os recursos da mesma.		<ul style="list-style-type: none"> <li>• % De serviços de TI abrangidos por acordos de serviço</li> <li>• % De clientes satisfeitos que a prestação de serviços atende níveis pré-acordados</li> </ul>
<b>03</b> Serviços de TI executados tal como estipulado nos acordos de serviço.		<ul style="list-style-type: none"> <li>• Número e a gravidade das brechas de serviço</li> <li>• % De serviços sendo monitorados nos níveis de serviço</li> <li>• % De metas de serviço sendo atendidas</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO09 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente)   CEO	Diretor Financeiro   CFO	Diretor de Operações   COO	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos   CRO	Diretor de Segurança da Informação   CSO	Conselho de Arquitetura	Comitê de Riscos da Organização	Conformidade	Auditor	Diretor de TI   CIO	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
APO09.01 Identificando serviços de TI	C	R	R	R	C	I								I	I	R	I	C	C	C	A	I	I		
APO09.02 Catálogo de serviços de TI				I	I		I							I	I	R	I	C	C	C	A	I	I		
APO09.03 Preparar e definir acordos de serviço			R	C		C	C							C	C	R		C	R	R	A	C	C		
APO09.04 Monitorar e reportar níveis de serviço	I	I	I	R				C						I	I	I	I	I	I	I	A				
APO09.05 Revisar contratos e acordo de serviços				A	C		C	C						C	C	R		C	R	R	R	C	C	I	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO09 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas	Saídas
<b>APO09.01 Identificar serviços de TI.</b> Analisar as necessidades dos negócios e a maneira em que Serviços de TI e níveis de serviço de suportam processos de negócios. Discutir e concordar sobre os potenciais serviços e níveis de serviço com o negócio e compará-los com o atual portfólio de serviços para identificar serviços novos ou alterados ou opções de nível de serviço.		<ul style="list-style-type: none"> <li>• Identificação de gaps em serviços de TI para o negócio</li> <li>• Definições de serviços padrão</li> </ul>
<b>Atividades</b>		
01 Avaliar níveis de serviço atuais para identificar gaps entre os serviços existentes e as atividades de negócios que sustentam serviço. Identificar áreas de melhoria dos serviços existentes e opções de nível de serviço.		
02 Analisar, estudar e estimar a demanda futura e confirmar a capacidade dos serviços habilitados existentes.		
03 Analisar as atividades do processo de negócios para identificar a necessidade de novos ou redesenhados serviços de TI.		
04 Comparar requisitos identificados de componentes de serviço existentes no portfolio. Se possível, empacotar componentes de serviço existentes (serviços, opções de nível de serviço e pacotes de serviços) em novos pacotes de serviço para atender requisitos de negócios identificados.		
05 Sempre que possível, corresponder as demandas para os pacotes de serviços e criar serviços normalizados para obter eficiência geral.		
06 Regularmente rever o portfólio de serviços de TI com gerenciamento de portfólio e gestão de relacionamento de negócios para identificar os serviços obsoletos. Acordar sobre retiradas e propor mudanças.		

Prática de Gestão	Entradas	Descrição	Descrição	Para
<b>APO09.02 Catálogo de serviços de TI</b> Definir e manter um ou mais catálogos de serviço para grupos-alvo relevantes. Publicar e manter vivo o Catálogos de serviços de TI	De	Descrição	Descrição	Para
	EDM04.01	• Plano de recursos aprovado	• Catálogo de serviços	APO08.05
	EDM04.02	• Comunicação de estratégias de criação de recursos		
APO05.05		• Portfolio de programas, serviços e bens		

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO09 Práticas de Processo, Entradas/Saídas e Atividades

### Atividades

01 Publicar em catálogos relevantes serviços de TI, pacotes de serviços e opções de nível de serviço do portfolio.

02 Continuamente, certificar-se de que os componentes de serviço em portfolio e os catálogos de serviços relacionados são completos e atualizados.

03 Informe a gestão de relacionamento de negócios de quaisquer atualizações para os catálogos de serviço.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
APO09.03 Definir e preparar os contratos de serviço. Definir e preparar os contratos de serviço com base em opções no serviço de catálogos. Incluir acordos operacionais internos.	APO11.03	<ul style="list-style-type: none"> <li>• Exigências do cliente para a gestão da qualidade</li> </ul>	<ul style="list-style-type: none"> <li>• SLAs</li> </ul>	APO05.03 APO08.04 DSS01.02  DSS02.01 DSS02.02 DSS04.01 DSS05.02 DSS05.03
	BAI03.02	<ul style="list-style-type: none"> <li>• Revisões de SLA e OLA</li> </ul>	<ul style="list-style-type: none"> <li>• OLAs</li> </ul>	DSS01.02 DSS02.07 DSS04.03 DSS05.03

### Atividades

01 Análise de requisitos para atualizações ou novos acordos de serviços recebidos pela gestão de relacionamento de negócios para garantir que as condições possam ser acertadas. Considere aspectos, tais como tempo de serviço, disponibilidade, desempenho, capacidade, segurança, continuidade, conformidade e questões regulatórias, usabilidade e restrições de demanda.

02 Esboçar acordos de serviços para o cliente baseados em serviços, pacotes de serviço, opções de níveis de serviço em catálogos de serviço relevantes.

03 Determinar, alinhar e documentar acordos operacionais internos para sustentar os acordos de serviço ao cliente, se aplicável.

04 Colaborar com a gestão de fornecedores para garantir que contratos comerciais sejam adequados com prestadores de serviços externos e sustentem os acordos de serviço ao cliente, se aplicável.

05 Finalizar acordos de serviço ao cliente com gestão de relacionamento de negócios.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO09 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
APO09.04 Monitorar e relatar os níveis de serviço. Monitorar os níveis de serviço, um relatório sobre as realizações e identificar tendências. Fornece as informações apropriadas de gestão para auxiliar o gerenciamento de desempenho.	EDM04.03	<ul style="list-style-type: none"> <li>Ações corretivas para desvios de gestão de recursos de endereço</li> </ul>	<ul style="list-style-type: none"> <li>Relatórios de desempenho de nível de serviço</li> </ul>	APO08.02 MEA01.03  APO02.02 APO08.02
	APO05.04	<ul style="list-style-type: none"> <li>Relatórios de desempenho do portfólio de investimento</li> </ul>	<ul style="list-style-type: none"> <li>Remediações e planos de ação de melhoria</li> </ul>	
	APO05.06	<ul style="list-style-type: none"> <li>Ações corretivas para melhorar a realização do benefício</li> <li>Resultados de benefício e comunicações relacionadas</li> </ul>		
	APO08.05	<ul style="list-style-type: none"> <li>Análises de satisfação</li> </ul>		
	APO11.04	<ul style="list-style-type: none"> <li>Resultados de avaliações de qualidade e auditorias</li> </ul>		
	APO11.05	<ul style="list-style-type: none"> <li>Causas de falhas de entrega de qualidade</li> <li>Resultados de solução e monitoramento de qualidade de entrega de serviço</li> </ul>		
	DSS02.02	<ul style="list-style-type: none"> <li>Solicitações de serviço Classificadas e hierarquizadas incidentes</li> </ul>		
	DSS02.06	<ul style="list-style-type: none"> <li>Incidentes e solicitações de serviço fechado</li> </ul>		
	DSS02.07	<ul style="list-style-type: none"> <li>Solicitação de cumprimento status e tendências relatório</li> <li>Relatório de situação e tendências de incidente</li> </ul>		
Atividades				

01 Estabelecer e manter medidas para monitorar e coletar dados de nível de serviço.

02 Avaliar o desempenho e fornecer relatórios regular e formalmente de execução de contrato de serviço, incluindo os desvios dos valores acordados. Distribuir este relatório de gestão de relacionamento de negócios.

03 Realizar revisões periódicas para previsão e identificar tendências no desempenho de nível de serviço.

04 Fornecer as informações apropriadas de gestão para auxiliar o gerenciamento de desempenho.

05 Alinhar planos de ação e remediações para quaisquer problemas de desempenho ou tendências negativas.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
APO09.05 Revisão de acordos de serviço e contratos. Realizar revisões periódicas dos acordos de serviço e revisar quando necessário.	EDM04.03	<ul style="list-style-type: none"> <li>Feedback sobre a alocação e a eficácia dos recursos e capacidades</li> </ul>	<ul style="list-style-type: none"> <li>Revisões de SLA</li> </ul>	Interno
	APO11.03	<ul style="list-style-type: none"> <li>Resultados da qualidade do serviço, incluindo o feedback dos clientes</li> </ul>		
	APO11.04	<ul style="list-style-type: none"> <li>Resultados de avaliações de qualidade e auditorias</li> </ul>		
	BAI04.01	<ul style="list-style-type: none"> <li>Avaliações contra os SLAs</li> </ul>		
Atividades				

01 Regularmente rever contratos de serviço de acordo com as condições acordadas para garantir que eles são eficazes e até à data e mudanças nas exigências, serviços habilitados, pacotes de serviços ou opções de nível de serviço são tidos em conta, quando apropriado.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO09 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	5.0 planejar e implementando serviços novos ou alterados 6.1 Gerenciamentos de nível de serviço
ITIL V3 2011	Estratégia de Serviço, 4.4 Gerenciamento de Demandas. Estratégia de Serviço, 4.2 Gerenciamento de Portfolio de Serviços. Estratégia de Serviço, 4.2 Gerenciamento de Catálogo de Serviços. Estratégia de Serviço, 4.3 Gerenciamento de Nível de Serviços.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO10 Gerenciar Fornecedores		Área: Gestão Dominio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b> Gerenciar serviços de TI prestados por todos os tipos de fornecedores para atender aos requerimentos da organização, incluindo a seleção de fornecedores, gerenciamento dos relacionamentos, gerenciamento de contratos, e revisão e monitoramento do desempenho de fornecedores para efetividade e conformidade.		
<b>Declaração de Propósito do Processo</b> Minimizar o risco associado a fornecedores com desempenho fraco e garantir preços competitivos.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
Objetivos de TI	Métricas Relacionadas	
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Percentual de processos críticos de negócios, serviços de TI e programas de negócio habilitados por TI cobertos pela avaliação de risco;</li> <li>Número de incidentes relevantes relacionados a TI que não foram identificados na avaliação de risco;</li> <li>Percentual de avaliações de risco organizacional incluindo riscos relacionados a TI;</li> </ul>	
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de paradas de negócio ocasionadas por incidentes de TI;</li> <li>Percentual de partes interessadas do negócio satisfeitas com a entrega de serviços atende os níveis de serviço acordados</li> <li>Percentual de usuários satisfeitos com a qualidade da entrega de serviços de TI</li> </ul>	
09 Agilidade de TI	<ul style="list-style-type: none"> <li>Nível de satisfação dos executivos de negócio com a capacidade de resposta de TI a novos requisitos</li> <li>Número de processos de negócio críticos suportados pela infraestrutura e aplicações atualizados</li> <li>Tempo médio para transformar objetivos de TI em iniciativas acordadas e aprovadas</li> </ul>	
<b>Objetivos e Métricas do Processo</b>		
Objetivo do Processo	Métricas Relacionadas	
01 Fornecedores desempenham conforme acordado	<ul style="list-style-type: none"> <li>Percentual de fornecedores que atendem aos requisitos acordados</li> </ul>	
02 Risco do fornecedor é avaliado e devidamente endereçado	<ul style="list-style-type: none"> <li>Número de eventos de risco que levaram a incidentes de serviço</li> <li>Frequência das sessões de gerenciamento de risco com o fornecedor</li> <li>Percentual de incidentes de risco resolvidos de forma aceitável (tempo e custo)</li> </ul>	
03 Relacionamento com os fornecedores está funcionando efetivamente.	<ul style="list-style-type: none"> <li>Número de reuniões de revisão de fornecedores</li> <li>Número de disputas formais com fornecedores</li> <li>Percentual de disputas resolvidas amigavelmente em um intervalo de tempo razoável</li> </ul>	

# COBIT® 5 : HABILITANDO PROCESSOS

APO10 Tabela RACI

Prática de Gestão	Conselho de Administração	Dirutor Executivo (Presidente) (CEO)	Dirutor Financeiro (CFO)	Dirutor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Dirutor de Riscos (CRO)	Dirutor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Dirutor de TI (CTO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>APO10.01</b> Identificar e avaliar o relacionamento com fornecedores e contratos.	C		C									C C C A C C C C R			C C C C C C C C R C C C C											
<b>APO10.02</b> Selecionar fornecedores.	C		C		I							C C C A C C C C R			C C C C C C C C R C C C C											
<b>APO10.04</b> Gerenciar relacionamento com fornecedores				C		R						C C C A C R R R			C C C C C C C C R C C C C											
<b>APO10.05</b> Monitorar o desempenho de fornecedores e a conformidade.	I		C			C						C C C A C R R R			C C C C C C C C R C C C C											

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO10 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO10.01 Identificar e avaliar o relacionamento com fornecedores e contratos.</b> Identificar fornecedores e contratos associados, e categorizá-los por tipo, relevância e criticidade. Estabelecer critérios de avaliação de fornecedores e contratos e avaliar o portfólio geral de contratos e fornecedores existentes e alternativos.	Referência externa ao COBIT	• Contratos do fornecedor	• Relevância do fornecedor e critério de avaliação • Catálogo de Fornecedores • Potenciais revisões dos contratos de fornecedor	Interno BAID2.02 Interno
<b>Atividades</b>				
01 Estabelecer e manter critérios relacionados ao tipo, relevância e criticidade dos fornecedores e contratos, habilitando o foco nos fornecedores preferidos e importantes.				
02 Estabelecer e manter fornecedores e critérios de avaliação de contrato para habilitar revisão generalizada e comparação do desempenho dos fornecedores de maneira consistente.				
03 Identificar, registrar e categorizar fornecedores existentes e contratos de acordo com critérios definidos para manter um registro detalhado dos fornecedores preferidos que precisam ser gerenciados de forma cuidadosa.				
04 Avaliar periodicamente e comparar o desempenho dos fornecedores existentes e alternativos, para identificar oportunidades ou uma necessidade atraente de reconsiderar os atuais contratos de fornecedores.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## APO10 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO10.02 Selecionar Fornecedores</b> Selecionar fornecedores de acordo com uma prática justa e formal, para garantir uma melhor adequação aos requisitos especificados.	BAI02.02	<ul style="list-style-type: none"> <li>• Plano de aquisição/desenvolvimento de alto nível</li> </ul>	<ul style="list-style-type: none"> <li>• Solicitação de Informação do fornecedor (RFI)</li> <li>• Avaliações de RFI e RFP</li> <li>• Resultados da decisão da avaliação de fornecedores</li> </ul>	BAI02.01 BAI02.02  BAI02.02  EDM04.01 BAI02.02
				<b>Atividades</b>

## 01 Revisar todas as RFIs e RFPs para garantir que elas:

- Definem claramente os requisitos
- Incluem um procedimento para esclarecer os requisitos
- Concedem aos fornecedores tempo suficiente para prepararem suas propostas
- Definem claramente o critério de premiação e o processo decisório

02 Avaliar RFIs e RFPs de acordo com o processo/critério de avaliação aprovado, e manter a evidência documental das avaliações.  
Verificar as referências dos candidatos a fornecedor.

03 Selecionar o fornecedor que melhor se adeque a RFP. Documentar e comunicar a decisão, e assinar o contrato.

04 No caso específico de aquisição de software, incluir e enfatizar os direitos e obrigações de todas as partes nos termos contratuais. Esses direitos e obrigações podem incluir propriedade e licenciamento de propriedade intelectual, manutenção, garantias, procedimentos arbitrais, termos de atualização e adequação para propósito, incluindo segurança, Garantia e direitos de acesso.

05 No caso específico de aquisição de desenvolvimento de recursos, incluir e enfatizar os direitos e obrigações de todas as partes nos termos contratuais. Esses direitos e obrigações podem incluir propriedade e licenciamento de propriedade intelectual; adequação para propósito, incluindo metodologias de desenvolvimento; testes; processos de gerenciamento de qualidade, incluindo critérios de desempenho requeridos; revisão de desempenho; base para pagamento; garantias; processos de arbitragem; gerenciamento de recursos humanos; e conformidade com as políticas da organização.

06 Obter aconselhamento legal para os acordos de aquisição de desenvolvimento de recursos, a respeito de propriedade e licenciamento de propriedade intelectual.

07 No caso específico de aquisição de infraestrutura, instalações e serviços relacionados, incluir e enfatizar os direitos e obrigações de todas as partes nos termos contratuais. Esses direitos e obrigações podem incluir níveis de serviço, procedimentos de manutenção, controles de acesso, segurança, revisão de desempenho, base para pagamento e procedimentos de arbitragem.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO10.03 Gerenciar relacionamentos e contratos com fornecedores.</b> Formalizar e gerenciar o relacionamento para cada fornecedor. Gerenciar, manter e monitorar contratos e entrega de serviços. Garantir que contratos novos ou alterados atendam a padrões da organização e requisitos legais e regulatórios. Lidar com disputas contratuais.	BAI03.04	<ul style="list-style-type: none"> <li>• Planos de aquisição aprovados</li> </ul>	<ul style="list-style-type: none"> <li>• Papéis e responsabilidades do fornecedor</li> <li>• Comunicação e revisão de processo</li> <li>• Resultados e melhorias sugeridas</li> </ul>	Interno  Interno  Interno
				<b>Atividades</b>

01 Atribuir proprietários de relacionamento para todos os fornecedores e torna-los prestadores de contas pela qualidade do serviço prestado.

02 Especificar um processo de comunicação e revisão formal, incluindo interações com fornecedores e agenda.

03 Acordar, gerenciar, manter e renovar contratos formais com o fornecedor. Garantir que os contratos estão em conformidade com os padrões da organização e requisitos legais e regulatórios.

04 Nos contratos com fornecedores de serviços chave, incluir provisões para revisão do local onde opera o fornecedor e práticas e controles internos por gerenciamento ou terceiros independentes.

05 Avaliar a efetividade do relacionamento e identificar melhorias necessárias.

06 Definir, comunicar e acordar formas de implementar as melhorias requeridas para o relacionamento.

07 Utilizar procedimentos estabelecidos para lidar com disputas contratuais, usando primeiro, quando possível, relacionamentos efetivos e comunicações para superar problemas de serviços.

08 Definir e formalizar papéis e responsabilidades para cada fornecedor de serviço. Onde há a combinação de vários fornecedores para prover um serviço, considerar a adoção do papel de contratante principal para um dos fornecedores para assumir a responsabilidade por um contrato geral.

# COBIT® 5 : HABILITANDO PROCESSOS

## APO10 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO 10.04 Gerenciar risco de fornecedores.</b> Identificar e gerenciar o risco relacionado a capacidade dos fornecedores de entregar serviços com segurança, eficiência e efetividade contínuas.	APO12.04	<ul style="list-style-type: none"> <li>Resultados das avaliações de risco de terceiros</li> <li>Relatórios de análise e perfil de risco para as partes interessadas</li> </ul>	<ul style="list-style-type: none"> <li>Risco de entrega do fornecedor identificado</li> <li>Requisitos contratuais para minimizar o risco identificados</li> </ul>	APO12.01 APO12.03 BAI01.01  Interno
<b>Atividades</b>				
<p>01 Identificar, monitorar e, onde for apropriado, gerenciar o risco relacionado a capacidade dos fornecedores de entregar serviços de forma eficiente, efetiva, segura e contínua.</p> <p>02 Quando definir o contrato, prever o potencial risco de serviço através de requisitos de serviço claramente definidos, incluindo acordo de Garantia de software, fornecedores alternativos ou acordos de prontidão para mitigar possíveis falhas do fornecedor; segurança e proteção da propriedade intelectual, e qualquer requisito legal ou regulatório.</p>				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO10.05 Monitorar o desempenho e conformidade do fornecedor</b> Revisar periodicamente o desempenho geral dos fornecedores, conformidade com os requisitos contratuais, valor financeiro, e endereçar questões identificadas.			<ul style="list-style-type: none"> <li>Critério de monitoramento de conformidade do fornecedor</li> <li>Revisão dos resultados do monitoramento de conformidade do fornecedor</li> </ul>	Interno  MEAO1.03
<b>Atividades</b>				
<p>01 Definir e documentar os critérios para monitorar o desempenho do fornecedor, alinhado com os acordos de nível de serviço, e garantir que o fornecedor reporta regularmente e de forma transparente com base nos critérios acordados.</p> <p>02 Monitorar e revisar a entrega de serviços para garantir que o fornecedor está provendo uma qualidade aceitável de serviços, atende os requisitos e está aderente às condições contratuais.</p> <p>03 Revisar o desempenho do fornecedor e valor financeiro para garantir que eles são confiáveis e competitivos, comparados com fornecedores alternativos e condições de mercado.</p> <p>04 Solicitar revisões independentes das práticas e controles internos do fornecedor, se necessário.</p> <p>05 Registrar e avaliar resultados de revisão periódica, e discutir esses resultados com o fornecedor, para identificar necessidades e oportunidades de melhoria.</p> <p>06 Monitorar e avaliar externamente as informações disponíveis sobre o fornecedor.</p>				

## APO10 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	7.3 Gerenciamento de Fornecedores
ITIL V3 2011	Desenho de Serviço, 4.8 Gerenciamento de Fornecedores
Project Management Body of Knowledge (PMBOK)	Processos de aquisição do PMBOK

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO11 Gerenciar Qualidade	Área: Gestão Domínio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b>	
Definir e comunicar os requisitos de qualidade em todos os processos, procedimentos e resultados relacionados da organização, incluindo controles, monitoramento contínuo, e o uso de provas práticas e padrões na melhoria contínua e esforços de eficiência.	
<b>Declaração de Propósito do Processo</b>	
Garantir a entrega consistente de soluções e serviços para atender aos requisitos de qualidade da organização e satisfazer as necessidades das partes interessadas.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	<ul style="list-style-type: none"> <li>Percentual de investimentos habilitadores de TI, onde a realização do benefício é monitorada através de todo o ciclo econômico.</li> <li>Percentual de serviços de TI onde os benefícios esperados são realizados.</li> <li>Percentual dos investimentos habilitadores de TI onde os benefícios afirmados foram atendidos ou excedidos</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de paradas de negócio ocasionadas por incidentes de serviço de TI</li> <li>Percentual de partes interessadas do negócio satisfeitas com a entrega de serviço atingindo os níveis de serviço acordados</li> <li>Percentual de usuários satisfeitos com a qualidade da entrega do serviço de TI</li> </ul>
13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	<ul style="list-style-type: none"> <li>Número de programas/Projetos no prazo e dentro do orçamento</li> <li>Percentual de partes interessadas satisfeitas com a qualidade dos programas/projetos</li> <li>Número de programas que precisam de retrabalho significativo em função de defeitos de qualidade</li> <li>Custo da manutenção de aplicações x custo total de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Partes Interessadas estão satisfeitas com a qualidade das soluções e serviços	<ul style="list-style-type: none"> <li>Taxa media de satisfação das partes interessadas com as soluções e serviços</li> <li>Percentual de partes interessadas satisfeitas com a qualidade de TI</li> <li>Número de serviços com um plano de gerenciamento de segurança formal.</li> </ul>
2.Resultados de Projetos e entrega de serviços são previsíveis	<ul style="list-style-type: none"> <li>Percentual de Projetos revisados que atingem a meta e os objetivos de qualidade</li> <li>Percentual de soluções e serviços entregues com certificação formal</li> <li>Número de defeitos antes da entrada em produção</li> </ul>
03 Requisitos de qualidade estão implementados em todos os processos.	<ul style="list-style-type: none"> <li>Número de processos com um requisito de qualidade definido</li> <li>Número de processos com um relatório formal de avaliação de qualidade</li> <li>Número de SLA's que incluem critérios de aceitação de qualidade</li> </ul>

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

APO11 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escrítorio de Programas e Projetos (PMO)	Escrítorio de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>APO11.01</b> Estabelecer um Sistema de Gerenciamento de Qualidade (QMS).	C	A	C	I	C	I	I				C		C	C	R	C	C	I	R	R	I	I	I			
<b>APO11.02</b> Definir e gerenciar os padrões de qualidade, práticas e procedimentos.	C			C	R	C		R			C		C	C	A	R	R	R	R	R	R	R	R	R		
<b>APO11.03</b> Focalizar o gerenciamento da qualidade nos clientes.				A	R	C		I					C	C	R	I	I	I	I	R	I	I				
<b>APO11.04</b> Realizar o monitoramento da qualidade, controle e revisões.	C		C	R	C	R	C	R					C	C	A	C	C	C	C	R	C	C	C			
<b>APO11.05</b> Integrar gerenciamento da qualidade nas soluções para desenvolvimento e entrega de serviços.				C	C				I					A	C	R	R	R	R							
<b>APO11.06</b> Manter a melhoria continua.				C	R	C		R					C	C	A	R	R	R	R	R	R	R	R	R		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO11 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO11.01</b> Estabelecer um Sistema de gerenciamento de qualidade (SGQ). Estabelecer e manter um SGQ que fornece uma abordagem padrão, formal e continua do gerenciamento de qualidade para informação, habilitando tecnologia e processos de negócio que estão alinhados com os requisitos de negócio e gerenciamento de qualidade da organização.	Referência externa ao COBIT	• Sistema de qualidade corporativo	• Papéis, responsabilidades e direitos de decisão do SGQ	APO01.02 DSS06.03
			• Planos de gerenciamento da qualidade	BAI01.09
			• Resultados da efetividade da revisão do SGQ	BAI03.06

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Alinear, Planejar e Organizar

**APO11 Práticas de Processo, Entradas/Saídas e Atividades**

Atividades				
01 Garantir que o framework de controle de TI e os processos de TI e negócio incluem um padrão, abordagem contínua e formal para o gerenciamento da qualidade que está alinhado com os requisitos da organização. No framework de controle de TI e nos processos de TI e negócio, identificar requisitos de qualidade e critérios (ex.: baseado em requisitos legais e requisitos dos clientes).				
02 Definir papéis, tarefas, direitos decisórios e responsabilidades para o gerenciamento da qualidade na estrutura organizacional.				
03 Definir planos de gerenciamento de qualidade para processos importantes, Projetos ou objetivos alinhados com os critérios e políticas de gerenciamento de qualidade da organização. Registrar dados de qualidade.				
04 Monitorar e medir a efetividade e a aceitação do gerenciamento da qualidade, e melhorá-los quando necessário.				
05 Alinhar o gerenciamento da qualidade de TI com o Sistema de qualidade da organização, para incentivar uma abordagem contínua e padronizada para a qualidade.				
06 Obter informações da gestão e das partes interessadas internas e externas sobre a definição dos requisitos de qualidade e critérios de gerenciamento de qualidade.				
07 Comunicar efetivamente a abordagem (e.x.: através de programas de treinamento de qualidade formais e regulares).				
08 Revisar regularmente a continuidade da relevância, eficiência e efetividade dos processos específicos de gerenciamento da qualidade. Monitorar o alcance dos objetivos de qualidade.				

**Prática de Gestão**

<b>APO11.02 Definir e gerenciar os padrões de qualidade, práticas e procedimentos.</b> Identificar e manter requisitos, padrões, procedimentos e práticas para processos-chave, para guiar a organização no alcance do propósito do sistema de gerenciamento da qualidade acordado.	<b>Entradas</b>	<b>Saídas</b>		
	<b>De</b>	<b>Descrição</b>	<b>Descrição</b>	<b>Para</b>
BAI02.04	• Revisões de qualidade aprovadas	• Padrões de gerenciamento de qualidade	Todos APO Todos BAI Todos DSS Todos MEA	
Referência externa ao COBIT	• Boas práticas do segmento • Certificações de qualidade disponíveis			

**Atividades**

- 01 Definir os padrões de gerenciamento de qualidade, práticas e procedimentos, alinhados com os requisitos do framework de controle de TI. Utilizar as boas práticas do segmento na melhoria e ajuste das práticas de qualidade da organização.

- 02 Considerar os benefícios e custos das certificações de qualidade.

**Prática de Gestão**

<b>APO11.03 Focalizar o gerenciamento da qualidade nos clientes.</b> Direcionar o gerenciamento da qualidade para os clientes, para determinar seus requisitos e garantir alinhamento com as práticas de gerenciamento da qualidade.	<b>Entradas</b>	<b>Saídas</b>		
	<b>De</b>	<b>Descrição</b>	<b>Descrição</b>	<b>Para</b>
Referência externa ao COBIT	• Requisitos de qualidade dos clientes e do negócio	• Requisitos dos clientes para o gerenciamento da qualidade	APO08.05 APO09.03 BAI01.09	
		• Critérios de aceitação	BAI02.01 BAI02.02	
		• Revisão dos resultados da qualidade do serviço, incluindo o retorno dos clientes	APO08.05 APO09.05 BAI05.01 BAI07.07	

**Atividades**

- 01 Direcionar o gerenciamento da qualidade para os clientes, para determinar seus requisitos internos e externos e garantir alinhamento com os padrões e práticas de gerenciamento da qualidade. Definir e comunicar papéis e responsabilidades no que tange a resolução de conflitos entre o usuário/cliente e a organização de TI.

- 02 Gerenciar as necessidades e expectativas do negócio para cada processo de negócio, serviço operacional de TI e novas soluções, e manter seu critério de aceitação de qualidade. Coletar os critérios de aceitação de qualidade para inclusão nos Acordos de Níveis de Serviço (SLAs).

- 03 Comunicar os requisitos e expectativas dos clientes ao longo do negócio e da organização de TI.

- 04 Obter periodicamente a visão dos clientes sobre os processos de negócio e provisionamento de serviços e entrega de soluções de TI, para determinar o impacto sobre padrões e práticas de TO, e garantir que as expectativas do cliente são atingidas e postas em prática.

- 05 Monitorar e revisar regularmente os critérios de aceitação acordados do Sistema de gerenciamento da qualidade. Incluir feedback dos clientes, usuários e gestão. Responder a discrepâncias na revisão dos resultados para melhorar continuamente o SGQ.

- 06 Coletar o critério de aceitação da qualidade para inclusão nos Acordos de Níveis de Serviço (SLAs).

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO11 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO11.04 Realizar o monitoramento, controle e revisões da qualidade.</b> Monitorar a qualidade dos processos e serviços em uma base contínua, conforme definido no SGQ. Definir, planejar e implementar medições para monitorar a satisfação do cliente com a qualidade, bem como o valor que o SGQ proporciona. A informação coletada deveria ser utilizada pelo dono do processo para melhorar a qualidade.	BAI03.06	<ul style="list-style-type: none"> <li>Resultados, exceções e correções da revisão de qualidade</li> <li>Plano de garantia de qualidade</li> </ul>	<ul style="list-style-type: none"> <li>Resultados das revisões e auditorias de qualidade</li> </ul>	
	DSS02.07	<ul style="list-style-type: none"> <li>Status dos cumprimentos de requisições e relatório de tendências</li> <li>Status de incidente e relatório de tendências</li> </ul>	<ul style="list-style-type: none"> <li>Métricas e metas do processo de qualidade de serviço</li> </ul>	Todos APO Todos BAI Todos DSS Todos MEA

### Atividades

- 01 Monitorar a qualidade dos processos e serviços em uma base contínua e sistemática através da descrição, medição, análise, melhoria/engenharia e controle dos processos.
- 02 Preparar e conduzir as revisões de qualidade
- 03 Reportar os resultados de revisões e iniciar melhorias onde apropriado.
- 04 Monitorar a qualidade dos processos, bem como o valor que a qualidade proporciona. Garantir que a medição, monitoramento e registro de informações é utilizado pelo dono do processo para tomar ações preventivas e corretivas apropriadas.
- 05 Monitorar as métricas de qualidade direcionadoras das metas, alinhadas aos objetivos gerais de qualidade, cobrindo a qualidade de Projetos e serviços individuais.
- 06 Garantir que a gestão e os donos de processo revisem regularmente o desempenho do gerenciamento da qualidade, em comparação com as métricas de qualidade definidas.
- 07 Analisar os resultados do desempenho do gerenciamento da qualidade geral.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO11.05 Integrar o gerenciamento da qualidade em soluções para desenvolvimento e entrega de serviços.</b> Incorporar práticas relevantes de gerenciamento da qualidade na definição, monitoramento, reporte e gerenciamento contínuo de desenvolvimento de soluções e oferta de serviços.			<ul style="list-style-type: none"> <li>Resultados do monitoramento da qualidade da entrega de serviços e solução</li> </ul>	APO08.05 APO09.04 BAI07.08
			<ul style="list-style-type: none"> <li>Causas-raiz de falhas na entrega de qualidade:</li> </ul>	APO08.02 APO09.04 BAI07.08 MEA02.04 MEA02.07 MEA02.08

### Atividades

- 01 Integrar práticas de gerenciamento de qualidade nos processos e práticas de desenvolvimento de soluções.
- 02 Monitorar continuamente os níveis de serviço, e incorporar práticas de gerenciamento da qualidade nos processos e práticas de entrega de serviços.
- 03 Identificar e documentar causas raiz para não-conformidade, e comunicar descobertas para a gestão de TI e outras partes interessadas de forma oportuna para habilitar a tomada de ações de remediação. Onde apropriado, realizar revisões de acompanhamento.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO11.06 Manter a melhoria contínua. Manter e comunicar regularmente um plano geral de qualidade que promova a melhoria contínua.</b> Isso deve incluir a necessidade e os benefícios da melhoria contínua. Coletar e analisar os dados do SGQ, e melhorar sua efetividade. Corrigir não-conformidades para prevenir a recorrência. Promover uma cultura de qualidade e melhoria contínua.			<ul style="list-style-type: none"> <li>Comunicações sobre melhoria contínua e boas práticas</li> </ul>	Todos APO Todos BAI Todos DSS Todos MEA
			<ul style="list-style-type: none"> <li>Exemplos de boas práticas a serem compartilhados</li> </ul>	Todos APO Todos BAI Todos DSS Todos MEA
			<ul style="list-style-type: none"> <li>Resultados da comparação das revisões de qualidade</li> </ul>	Todos APO Todos BAI Todos DSS Todos MEA

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**APO11 Práticas de Processo, Entradas/Saídas e Atividades**

Atividades
01 Manter e comunicar regularmente a necessidade e os benefícios da melhoria contínua.
02 Estabelecer uma plataforma para compartilhar boas práticas e para coletar informações sobre defeitos e erros, para proporcionar aprendizado através deles.
03 Identificar exemplos recorrentes de defeitos de qualidade, determinar suas causas raiz, avaliar seus impactos e resultados e ações de melhoria acordadas com os times de entrega de projetos e serviços.
04 Identificar exemplos de processos de entrega de qualidade de excelência, que possam beneficiar outros serviços ou Projetos, e compartilhá-los com os times de entrega de Projetos e serviços para incentivar a melhoria.
05 Promover uma cultura de qualidade e melhoria contínua.
06 Estabelecer um ciclo de feedback entre gerenciamento da qualidade e gerenciamento de problemas.
07 Fornecer treinamento aos colaboradores nos métodos e ferramentas de melhoria contínua.
08 Comparar os resultados das revisões de qualidade com dados históricos internos, diretrizes do segmento, padrões e dados de tipos de organizações similares.

**APO11 Orientação Relacionada**

Padrão Relacionado	Referência Detalhada
ISO/IEC 9001:2008	

# COBIT® 5 : HABILITANDO PROCESSOS

APO12 Gerenciar Riscos	Área: Gestão Dominio: Alinhar, Planejar e Organizar
<b>Descrição do Processo</b> Identificar, avaliar e reduzir continuamente o risco relacionado a TI dentro dos níveis de tolerância definidos pela gestão executiva da organização.	
<b>Declaração de Propósito do Processo</b> Integrar o gerenciamento do risco organizacional relacionado a TI com o risco organizacional em geral, e balancear os custos e benefícios do gerenciamento do risco organizacional relacionado a TI.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo de não conformidade de TI, incluindo liquidações e multas, e o impacto da perda de reputação</li> <li>Número de não conformidades relacionadas a TI reportadas à alta gestão ou que causaram comentário público ou constrangimento</li> <li>Número de não conformidades relacionadas a acordos contratuais com provedores de serviços de TI</li> <li>Cobertura das avaliações de conformidade.</li> </ul>
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Percentual de processos de negócio críticos, serviços de TI e programas de negócio habilitados por TI cobertos pela avaliação de risco</li> <li>Número de incidentes relevantes relacionados a TI que não foram identificados pela avaliação de risco</li> <li>Percentual de avaliações de risco organizacional que incluem riscos relacionados a TI</li> <li>Frequência de atualização do perfil de risco</li> </ul>
06 Transparência dos custos, benefícios e riscos de TI	<ul style="list-style-type: none"> <li>Percentual de casos de negócio de investimento com custos e benefícios relacionados à TI esperados claramente definidos e aprovados</li> <li>Percentual de serviços de TI com custos operacionais e benefícios esperados claramente definidos e aprovados</li> <li>Pesquisa de satisfação com partes interessadas chave, a respeito do nível de transparência, compreensão e precisão das informações financeiras de TI</li> </ul>
10 Segurança da informação, infraestrutura de processamento e aplicativos	<ul style="list-style-type: none"> <li>Número de incidentes de segurança que causaram perda financeira, parada do negócio ou constrangimento público</li> <li>Número de serviços de TI com requisitos de segurança excepcionais</li> <li>Tempo para conceder, alterar e remover privilégios de acesso, comparado aos níveis de serviço acordados</li> <li>Frequência das avaliações de segurança, comparados com os padrões e guias mais atuais.</li> </ul>
13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	<ul style="list-style-type: none"> <li>Número de programas/projetos no prazo e dentro do orçamento</li> <li>Percentual de partes interessadas satisfeitas com a qualidade dos programas/projetos</li> <li>Número de programas com necessidade de retrabalho, devido a defeitos de qualidade</li> <li>Custo da manutenção de aplicação x custo geral de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Risco relacionado a TI é identificado, analisado, gerenciado e reportado.	<ul style="list-style-type: none"> <li>Grau de visibilidade e reconhecimento do ambiente atual</li> <li>Número de eventos de perda com características chave documentadas em repositórios</li> </ul>
02 Um perfil de risco completo e atual existe.	<ul style="list-style-type: none"> <li>Percentual de processos de negócio chave incluídos no perfil de risco</li> <li>Abrangência de atributos e valores no perfil de risco</li> </ul>
03 Todas as ações de gerenciamento de risco significativas são gerenciadas e estão sob controle.	<ul style="list-style-type: none"> <li>Percentual de propostas de gerenciamento de risco rejeitadas devido a falha na consideração de outros riscos relacionados</li> <li>Número de incidentes significativos não identificados e incluídos no portfólio de gerenciamento de risco</li> </ul>
04 Ações de gerenciamento de risco são efetivamente implementadas.	<ul style="list-style-type: none"> <li>Percentual de planos de ação de risco de TI executados conforme foram desenhados</li> <li>Número de medições que não reduzem o risco residual</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO12 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>APO12.01</b> Coletar dados	I			R		R	R	R	I	C	C	A	R	R	R	R	R	R	R	R	R	R	R	R	R	
<b>APO12.02</b> Analisar risco	I			R		C	R	C	I	R	R	A	C	C	C	C	C	C	C	C	C	C	C	C	C	
<b>APO12.03</b> Manter um perfil de risco	I			R		C	A	C	I	R	R	R	C	C	C	C	C	C	C	C	C	C	C	C	C	
<b>APO12.04</b> Articular risco	I			R		C	R	C	I	C	C	A	C	C	C	C	C	C	C	C	C	C	C	C	C	
<b>APO12.05</b> Definir um portfolio de ações de gerenciamento de risco	I			R		C	A	C	I	C	C	R	C	C	C	C	C	C	C	C	C	C	C	C	C	
<b>APO12.06</b> Responder ao risco	I			R		R	R	R	I	C	C	A	R	R	R	R	R	R	R	R	R	R	R	R	R	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO12 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO12 Coletar dados</b> Identificar e coletar dados relevantes para habilitar a efetiva identificação do risco relacionado a TI, análise e reporte.	EDM03.01	• Avaliação das atividades de gerenciamento do risco	• Dados sobre o ambiente operacional relacionados ao risco	Interno
	EDM03.02	• Processo para gerenciamento da medição do risco aprovados • Objetivos-chave a serem monitorados pelo gerenciamento do risco • Políticas de gerenciamento do risco	• Dados sobre eventos de risco e fatores contribuintes	Interno
	APO02.02	• Lacunas e riscos relacionados às capacidades atuais	• Fatores e problemas de risco emergentes	EDM03.01 APO01.03 APO02.02
	APO02.05	• Iniciativas de avaliação do risco		
	APO10.04	• Risco de entrega do fornecedor identificado		
	DSS02.07	• Status de incidentes e relatório de tendências		

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO12 Práticas de Processo, Entradas/Saídas e Atividades

Atividades			
01 Estabelecer e manter um método para a coleta, classificação e análise dos dados relacionados ao risco de TI, acomodando múltiplos tipos de eventos, múltiplas categorias de risco de TI e fatores de risco.			
02 Registrar dados relevantes sobre o ambiente operacional interno e externo da organização, que possa exercer um papel significativo no gerenciamento do risco.			
03 Pesquisar e analisar os dados históricos do risco relacionado a TI e experiências de perda, a partir de dados e tendências externas disponíveis, pares através de logs de evento do segmento de negócio, bases de dados, e acordos do segmento para divulgação de eventos comuns.			
04 Registrar dados sobre eventos de risco que tenham causado ou podem causar impactos para a habilitação do benefício/valor de TI, programas de TI e entrega de projetos, e/ou operações de TI e entrega de serviços. Coletar dados relevantes de questões relacionados, incidentes, problemas e investigações.			
05 Para classes similares de eventos, organizar os dados coletados e destacar fatores contribuintes. Determinar fatores contribuintes comuns dentre os múltiplos eventos.			
06 Determinar as condições específicas que existiram ou estiveram ausentes quando os eventos de risco ocorreram, e a forma como as condições afetaram a frequência de eventos e a extensão da perda.			
07 Realizar análise periódica de evento e fator de risco para identificar problemas novos ou emergentes, e para obter a compreensão dos fatores de risco internos e externos associados.			

Prática de Gestão	Entradas	Saídas	
<b>APO12.02 Analisar Risco.</b> Desenvolver informações úteis para suportar as decisões de risco que levam em conta a relevância para o negócio dos fatores de risco.	<p><b>De</b></p> <p>DSSD4.02</p> <ul style="list-style-type: none"> <li>Análises de impacto ao negócio</li> </ul> <p>DSSS5.01</p> <ul style="list-style-type: none"> <li>Avaliações de potenciais ameaças</li> </ul> <p>Referência externa ao COBIT</p> <ul style="list-style-type: none"> <li>Avisos de ameaças</li> </ul>	<p><b>Descrição</b></p> <ul style="list-style-type: none"> <li>Escopo dos esforços de análise de risco</li> </ul> <p>Cenários de risco de TI</p> <p>Resultados de análise de risco</p>	<p><b>Para</b></p> <p>Interno</p> <p>Interno</p> <p>EDM03.03 APO01.03 APO02.02 BAI01.10</p>

Atividades			
01 Definir a largura e profundidade apropriados para os esforços de análise de risco, considerando todos os fatores de risco e a criticidade para o negócio dos ativos. Estabelecer o escopo da análise de risco depois de realizar uma análise de custo-benefício.			
02 Construir e atualizar regularmente cenários de riscos de TI, incluindo cenários compostos de tipos de ameaças de cascataamento e/ou coincidentes, e desenvolver expectativas para atividades de controle específicas, capacidades de detecção e outras medidas de resposta.			
03 Estimar a frequência e magnitude da perda ou ganho associado aos cenários de risco de TI. Levar em consideração todos os fatores de risco aplicáveis, avaliar os controles operacionais conhecidos e estimar os níveis de risco residual.			
04 Comparar risco residual a tolerância ao risco aceitável, e identificar exposições que possam requerer uma resposta ao risco.			
05 Analisar o custo-benefício das potenciais opções de resposta ao risco, como evitar, reduzir/mitigar, transferir/compartilhar, e aceitar e explorar/assumir. Propor a resposta ao risco otimizada.			
06 Especificar requisitos de alto nível para projetos ou programas que vão implementar a resposta ao risco selecionada. Identificar requisitos e expectativas para os controles-chave apropriados para respostas de mitigação de risco.			
07 Validar os resultados da análise de risco antes de usá-los para tomada de decisão, confirmando que a análise está alinhada com os requisitos da corporação, e verificando que as estimativas foram devidamente calibradas e minuciosamente examinadas para o propósito.			

Prática de Gestão	Entradas	Saídas	
<b>APO12.03 Manter o perfil do risco</b> Manter um inventário de risco conhecido e atributos de risco (incluindo frequência esperada, impacto potencial e respostas) e dos recursos relacionados, capacidades e atividades de controle atuais.	<p><b>De</b></p> <p>EDM03.01</p> <ul style="list-style-type: none"> <li>Níveis de tolerância de risco aprovados</li> <li>Guia de apetite de risco</li> </ul> <p>APO10.04</p> <ul style="list-style-type: none"> <li>Risco de entrega do fornecedor identificado</li> </ul> <p>DSSS5.01</p> <ul style="list-style-type: none"> <li>Avaliações de ameaças potenciais</li> </ul>	<p><b>Descrição</b></p> <ul style="list-style-type: none"> <li>Cenários de risco documentados por linha de negócio e função</li> </ul> <p>Perfil de risco agrupado, incluindo status de ações de gerenciamento de risco</p>	<p><b>Para</b></p> <p>Interno</p> <p>EDM03.02 APO02.02</p>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**APO12 Práticas de Processo, Entradas/Saídas e Atividades**

Atividades				
01 Inventariar processos de negócio, incluindo pessoal de suporte, aplicações, infraestrutura, instalações, registros manuais críticos, fornecedores e provedores externos, e documentar a dependência dos processos de gerenciamento de serviços de TI e recursos de infraestrutura de TI				
02 Determinar e acordar quais serviços de TI e recursos de infraestrutura de TI são essenciais para manter a operação dos processos de negócio. Analisar dependências e identificar elos fracos.				
02 Agrupar cenários atuais de risco por categoria, linha de negócio e área funcional.				
03 Regularmente, coletar todas as informações de perfil de risco e consolida-las em um perfil de risco agrupado.				
04 Com base em todos os dados de perfil de risco, definir um grupo de indicadores de risco que permitam a rápida identificação e monitoramento do risco atual e tendências de risco.				
05 Coletar informações sobre eventos de risco de TI que se concretizaram, para inclusão no perfil de risco de TI da organização.				
06 Coletar informações sobre o status do plano de ação de risco, para inclusão no perfil de risco de TI da organização.				

Prática de Gestão	Entradas	Saídas	
	De	Descrição	Para
<b>APO12.04 Articular o risco.</b> Fornecer informação para o estado atual de exposições relacionadas a TI e oportunidades em tempo hábil para todas as partes interessadas requeridas, para resposta apropriada.		<ul style="list-style-type: none"> <li>Análise de risco e perfil de risco reportados para as partes interessadas</li> </ul>	EDM03.03 EDM05.02 APO10.04 MEA02.08
		<ul style="list-style-type: none"> <li>Resultados das avaliações de risco de terceiros</li> </ul>	EDM03.03 APO10.04 MEA02.01
		<ul style="list-style-type: none"> <li>Oportunidades de aceitação de riscos maiores</li> </ul>	EDM03.03

Atividades				
01 Reportar os resultados da análise de risco a todas as partes interessadas afetadas, formatando-os de forma útil para suportar as decisões da organização. Onde for possível, incluir probabilidades e escalas de prejuízo ou ganho ao longo dos níveis de confiança que habilitam a gestão, para balancear o risco sobre o retorno.				
02 Fornecer aos tomadores de decisão um entendimento do pior cenário e do mais provável, exposições e reputação significativa, considerações legais ou regulatórias.				
03 Reportar o perfil de risco atual a todas as partes interessadas, incluindo a efetividade do processo de gerenciamento de risco, efetividade do controle, lacunas, inconsistências, redundâncias, status de remediação e seus impactos no perfil de risco.				
04 Revisar os resultados das avaliações objetivas de fornecedores, auditoria interna e revisões de garantia de qualidade, e mapeá-los para o perfil de risco. Revisar lacunas identificadas e exposições para determinar a necessidade de uma análise de risco adicional.				
05 Periodicamente, para áreas com risco relativo e paridade na capacidade de risco, identificar as oportunidades relacionadas a TI que permitiriam o aceite de um risco maior e incrementem o crescimento e o retorno.				

Prática de Gestão	Entradas	Saídas	
	De	Descrição	Saída
<b>APO12.05 Definir um portfolio de ações de gerenciamento de risco</b> Gerenciar oportunidades para reduzir o risco em um nível aceitável como um portfólio.		<ul style="list-style-type: none"> <li>Propostas de projeto para redução do risco</li> </ul>	APO02.02 APO13.02

Atividades				
01 Manter um inventário de atividades de controle que estão estabelecidas para gerenciar o risco, e que habilitem a ser assumido em linha com a tolerância e o apetite de risco. Classificar atividades de controle e mapeá-las para as declarações de risco de TI específicas, e aglomerações de risco de TI.				
02 Determinar quando cada entidade organizacional monitora o risco e aceita a prestação de contas por operar dentro de seu portfólio e níveis de tolerância individuais.				
03 Definir um grupo balanceado de propostas de projeto, desenhadas para reduzir o risco e/ou projetos que habilitem oportunidades estratégicas para a organização, considerando custo/benefício, efeito no perfil de risco atual e regulações.				

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## APO12 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO12.06 Responder ao risco.</b> Responder em tempo hábil com medições efetivas para limitar a magnitude dos prejuízos relacionados a eventos de TI.	EDM03.03	<ul style="list-style-type: none"> <li>• Ações corretivas para endereçar desvios no gerenciamento de risco</li> </ul>	<ul style="list-style-type: none"> <li>• Planos de resposta a incidentes relacionados a risco</li> <li>• Comunicação do impacto do risco</li> <li>• Causas raiz relacionadas ao risco</li> </ul>	DSS02.05 APO01.04 APO08.04 DSS04.02 DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08
<b>Atividades</b>				
<p>01 Preparar, manter e testar planos que documentem passos específicos a serem tomados quando um evento de risco puder causar um incidente operacional ou de desenvolvimento significativo, com sérios impactos ao negócio. Garantir que os planos possuam fluxos de escalação através da organização.</p> <p>02 Categorizar incidentes, e comparar a exposição atual com os limites de tolerância de risco. Comunicar os impactos de negócio para tomada de decisão como parte de um perfil de risco atualizado e reportado.</p> <p>03 Aplicar o plano de resposta apropriado para minimizar o impacto quando o risco de incidentes ocorrer.</p> <p>04 Examinar eventos adversos/prejuízos e oportunidades perdidas passadas, e determinar as causas raiz. Comunicar a causa raiz, requisitos de resposta de risco adicional e melhorias no processo para tomada de decisão apropriada, e garantir que a causa, requisitos de resposta e melhoria de processos estão incluídas no processo de governança de risco.</p>				

## APO12 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 27001:2005	Sistemas de Gerenciamento de Segurança da Informação – Requisitos, Seção 4
ISO/IEC 27002:2011	
ISO/IEC 31000	06 Processos para Gerenciamento de Risco

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO13 Gerenciar Segurança		Área: Gestão Dominio: Alinhar, Planejar e Organizar
Descrição do Processo		
Definir, operar e monitorar um Sistema para gerenciamento de segurança da informação.		
Declaração de Propósito do Processo		
Manter o impacto e a ocorrência de incidentes de segurança da informação dentro dos níveis de apetite de risco da organização		
O processo suporta a realização de um conjunto primário de objetivos de TI:		
Objetivos de TI	Métricas Relacionadas	
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo da não conformidade de TI, incluindo liquidações e multas, e o impacto da perda de reputação</li> <li>Número de não conformidades relacionadas a TI reportadas à alta gestão ou que causaram comentário público ou constrangimento</li> <li>Número de não conformidades relacionadas a acordos contratuais com provedores de serviços de TI</li> <li>Cobertura das avaliações de conformidade</li> </ul>	
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Percentual de processos de negócio críticos, serviços de TI e programas de negócio relacionados a TI cobertos pela avaliação de risco</li> <li>Número de incidentes relevantes relacionados a TI que não foram identificados pela avaliação de risco</li> <li>Percentual de avaliações de risco organizacional incluindo riscos relacionados a TI</li> <li>Frequência de atualização do perfil de risco</li> </ul>	
06 Transparência dos custos, benefícios e riscos de TI	<ul style="list-style-type: none"> <li>Percentual de casos de negócios de investimento com custos e benefícios relacionados a TI claramente definidos e aprovados</li> <li>Percentual de serviços de TI com custos operacionais e benefícios esperados claramente definidos e aprovados</li> <li>Pesquisa de satisfação com partes interessadas chave, a respeito do nível de transparência, compreensão e precisão das informações financeiras de TI</li> </ul>	
10 Segurança da informação, infraestrutura de processamento e aplicativos	<ul style="list-style-type: none"> <li>Número de incidentes de segurança que causaram perda financeira, parada do negócio ou constrangimento público</li> <li>Número de serviços de TI com requisitos de segurança excepcionais</li> <li>Tempo para conceder, alterar e remover privilégios de acesso, comparado aos níveis de serviço acordados</li> <li>Frequência das avaliações de segurança, comparadas com os padrões e guias mais atuais.</li> </ul>	
14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	<ul style="list-style-type: none"> <li>Nível de satisfação dos usuários de negócio com a qualidade e oportunidade (ou disponibilidade) de informações de gerenciamento</li> <li>Número de incidentes em processos de negócio causados pela não disponibilidade da informação</li> <li>Taxa e dimensão de decisões de negócio errôneas onde a indisponibilidade de informação ou a informação errada foi um fator chave</li> </ul>	
Objetivos e Métricas do Processo		
Objetivo do Processo	Métricas Relacionadas	
01 Um Sistema que considera e endereça efetivamente os requisites de segurança da informação da organização está disponível.	<ul style="list-style-type: none"> <li>Número de papéis chave de segurança claramente definidos</li> <li>Número de incidentes de segurança relatados</li> </ul>	
02 Um plano de segurança tem sido estabelecido, aceito e comunicado por toda a organização	<ul style="list-style-type: none"> <li>Nível de satisfação das partes interessadas com o plano de segurança por toda a organização</li> <li>Número de soluções de segurança que se desviam do plano</li> <li>Número de soluções de segurança que se desviam da arquitetura da organização</li> </ul>	
03 Soluções de segurança da informação são implementadas e operadas consistentemente por toda a organização	<ul style="list-style-type: none"> <li>Número de serviços com alinhamento confirmado com o plano de segurança</li> <li>Número de incidentes de segurança causados pela não aderência ao plano de segurança</li> <li>Número de soluções desenvolvidas com alinhamento confirmado com o plano de segurança</li> </ul>	

# COBIT<sup>®</sup> 5: HABILITANDO PROCESSOS

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

APO13 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO13.01 Estabelecer e manter um Sistema de Gerenciamento de Segurança da Informação (ISMS).</b>  Estabelecer e manter um ISMS que forneça um padrão, abordagem formal e contínua para gerenciamento de segurança para informação, habilitando tecnologia segura e processos de negócios que estão alinhados com os requisitos do negócio e gerenciamento de segurança da organização.	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>• Abordagem de segurança da organização</li> </ul>	<ul style="list-style-type: none"> <li>• Política do ISMS</li> <li>• Declaração de escopo do ISMS</li> </ul>	Interno  APO01.02 DSS06.03
<b>Atividades</b>				
01 Definir o escopo e limites do ISMS, em termos de características da organização, sua disposição, localização, ativos e tecnologia. Incluir detalhes de, e justificativa para quaisquer exclusões do escopo.				
02 Definir um ISMS de acordo e alinhado com a política da organização, sua disposição, localização, ativos e tecnologia.				
03 Alinhar o ISMS com a abordagem da organização geral para o gerenciamento de segurança.				
04 Obter autorização da gestão para implementar e operar ou alterar o ISMS.				
05 Preparar e manter uma declaração de aplicabilidade que descreva o escopo do ISMS.				
06 Definir e comunicar os papéis e responsabilidades de segurança da informação				
07 Comunicar a abordagem ISMS.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

APO13 Práticas de Processo, Entradas/Saídas e Atividades				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>APO13.02 Definir e gerenciar um plano de tratamento de risco de segurança da informação.</b> Manter um plano de segurança da informação que descreva como o risco de segurança da informação está sendo gerenciado e alinhado com a estratégia e arquitetura corporativa. Garantir que as recomendações para implementação de melhorias de segurança são baseadas em casos de negócios aprovados, e implementados como parte integral do desenvolvimento de soluções e serviços, sendo assim, operando como parte integral da operação de negócio.	APO02.04		• Plano de tratamento do risco de segurança	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	APO03.02	• Descrição do baseline e definição da arquitetura	• Casos de negócios de segurança da informação	APO02.05
	APO12.05	• Propostas de projeto para redução de risco		
Atividades				
01 Formular e manter um plano de tratamento de risco de segurança da informação alinhado com os objetivos estratégicos e arquitetura corporativa. Garantir que o plano identifica as práticas de gestão apropriadas e otimizadas e soluções de segurança, com recursos associados, responsabilidades e prioridades para gerenciar o risco de segurança da informação identificado.				
02 Manter como parte da arquitetura corporativa, um inventário de componentes de solução que será utilizado para gerenciar o risco relacionado à segurança.				
03 Desenvolver propostas para implementar o plano de tratamento de risco de segurança da informação, suportado por casos de negócios aplicáveis, que incluem a consideração de financiamento e alocação de papéis e responsabilidades.				
04 Fornecer entrada para o desenho e desenvolvimento de práticas de gerenciamento e soluções selecionadas do plano de tratamento de risco de segurança da informação.				
05 Definir como medir a efetividade das práticas de gestão selecionadas e especificar como essas medições são usadas para avaliar a efetividade para produzir resultados comparáveis e reproduzíveis.				
06 Recomendar treinamento de segurança da informação e programas de conscientização.				
07 Integrar o planejamento, desenho, implementação e monitoramento dos procedimentos de segurança da informação e outros controles capazes de habilitar prevenção imediata, detecção de eventos de segurança e resposta a incidentes de segurança				
Prática de Gestão				
<b>APO13.03 Monitorar e revisar o ISMS.</b> Manter e comunicar regularmente a necessidade e os benefícios de segurança da informação contínua. Coletar e analisar dados sobre o ISMS, e melhorar a efetividade do ISMS. Corrigir não-conformidades para prevenir recorrências. Promover uma cultura de segurança e melhoria contínua.	• De	• Descrição	• Descrição	• Para
	DSS02.02	• Requisições de Serviço e Incidentes classificados e priorizados	• Relatórios de auditoria do ISMS	MEA02.01
			• Recomendações para melhoria do ISMS	Interno
Atividades				
01 Realizar revisões regulares da efetividade do ISMS, incluindo o alcance das políticas e objetivos do ISMS, e revisão das práticas de segurança. Leva em conta os resultados das auditorias de segurança, incidentes, resultados de medições de efetividade, sugestões e feedback de todas as partes interessadas.				
02 Conduzir auditorias ISMS internas em intervalos planejados				
02 Realizar uma revisão do gerenciamento do ISMS periodicamente para garantir que o escopo permanece adequado e as melhorias nos processos do ISMS são identificadas				
04 Prover entrada para manutenção dos planos de segurança para levar em conta as descobertas do monitoramento e atividades de revisão				
05 Registrar ações e eventos que poderiam gerar impacto na efetividade ou desempenho do ISMS				

APO13 Orientação Relacionada	
Padrão Relacionado	Referência Detalhada
ISO/IEC 27001:2005	Sistemas de gerenciamento de segurança da informação – Requisitos, seção 4
ISO/IEC 27002:2011	
National Institute of Standards and Technology (NIST) SP800-53 Rev 1	Controles de Segurança Recomendados pelo Sistema de Informações Federais dos EUA
ITIL V3 2011	Desenho de serviço, 4.7 Gerenciamento de Segurança da Informação

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

Página intencionalmente deixada em branco

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

# CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI)

- 01 Gerenciar programas e projetos
- 02 Gerenciar definição de requisitos
- 03 Gerenciar identificação e desenvolvimento de soluções
- 04 Gerenciar disponibilidade e capacidade
- 05 Gerenciar capacidade da mudança organizacional
- 06 Gerenciar mudanças
- 07 Gerenciar aceitação e transição da mudança
- 08 Gerenciar conhecimento
- 09 Gerenciar ativos
- 10 Gerenciar configuração

# COBIT® 5 : HABILITANDO PROCESSOS

BAI01 Gerenciar programas e projetos	Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Gerenciar todos os programas e projetos do portfólio de investimentos alinhados às estratégias corporativas e de forma coordenada. Iniciar, planejar, controlar, e executar programas e projetos, e finalizar com revisão pós-implantação.	
<b>Declaração de Propósito do Processo</b> Identificar os benefícios de negócios e reduzir os riscos de atrasos inesperados, custos e perda de valor por meio do aprimoramento de comunicação e envolvimento de negócios e usuários finais, assegurando o valor e qualidade dos entregáveis de projetos e maximizando a contribuição deles para o portfólio de investimentos e serviços.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de metas e requisitos estratégicos corporativos suportados por metas estratégicas de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio de programas e serviços planejados</li> <li>Percentual de direcionadores de valor de TI definido aos direcionadores de valor do negócio</li> </ul>
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Percentual de processos de negócios críticos, serviços de TI e programas de negócios para TI cobertos por avaliação de riscos</li> <li>Número de incidentes significativos de TI não identificados na avaliação de riscos</li> <li>Percentual de avaliações de riscos corporativos incluindo riscos relacionados a TI</li> <li>Frequência de atualização do perfil de risco</li> </ul>
05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	<ul style="list-style-type: none"> <li>Percentual de investimentos habilitados por TI no qual os benefícios ganhos são monitorados por meio de todo o ciclo de vida econômico.</li> <li>Percentual de serviços de TI no qual benefícios esperados são atingidos</li> <li>Percentual de investimentos habilitados por TI no qual os benefícios esperados são atingidos ou ultrapassados</li> </ul>
13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos.	<ul style="list-style-type: none"> <li>Quantidade de programas/projetos dentro do prazo e orçamento</li> <li>Percentual de partes interessadas satisfeitas com a qualidade do programa/projeto</li> <li>Quantidade de programas necessitando de significativo trabalho por falhas de qualidade</li> <li>Custo de manutenção de aplicação vs. custo geral de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 As partes interessadas relevantes estão envolvidas nos programas e projetos	<ul style="list-style-type: none"> <li>Percentual de partes interessadas efetivamente envolvidas</li> <li>Nível de satisfação das partes interessadas com o envolvimento.</li> </ul>
02 O escopo e os resultados dos programas e projetos são viáveis e alinhados com os objetivos.	<ul style="list-style-type: none"> <li>Percentual de partes interessadas que aprovam as necessidades corporativas, escopo, resultados planejados e nível de risco do projeto</li> <li>Percentual de projetos realizados sem casos de negócios aprovados</li> </ul>
03 Os resultados esperados dos planos programas e projetos são suscetíveis de atingimento.	<ul style="list-style-type: none"> <li>Percentual de atividades alinhadas ao escopo e aos resultados esperados.</li> <li>Percentual de programas ativos realizados sem mapas de valor do programa válidos e atualizados</li> </ul>
04 As atividades dos programas e projetos são executadas de acordo com os planos.	<ul style="list-style-type: none"> <li>Frequência de revisão do status</li> <li>Percentual de desvios do plano endereçado</li> <li>Percentual das partes interessadas assinando as revisões de mudança de fase.</li> </ul>
05 Há recursos suficientes aos programas e projetos para realizar as atividades de acordo com os planos.	<ul style="list-style-type: none"> <li>Quantidade de problemas de recursos (ex. competência, capacidade)</li> </ul>
06 Os benefícios esperados dos programas e projetos são atingidos e reconhecidos.	<ul style="list-style-type: none"> <li>Percentual de atingimento dos benefícios previstos</li> <li>Percentual de resultados com aceitação na primeira avaliação</li> <li>Nível de satisfação das partes interessadas manifestadas durante a revisão de finalização</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI01 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>BAI01.01</b> Mantenha uma abordagem padrão para a gestão de programas e projetos.	I	A	C	C	R	R			C	C					C	C	R		C	C	C	C	C	C	C	
<b>BAI01.02</b> Inicie um programa.	I	R	C	C	A	R	R	R	R									C	C	C	C	C	C	C	C	
<b>BAI01.03</b> Gerencie a participação das partes interessadas.	A	C	R	R	R	C	R	I	I									R	C	C	C	C	C	C	C	
<b>BAI01.04</b> Desenvolva e mantenha o plano do programa.	C	C	A	C		R	R	R	C						C	C	C	C	C	C	C	C	C	C		
<b>BAI01.05</b> Lance e execute o programa.	C	C	A	R		R	R	I	C						C	C	R	R	R	R	C	C	C	C		
<b>BAI01.06</b> Monitore, controle e reporte os resultados do programa.			A	C	I	R	R	R	C						C	R	R	C	C		C					
<b>BAI01.07</b> Lance e inicie projetos dentro de um programa.			R	R	I	A	R								C	C	R	C	C	C	C	C	C	C		
<b>BAI01.08</b> Planeje os projetos.			C	I	A	R									C	C	C	C	C	C	C	C	C	C		
<b>BAI01.09</b> Gerencie a qualidade dos programas e dos projetos.			R	R	I	A	R		C						C	C	C	C	R	C	C	C	C	C		
<b>BAI01.10</b> Gerencie os riscos dos programas e dos projetos.			R	R	I	A	R		C						C	C	C	C	R	C	C	C	C	C		
<b>BAI01.11</b> Monitore e controle os projetos.			I	R	I	A	R		C						C	R	C	C	R	C	C	C	C	C		
<b>BAI01.12</b> Gerencie recursos dos projetos e pacotes de trabalho.			R	I	A	R		C							C	C	C	C	R	C	C	C	C	C		
<b>BAI01.13</b> Finalize um projeto ou iteração.			C	C	I	A	R		C						C	C	C	C	C	C	C	C	C	C		
<b>BAI01.14</b> Finalize um programa.	I	C	C	C	A	R	I	R	R							R	C	C	C		C	C	C	C		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

# COBIT® : HABILITANDO PROCESSOS

## BAI01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.01 Mantenha uma abordagem padrão para a gestão de programas e projetos.</b> Manter uma abordagem padronizada para gestão de programas e projetos que permita a avaliação da governança e gestão e tomada de decisão e atividades de gestão de entrega focados em alcançar valor e metas (requisitos, riscos, custos, cronograma, qualidade) para o negócio de forma consistente.	EDM02.02	<ul style="list-style-type: none"> <li>• Requisitos para revisões de mudança de fase.</li> </ul>	<ul style="list-style-type: none"> <li>• Abordagens do programa e projetos atualizados</li> </ul>	Interno
	EDM02.03	<ul style="list-style-type: none"> <li>• Ações para aprimorar a entrega de valor</li> </ul>		
	APO03.04	<ul style="list-style-type: none"> <li>• Requisitos de governança de arquitetura</li> <li>• Descrições da fase de implementação</li> </ul>		
	APO05.05	<ul style="list-style-type: none"> <li>• Portfólios atualizados de programas, serviços e ativos</li> </ul>		
	APO10.04	<ul style="list-style-type: none"> <li>• Riscos mapeados de entrega dos fornecedores</li> </ul>		

### Atividades

01 Manter e reforçar uma abordagem padrão para gestão dos programas e projetos alinhada ao ambiente específico corporativo e com as boas práticas baseadas em processos definidos e o uso da tecnologia apropriada. Assegure que a abordagem cubra todo o ciclo de vida e disciplinas a serem seguidas, incluindo a gestão de escopo, recursos, riscos, custos, qualidade, tempo, comunicação, atuação das partes envolvidas, compras, controle de mudanças, integração e concepção do benefício.

02 Atualizar a abordagem de gestão dos programas e projetos baseado nas lições aprendidas da utilização.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.02 Inicie um programa.</b> Iniciar um programa para confirmar os benefícios esperados e obter autorização para prosseguir. Isso inclui um acordo sobre o patrocínio do programa a confirmar o mandato do programa através da aprovação do plano de negócios conceitual, designando o conselho do programa ou membros do comitê produzindo o resumo, revisando e atualizando o caso de negócios, desenvolvendo um plano de benefícios obtidos, e obter aprovação das patrocinadores para prosseguir.	APO03.04	<ul style="list-style-type: none"> <li>• Descrições da fase de implementação</li> <li>• Necessidade de recursos</li> </ul>	<ul style="list-style-type: none"> <li>• Caso de negócio para o conceito do programa</li> <li>• Instruções e ordens do programa</li> <li>• Plano de obtenção dos benefícios do programa</li> </ul>	APO05.03 APO05.03 APO05.03 APO06.05
	APO05.03	<ul style="list-style-type: none"> <li>• Caso de negócio do programa</li> </ul>		
	APO07.03	<ul style="list-style-type: none"> <li>• Matriz de habilidades e competências</li> </ul>		
	BAI05.02	<ul style="list-style-type: none"> <li>• Visão e objetivos comuns</li> </ul>		

### Atividades

01 Acordar com o patrocínio do programa e nomear uma diretoria/comitê com membros com interesses estratégicos no programa, que tenham responsabilidade pelas tomadas de decisão de investimento, e que serão significativamente impactados pelo programa e serão necessários por permitir a entrega da mudança.

02 Confirmar o mandato do programa com os patrocinadores e partes interessadas. Articular os objetivos estratégicos ao programa, as estratégias potenciais de entrega, melhoria e benefícios que são esperados ao resultado, e como o programa se encaixa com outras iniciativas.

03 Desenvolver um caso de negócio detalhado ao programa, se necessário. Envolver todas as partes interessadas para desenvolver e documentar o entendimento completo dos resultados corporativos esperados, os riscos envolvidos e os impactos sobre todos os aspectos corporativos. Identificar e avaliar cursos alternativos para alcançar os resultados empresariais.

04 Desenvolver um plano de atingimento dos benefícios do qual será gerido ao longo do programa para assegurar que os benefícios planejados estão atrelados a donos e são alcançados, sustentáveis e otimizados.

05 Preparar e submeter em princípio, a aprovação (conceitual) do caso de negócio do programa inicial, fornecendo informações essenciais de tomada de decisão em relação propósito, contribuição aos objetivos de negócio, valor esperado gerado, prazos, etc.

06 Nomear um gestor dedicado ao programa, com as competências e habilidades compatíveis para gerir o programa de forma eficaz e eficiente.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.03 Gerencie a participação das partes interessadas.</b> Gerencie a participação das partes interessadas para assegurar um intercâmbio ativo de informações precisas, consistentes e oportunas que atinjam todas as partes interessadas. Isso inclui planejamento, identificação e envolvimento das partes interessadas e a gestão de suas expectativas.			<ul style="list-style-type: none"> <li>• Plano de envolvimento das partes interessadas</li> <li>• Resultados de avaliação de eficácia do envolvimento das partes interessadas</li> </ul>	Interno

## Atividades

- 01 Planejar como as partes interessadas de dentro e fora da companhia serão identificadas, analisadas, envolvidas e gerenciadas através do ciclo de vida dos projetos.
- 02 Identificar, envolver e gerenciar as partes envolvidas estabelecendo e mantendo níveis adequados de coordenação, comunicação e colaboração de forma a assegurar que estes estarão envolvidos no programa/projeto.
- 03 Mensurar a eficácia da participação das partes interessadas e tomar ações corretivas quando for necessário.
- 04 Analisar os interesses e necessidades das partes interessadas.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.04 Desenvolver e manter o plano do programa.</b> Formular um programa para iniciar a plataforma e posicioná-la para execução bem sucedida formalizando o escopo do trabalho a ser executado e identificando os entregáveis, nos quais irão satisfazer suas metas e a entrega de valor. Manter e atualizar o plano do programa e o caso de negócios em todo o ciclo de vida econômico do programa, assegurando alinhamento com os objetivos estratégicos e refletindo o status atual e perspectivas atualizadas adquiridas até a data.	APO05.03	<ul style="list-style-type: none"> <li>• Programas selecionados com marcos de retorno sobre investimento (ROI)</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de programa</li> </ul>	Interno
	APO07.03	<ul style="list-style-type: none"> <li>• Matriz de habilidades e competências</li> </ul>	<ul style="list-style-type: none"> <li>• Orçamento do programa e registro de benefícios</li> </ul>	APO05.06 APO06.05
	APO07.05	<ul style="list-style-type: none"> <li>• Inventário de recursos humanos de negócios e TI</li> </ul>	<ul style="list-style-type: none"> <li>• Funções e requisitos de recurso</li> </ul>	APO07.05 APO07.06
	BAI05.02	<ul style="list-style-type: none"> <li>• Time e funções de implementação</li> </ul>		
	BAI05.03	<ul style="list-style-type: none"> <li>• Plano de comunicação de visão</li> </ul>		
	BAI05.04	<ul style="list-style-type: none"> <li>• Ganhos rápidos identificados</li> </ul>		
	BAI07.03	<ul style="list-style-type: none"> <li>• Plano de teste de aceitação aprovado</li> </ul>		
	BAI07.05	<ul style="list-style-type: none"> <li>• Aceite aprovado e liberação para a produção</li> </ul>		

## Atividades

- 01 Definir e documentar o plano do programa abrangendo todos os projetos, incluindo o que é necessário para trazer as mudanças corporativas; sua imagem, produtos e serviços; processos de negócio; habilidades e quantidade de pessoas; relacionamento com as partes interessadas, clientes, fornecedores e outros; necessidades tecnológicas; e reestruturação organizacional necessária para atingir os resultados corporativos esperados do programa.
- 02 Especificar os recursos e habilidades requeridas necessárias para executar o projeto, incluindo gerentes de projeto e times do projeto, assim como os recursos de negócios. Especificar o financiamento, custos, cronograma e interdependências com outros projetos. Especificar a base para aquisição e atribuição de membros de equipes e/ou funcionários contratados competentes. Definir as funções e responsabilidades a todos os membros dos times e outras partes interessadas.
- 03 Atribuir clara e assertivamente a responsabilidade por cada projeto, incluindo a realização dos benefícios, controlando os custos, gerenciando os riscos e coordenando as atividades do projeto.
- 04 Assegurar que haja uma comunicação eficaz entre os planos do programa e relatórios de projeto em andamento com todos os projetos e o programa geral. Assegure que todas as mudanças feitas nos planos individuais sejam refletidas nos outros planos de programa corporativos.
- 05 Manter o plano do programa para assegurar que este está atualizado e reflete o alinhamento com os atuais objetivos estratégicos, real progresso e alterações relevantes aos resultados, benefícios, custos e riscos. O negócio deve conduzir os objetivos e priorizar o trabalho de forma a assegurar que o programa como definido irá atingir os requisitos corporativos. Revisar o progresso dos projetos individuais e ajustá-los conforme necessário de forma a cumprir as etapas estabelecidas.
- 06 Atualizar e manter, por todo o ciclo de vida econômico do programa do caso de negócio e registro dos benefícios e definir os benefícios chave decorrentes da realização do programa.

# COBIT® 5 : HABILITANDO PROCESSOS

## BAI01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.05 Lançar e executar o programa</b> Lançar e executar o programa para adquirir e dirigir os recursos necessários para atingir aos objetivos e benefícios do programa, tal como definido no plano de programa. De acordo com o critério de revisão de mudança de fase ou publicação, preparar revisão para a mudança de fase, iteração ou publicação sobre o progresso do programa e para permitir montar o plano do próximo financiamento da próxima revisão de mudança de fase ou publicação.	BAI05.03	<ul style="list-style-type: none"> <li>• Comunicações da visão</li> </ul>	<ul style="list-style-type: none"> <li>• Resultados da monitoração dos benefícios alcançados</li> <li>• Resultados da monitoração do alcance das metas do programa</li> <li>• Planos de auditoria do programa</li> </ul>	APO05.06 APO06.05  APO02.04  MEA02.06

### Atividades

- 01 Planejar, reservar e delegar os projetos necessários para alcançar os resultados do programa, com base na avaliação de recursos financeiros e aprovação em cada revisão de mudança de fase.
- 02 Estabelecer etapas previamente acordadas ao processo de desenvolvimento (pontos de checagem de desenvolvimento). Ao final de cada etapa, permitir discussões formais dos critérios aprovados com as partes interessadas. Após a conclusão bem sucedida da funcionalidade, desempenho e revisões de qualidade, e antes de finalizar as atividades das etapas, obter a aprovação formal e assinatura das partes interessadas e do patrocinador/dono do processo de negócio.
- 03 Executar um processo de compreensão dos benefícios ao longo do programa a fim de assegurar que os benefícios planejados estejam associados a donos e são possíveis de atingimento, são sustentáveis e otimizados. Monitorar a entrega de benefícios e reportar as metas de desempenho nas mudanças de fases ou revisões de iteração e lançamento. Executar análises de causa-raiz para desvios do plano e identificar e solucionar quaisquer ações corretivas necessárias.
- 04 Gerenciar cada programa ou projeto de forma a assegurar que a tomada de decisão e as atividades de entrega estão focadas no valor através da obtenção de benefícios para o negócio e metas de forma consistente, abordando riscos e alcançando os requisitos das partes interessadas.
- 05 Configurar escritório(s) de gestão do programa/projeto e planejar auditorias, revisões de qualidade, revisões de mudança de fase e revisões de benefícios percebidos.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.06 Monitorar, controlar e reportar os resultados do programa</b> Monitorar e controlar o desempenho do programa (entrega da solução) e da companhia (valor/resultados) em relação ao plano através do ciclo de vida econômico do investimento. Reportar o desempenho ao Comitê Diretor do programa e aos patrocinadores.	EDM02.03	<ul style="list-style-type: none"> <li>• Opinião quanto ao desempenho do portfólio e do programa</li> </ul>	<ul style="list-style-type: none"> <li>• Resultado de revisões do desempenho dos programas</li> </ul>	MEA01.03
	APO05.02	<ul style="list-style-type: none"> <li>• Expectativas de retorno de investimento</li> </ul>	<ul style="list-style-type: none"> <li>• Resultados da revisão de mudança de fase</li> </ul>	EDM02.01 APO02.04 APO05.04
	APO05.03	<ul style="list-style-type: none"> <li>• Avaliação do estudo do negócio</li> </ul>		
	APO05.04	<ul style="list-style-type: none"> <li>• Relatório de desempenho do portfólio de investimento</li> </ul>		
	APO05.06	<ul style="list-style-type: none"> <li>• Ações corretivas para aumento da obtenção de benefícios</li> <li>• Benefícios alcançados e as comunicações relacionadas</li> </ul>		
	APO07.05	<ul style="list-style-type: none"> <li>• Registro de utilização de recursos</li> <li>• Análise de deficiência de recursos</li> </ul>		
	BAI05.04	<ul style="list-style-type: none"> <li>• Comunicação de benefícios</li> </ul>		
	BAI06.03	<ul style="list-style-type: none"> <li>• Relatórios de status de requisição de mudanças</li> </ul>		
	BAI07.05	<ul style="list-style-type: none"> <li>• Resultados da avaliação de aceites</li> </ul>		

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI01 Práticas de Processo, Entradas/Saídas e Atividades

Atividades
01 Monitorar e controlar o desempenho do programa geral e os projetos dentro do programa, incluindo contribuições do negócio e de TI aos projetos, e informar de forma tempestivamente, completa e precisa. Relatórios podem incluir a programação, financiamento, funcionalidade, satisfação do usuário, controles internos e aceitação de responsabilidades.
02 Monitorar e controlar o desempenho frente às estratégias e objetivos corporativos e de TI, e relatar à gestão das mudanças empresariais implantados, benefícios realizados frente ao plano de realização de benefícios, bem como a adequação do processo de benefícios alcançados.
03 Monitorar e controlar os serviços de TI, ativos e recursos criados ou alterados como resultado do programa. Atentar a datas de implementação e ativação de serviços. Informar à gestão dos níveis de desempenho, prestação de serviços sustentados e contribuição para o valor.
04 Gerenciar o desempenho do programa em relação aos critérios-chave (por exemplo o escopo, cronograma, qualidade, realização de benefícios, custo, riscos e velocidade), identificar desvios do plano e tomar medidas de remediação tempestivas quando necessário.
05 Monitorar o desempenho individual dos projetos relacionados à entrega das capacidades esperadas, cronograma de obtenção dos benefícios, custos, riscos ou outras métricas para identificar potenciais impactos sobre o desempenho do programa. Tomar as medidas necessárias tempestivamente.
06 Atualizar os portfólios operacionais de TI refletindo as alterações que resultam do programa nos serviços de TI, ativos ou recursos relevantes.
07 De acordo com critério de alteração de fase, critérios de revisão de lançamento ou iteração, condução de revisões para informar o andamento do programa, de forma que a gestão possa dar prosseguimento ou decisões de ajuste e aprovar os próximos financiamentos as seguintes liberações de fase, lançamentos ou iteração.

Prática de Gestão	Entradas	Saídas	
Prática de Gestão	Entradas	Descrição	Para
<b>BAI01.07 Lance e inicie projetos dentro de um programa.</b> Definir e documentar a natureza e o escopo do projeto de forma a confirmar e desenvolver entre as partes interessadas um entendimento comum do escopo do projeto e como se relaciona com outros projetos dentro do programa de investimentos habilitado por TI. A definição deve ser formalmente aprovada pelo programa e patrocinadores dos projetos.	De	<ul style="list-style-type: none"> <li>• Confirmação do escopo do projeto</li> <li>• Definições do projeto</li> </ul>	Interno Interno

Atividades
01 Criar um entendimento comum do escopo do projeto entre as partes interessadas, fornecer às partes interessadas uma declaração escrita de forma clara definindo a natureza, escopo e benefícios de cada projeto.
02 Assegura que cada projeto tenha um ou mais patrocinadores com autoridade suficiente para gerir a execução do projeto dentro do programa geral.
03 Assegurar que as partes interessadas e patrocinadores chaves dentro da organização e TI concordem e aceitem os requisitos para o projeto, incluindo definição dos critérios de sucesso do projeto (aceitação) e indicadores chave de desempenho (KPIs)
04 Assegurar que a definição do projeto descreva os requisitos para um plano de comunicação do projeto que identifique comunicações internas e externas.
05 Com a aprovação das partes interessadas, manter a definição do projeto ao longo do projeto, refletindo as mudanças de requisitos.
06 Acompanhar a execução de um projeto, criar mecanismos tais como relatórios periódicos e conclusão de fases, publicações ou revisões de fases tempestivas com aprovação adequada.

Prática de Gestão	Entradas	Saídas	
Prática de Gestão	Entradas	Descrição	Para
<b>BAI01.08 Planeje os projetos</b> Estabelecer e manter um plano de projeto integrado, aprovado e formal (cobrindo recursos de negócios e de TI) para orientar a execução e controle do projeto ao longo da vida do projeto. O escopo dos projetos devem ser claramente definidos e amarrados para construir ou aumentar a capacidade dos negócios.	De	<ul style="list-style-type: none"> <li>• Plano de testes de aceitação aprovado</li> </ul>	<ul style="list-style-type: none"> <li>• Planos de projeto</li> <li>• Parâmetros do projeto</li> <li>• Relatórios e comunicações do projeto</li> </ul>
	BAI07.03		

# COBIT® : HABILITANDO PROCESSOS

## BAI01 Práticas de Processo, Entradas/Saídas e Atividades

### Atividades

- 01 Desenvolver um plano de projeto que forneça informações para permitir o gerenciamento para controlar progressivamente a evolução do projeto. O plano deve incluir detalhes dos entregáveis do projeto e critérios de aceitação, recursos e responsabilidades internas e externas necessárias, estruturas claras de divisão de trabalho e pacotes de trabalho, estimativa de recursos necessários, marcos/plano de lançamento/fases, dependências chave, e identificação do caminho crítico.
- 02 Manter o plano do projeto e outros planos dependentes (por exemplo plano de risco, plano de qualidade, plano de atingimento dos benefícios) para assegurar que estes estarão atualizados e refletem o real progresso e as alterações materiais aprovadas.
- 03 Assegurar que haja comunicação eficaz dos relatórios dos planos de projeto e progresso entre todos os projetos e com o programa geral. Assegure que toda modificação feita aos planos individuais serão refletidas nos demais planos.
- 04 Determinar as atividades, interdependências e colaboração e comunicação necessárias entre vários projetos dentro de um programa.
- 05 Assegurar que cada etapa é acompanhada por entregas significativas que requerem revisão e assinatura.
- 06 Estabelecer um parâmetro ao projeto (por exemplo, custo, cronograma, escopo, qualidade) devidamente revisado, aprovado e incorporado ao plano de projeto integrado.

### Prática de Gestão

### Entradas

### Saídas

	De	Descrição	Descrição	Para
<b>BAI01.09 Gerencie a qualidade dos programas e dos projetos.</b> Preparar e executar um plano de gestão de qualidade, processos e práticas, alinhadas com o sistema de gestão de qualidade no qual descreve a abordagem de qualidade do programa e projeto e como será implantado. O plano deve ser formalmente revisado e aceito por todas as partes interessadas e, em seguida, incorporado nos programas integrados e planos dos projetos.	APO11.01	<ul style="list-style-type: none"> <li>• Planos de gestão de qualidade</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de gestão de qualidade</li> </ul>	BAI02.04 BAI03.06 BAI07.01
	APO11.03	<ul style="list-style-type: none"> <li>• Necessidades dos clientes para gestão de qualidade</li> </ul>	<ul style="list-style-type: none"> <li>• Requisitos para a verificação independente dos resultados.</li> </ul>	BAI07.03

### Atividades

- 01 Identificar as tarefas e práticas de garantia necessárias para apoiar o reconhecimento de sistemas novos ou modificados durante o planejamento dos programas e projetos, e inclui-lo nos planos integrados. Assegurar que as tarefas fornecidas assegurem que os controles internos e soluções de segurança atendam os requisitos definidos.
- 02 Fornecer garantia de qualidade para os entregáveis do projeto, identificar propriedade e responsabilidades, processo de revisão de qualidade, critérios de sucesso e métricas de performance.
- 03 Definir os requisitos para a validação independente e verificação da qualidade dos resultados no plano
- 04 Executar atividades de garantia e controle de qualidade de acordo com o plano de gestão da qualidade e sistema de gestão de qualidade.

### Prática de Gestão

### Entradas

### Saídas

	De	Descrição	Descrição	Para
<b>BAI01.10 Gerenciar os riscos dos programas e dos projetos.</b> Eliminar ou minimizar os riscos específicos associados aos programas e projetos por meio de um processo sistemático de planejamento, identificação, análise, resposta e monitoramento e controle de áreas e eventos com potencial de causar alterações indesejadas. Riscos enfrentados pela gestão dos programas e projetos devem ser estabelecidos e registrados centralizadamente.	APO12.02	<ul style="list-style-type: none"> <li>• Resultados da análise de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de gestão de riscos do projeto</li> </ul>	Interno
	BAI02.03	<ul style="list-style-type: none"> <li>• Ações de mitigação de riscos</li> <li>• Registros dos requisitos de risco</li> </ul>	<ul style="list-style-type: none"> <li>• Resultados da avaliação de riscos do projeto</li> </ul>	Interno
	For a do COBIT	<ul style="list-style-type: none"> <li>• Estrutura do ERM</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos do projeto</li> </ul>	Interno

### Atividades

- 01 Estabelecer uma abordagem formal de gestão de risco do projeto alinhada com a estrutura de ERM. Assegurar de que a abordagem inclua identificar, analisar, responder, mitigar, monitorar e controlar os riscos.
- 02 Atribuir pessoal devidamente qualificado para a responsabilidade de executar os processos de gestão de riscos de projetos corporativos dentro de um projeto e assegurar que este está incorporado nas práticas de desenvolvimento de solução. Considerar alocar esse papel a uma equipe independente, especialmente se um ponto de vista específico é necessário ou um projeto é considerado crítico.
- 03 Efetuar a avaliação de risco do projeto para identificação e quantificação de risco de forma contínua ao longo do projeto. Gerir e comunicar os riscos adequadamente dentro da estrutura de governança do projeto.
- 04 Reavaliar o risco do projeto periodicamente, incluindo no início de cada fase principal e como parte das principais avaliações de solicitação de mudanças.
- 05 Identificar os responsáveis pelas ações para evitar, aceitar ou mitigar os riscos.
- 06 Manter e revisar um registro de riscos do projeto de todos os potenciais riscos de projeto, e um registro de mitigação de risco de todos os problemas do projeto e suas resoluções. Analisar o registro periodicamente para tendências e problemas recorrentes de

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

#### BAI01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.11 Monitore e controle os projetos.</b> Medir o desempenho do projeto em relação aos critérios chave de desempenho do projeto tais como cronograma, qualidade, custos e riscos. Identificar quaisquer desvios do esperado. Avaliar o impacto dos desvios de projeto e do programa geral, e reportar os resultados às principais partes interessadas.			<ul style="list-style-type: none"><li>• Critérios de desempenho do projeto</li><li>• Relatórios de progresso do projeto</li><li>• Aceites de alterações no projeto</li></ul>	Interno
<b>Atividades</b>				
01 Estabelecer e utilizar um conjunto de critérios de projeto incluindo, mas não se limitado a escopo, cronograma , qualidade, custo e nível de risco aceitável.				
02 Medir o desempenho do projeto em relação aos critérios de desempenho chave do projeto. Analisar desvios de critérios de desempenho-chave do projeto, estabelecidos pelas causas, e avaliar os efeitos positivos e negativos sobre o programa e seus projetos constituintes.				
03 Reportar às partes interessadas o progresso do projeto dentro do programa, desvios aos critérios chave estabelecidos de desempenho do projeto, e potenciais efeitos positivos e negativos no programa e os seus projetos constituintes.				
04 Monitorar alterações ao programa e revisar critérios chave de desempenho existentes de projeto para determinar se estes ainda representam parâmetros válidos de progresso.				
05 Documentar e apresentar alterações necessárias às partes interessadas do programa para aprovação antes da adoção. Comunicar os critérios revistos aos gestores do projeto para utilização em futuros relatórios de desempenho.				
06 Recomendar e monitorar ações corretivas, quando necessário, de acordo com a estrutura de governança dos programas e projetos				
07 Obter aprovação e assinatura dos entregáveis produzidos em cada iteração, publicação ou fase do projeto de gestores e usuários designados no negócio nos negócios afetados e funções de TI.				
08 Base de dados do processo de aprovação de critérios de aceitação claramente definidos acordado por as principais partes interessadas antes de trabalhar com início na fase de projeto ou entregável de iteração.				
09 Avaliar os acordos das mudanças de fase significativas, publicações ou iterações e realizar decisões de passa/não-passa baseado em critérios críticos de sucesso pré-determinados.				
10 Estabelecer e operar um sistema de controle de mudanças ao projeto de modo que todas as mudanças dos parâmetros do projeto (ex. custo, cronograma, escopo, qualidade) sejam devidamente revisados, aprovados e incorporados ao plano do projeto de acordo com a estrutura de governança dos programas e projetos.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.12 Gerenciar recursos e pacotes de trabalho do projeto</b> Gerenciar os pacotes de trabalho do projeto, estabelecendo requisitos formais de autorização e aceite de pacotes de trabalho, e atribuindo e coordenando recursos de negócios e de TI adequados.			<ul style="list-style-type: none"><li>• Necessidade de recursos do projeto</li><li>• Funções e responsabilidades do projeto</li><li>• Falhas no planejamento do projeto</li></ul>	APO07.05 APO07.06 Interno
<b>Atividades</b>				
01 Identificar as necessidades de recursos de negócios e de TI para o projeto e mapear os papéis e responsabilidades, com escalonamento e alçada acordados e compreendidos.				
02 Identificar as habilidades necessárias e o tempo requerido para todos os indivíduos envolvidos nas etapas do projeto em relação aos papéis relacionados. Relacione os papéis baseados nas habilidades disponíveis (ex. Matriz de habilidades de TI).				
03 Utilizar recursos experientes de gerência de projetos e líder de time com competências adequadas ao tamanho, complexidade e riscos do projeto.				
04 Considerar e definir claramente os papéis e responsabilidade de outras partes envolvidas, incluindo finanças, jurídico, compras, recursos humanos, auditoria interna e compliance.				
05 Definir e acordar claramente sobre a responsabilidade pela contratação e gestão dos produtos e serviços de terceiros e gerenciar os relacionamentos.				
06 Identificar e autorizar a execução do trabalho de acordo com o plano do projeto.				
07 Identificar falhas no plano do projeto e fornecer opinião ao gerente do projeto para remediação.				

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## BAI01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.13 Finalize um projeto ou iteração.</b> Ao final de cada projeto, publicação ou iteração, solicitar as partes interessadas do projeto que verifiquem se o projeto, publicação ou iteração entregou os resultados planejados e valor. Identificar e comunicar quaisquer atividades pendentes necessárias para atingir os resultados planejados do projeto e os benefícios do programa e identificar e documentar as lições aprendidas para uso em projetos futuros, publicações, iterações e programas.	BAI07.08	<ul style="list-style-type: none"> <li>• Plano de medidas correctivas</li> <li>• Relatório de revisão pós-implementação</li> </ul>	• Resultados da revisão pós-implementação	APO02.04
			• Lições aprendidas do projeto	Interno
			• Confirmações aceitação do projeto pelas partes interessadas	Interno

### Atividades

- 01 Definir e aplicar fases chave para a finalização do projeto, incluindo análises pós-implementação para avaliar se um projeto alcançou resultados e benefícios desejados.
- 02 Planejar e executar revisões pós-implementação para determinar se os projetos entregaram os benefícios esperados e melhorar a gestão de projetos e a metodologia de processo de desenvolvimento de sistemas.
- 03 Identificar, atribuir, comunicar e controlar todas as atividades não concluídas necessárias para alcançar os resultados e benefícios planejados pelos projetos.
- 04 Regularmente, e após a conclusão do projeto, coletar as lições aprendidas dos participantes do projeto. Revise estes e as atividades-chave que levaram a entrega dos benefícios e de valor. Analisar os dados e fazer recomendações para melhorar o projeto atual, bem como o método de gestão de projeto para projetos futuros.
- 05 Obter a aceitação das partes interessadas das entregas do projeto e transferir a posse.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI01.14 Fechar um programa</b> Remover o programa a partir do portfólio de investimento ativo quando há um consenso de que o desejado valor foi alcançado ou quando é evidente que não será alcançado dentro dos critérios de valor definido para o programa.	BAI07.08	<ul style="list-style-type: none"> <li>• Plano de medidas corretivas</li> <li>• Relatório de revisão pós-implementação</li> </ul>	<ul style="list-style-type: none"> <li>• Comunicação da finalização do programa e atribuição de responsabilidades que seguem</li> </ul>	APO05.05 APO07.06
<b>Atividades</b>				

- 01 Trazer o programa para um encerramento ordenado, incluindo a aprovação formal, a dissolução da organização do programa e funções de apoio, validação de resultados e comunicação de fechamento.
- 02 Rever e documentar as lições aprendidas. Uma vez que o programa é finalizado, removê-lo do portfólio ativo de investimentos.
- 03 Atribuir responsabilidade e processos para garantir que a empresa continue a otimizar o valor do serviço, ativos ou recursos. Investimentos adicionais podem ser necessários em algum momento futuro para garantir que isso ocorra.

## BAI01 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
PMBOK	
PRINCE2	

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI02 Gerenciar Definição de Requisitos	Área: Gestão Dominio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Identificar soluções e analisar requisitos antes da aquisição ou criação de forma a assegurar que estes estão em conformidade com os requisitos estratégicos corporativos abrangendo os processos de negócio, aplicações, informações/dados, infraestrutura e serviços. Coordenar com as partes interessadas envolvidas a revisão das opções de viabilidade incluindo custos e benefícios relacionados, análises de risco, e aprovação dos requisitos e soluções propostas.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
01 Alinhamento da estratégia de negócios e de TI	<ul style="list-style-type: none"> <li>Percentual de objetivos e requisitos estratégicos corporativos suportados por objetivos estratégicos de TI</li> <li>Nível de satisfação das partes interessadas com o escopo do portfólio planejado dos programas e serviços</li> <li>Percentual de direcionadores de valor de TI mapeados para direcionadores de valor ao negócio</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Quantidade de interrupções de negócios devido a serviços de TI.</li> <li>Percentual das partes interessadas no negócio satisfeitas com os serviços de TI que atingiram os níveis de serviço.</li> <li>Percentual de usuários satisfeitos com a qualidade de prestação dos serviços de TI</li> </ul>
12 Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia	<ul style="list-style-type: none"> <li>Quantidade de incidentes de processamento de negócios causada por erros de integração de tecnologia</li> <li>Quantidade de mudanças de processo de negócios que precisa ser atrasada ou reformulada devido à problemas de integração de tecnologia</li> <li>Quantidade de programas de negócios habilitados por TI atrasados ou que incorreram em custo adicional devido à problemas de integração de tecnologia</li> <li>Quantidade de aplicações ou infraestrutura crítica operando em silos e não integrados</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Requisitos funcionais e técnicos de negócios refletem as necessidades e expectativas corporativas.	<ul style="list-style-type: none"> <li>Percentual de retrabalho de requisitos devido ao desalinhamento com as necessidades e expectativas corporativas.</li> <li>Nível de satisfação das partes interessadas com os requisitos.</li> </ul>
02 A solução proposta satisfaz os requisitos funcionais, técnicos e de conformidade do negócio.	<ul style="list-style-type: none"> <li>Percentual de requisitos cobertos pela solução proposta</li> </ul>
03 Risco associado com os requisitos foi endereçado na solução proposta.	<ul style="list-style-type: none"> <li>Quantidade de incidentes não identificados como de risco</li> <li>Percentual de riscos não mitigados</li> </ul>
04 Requisitos e soluções propostas atendem aos objetivos do caso de negócio (valor esperado e custos prováveis).	<ul style="list-style-type: none"> <li>Percentual de objetivos do caso de negócio atendidos pelasolução proposta.</li> <li>Percentual de partes interessadas que não aprovam a solução em relação ao caso de negócio.</li> </ul>

# COBIT® : HABILITANDO PROCESSOS

BAI02 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês, Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Conselho de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>BAI02.02</b> Realize um estudo de viabilidade e formule soluções alternativas.					I	R	A	R		C					C	C	C	R	R	C	C	C	C	C	C	
<b>BAI02.03</b> Gerencie os riscos de requisitos.					R	R	A	R							C	C	C	C	R	C	C	C	C	C	C	
<b>BAI02.04</b> Obtenha aprovação dos requisitos e soluções.					R	R	A	R	R						C	C	R	C	R	R	C	C	C	C	C	
<b>BAI02.02</b> Realize um estudo de viabilidade e formule soluções alternativas.					R	R	A	R							C	C	C	C	C	C	C	C	C	C	C	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI02 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>Bai02.01 Defina e mantenha os requisitos funcionais e técnicos.</b> Baseado no caso de negócio, identificar, priorizar, especificar e alinhar com informações de negócios, requisitos funcionais, técnicos e de controle cobrindo o escopo/entendimento de todas as iniciativas necessárias para atingir os resultados esperados da solução de negócios habilitada por TI.	APO01.06	<ul style="list-style-type: none"> <li>• Procedimentos de integridade de dados</li> <li>• Diretrizes de segurança e controle de dados</li> <li>• Diretrizes de classificação de dados</li> </ul>	<ul style="list-style-type: none"> <li>• Respositório de definição de requisitos</li> </ul>	BAI03.01 BAI03.02 BAI04.01 BAI05.01
	APO03.01	<ul style="list-style-type: none"> <li>• Princípios de arquitetura</li> </ul>	<ul style="list-style-type: none"> <li>• Critérios de aceitação confirmados pelas partes interessadas</li> </ul>	BAI03.01 BAI03.02 BAI04.03 BAI05.01 BAI05.02
	APO03.02	<ul style="list-style-type: none"> <li>• Modelo de arquitetura da informação</li> <li>• Descrições dos parâmetros de domínio e definição de arquitetura</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de requisitos de solicitações de mudanças</li> </ul>	BAI03.09
	APO03.05	<ul style="list-style-type: none"> <li>• Guia de desenvolvimento de soluções</li> </ul>		
	APO10.02	<ul style="list-style-type: none"> <li>• RFI e RFP de fornecedores</li> </ul>		
	APO11.03	<ul style="list-style-type: none"> <li>• Critérios de aceitação</li> </ul>		

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI02 Práticas de Processo, Entradas/Saídas e Atividades

Atividades			
01 Definir e implementar uma definição de requisitos e procedimentos de manutenção e um repositório de requisitos que são apropriados ao tamanho, complexidade, objectivos e riscos da iniciativa que a empresa está considerando conduzir.			
02 Expressar os requisitos de negócios em termos de como a diferença entre as capacidades de negócios atuais e desejadas precisa ser endereçada e como uma função irá interagir com a solução e como utilizá-la.			
03 Ao longo do projeto, extrair, analisar e confirmar que todos os requisitos das partes interessadas, incluindo critérios relevantes de aceitação, são considerados, capturados, priorizados e registrados de modo que seja compreensível às partes interessadas, patrocinadores de negócio e time técnico de implantação, reconhecendo que os requisitos podem mudar e se tornarem mais detalhados a medida que são implementados.			
04 Especificar e priorizar as informações, os requisitos funcionais e técnicos com base nos requisitos das partes interessadas. Incluir requisitos de controle de informação nos processos de negócios, processos automatizados e ambientes de TI para endereçar os riscos de informação e cumprir com leis, regulamentos e contratos comerciais.			
05 Validar todos os requisitos por meio de abordagens tais como revisão por pares, validação de modelo ou protótipo operacional			
06 Confirmar a aceitação dos aspectos essenciais dos requisitos, incluindo as regras corporativas, controles de informação, continuidade dos negócios, conformidade legal e regulatória, auditabilidade, ergonomia, funcionalidade e usabilidade, segurança e documentação de suporte.			
07 Acompanhar e controlar o escopo, os requisitos e mudanças pelo ciclo de vida da solução ao longo do projeto assim como compreendendo as soluções evoluem.			
08 Considere os requisitos relacionados com as políticas e padrões corporativos, arquitetura corporativa, planos estratégicos e táticos de TI, negócios internos e terceirizados e processos de TI, requisitos de segurança, requisitos regulatórios, competências de pessoas, estrutura organizacional, casos de negócios e habilitadores de tecnologia.			

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI02.02 Realizar estudo de viabilidade e reformular soluções alternativas.</b> Realizar estudo de viabilidade de soluções alternativas potenciais, avaliar as viabilidades destes e selecionar a solução mais adequada. Se for o caso, implantar a opção selecionada como um piloto para determinar possíveis melhorias.	APO03.05	• Guia de desenvolvimento de soluções	• Relatório de estudo de viabilidade	BAI03.02 BAI03.03
	APO10.01	• Catálogo de fornecedores	• Plano de aquisição/desenvolvimento em alto-nível	APO10.02 BAI03.01
	APO10.02	• Decisões sobre as avaliações dos fornecedores • Avaliações de RFI e RFP • RFI e FRP de fornecedores		
	APO11.03	• Critérios de aceite		

Atividades			
01 Definir e executar um estudo de viabilidade, piloto ou solução de trabalho básico que de forma clara e consistente descreva as soluções alternativas que irão cobrir satisfatoriamente os requisitos funcionais e de negócios. Incluir uma avaliação de viabilidade tecnológica e econômica.			
02 Identificar as ações necessárias para a aquisição de soluções ou desenvolvimento baseado na arquitetura corporativa, e levar em conta limitações de escopo e/ou de tempo e/ou orçamentária.			
03 Revisar as soluções alternativas com todas as partes interessadas e selecionar a mais adequada baseada em critérios de viabilidade, incluindo riscos e custos.			
04 Traduzir o direcionamento de ação em um plano de alto nível de aquisição/desenvolvimento identificando recursos a serem utilizados e etapas que exigem uma decisão de passa/não passa.			

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI02.03 Gerenciar os requisitos de risco.</b> Identificar, documentar, priorizar e mitigar riscos funcionais, técnicos e de informação relacionados aos processos com os requisitos corporativos e solução proposta.			• Registro riscos de requisitos	BAI01.10 BAI03.02 BAI04.01 BAI05.01
			• Ações de mitigação de riscos	BAI01.10 BAI03.02 BAI05.01

# COBIT® 5 : HABILITANDO PROCESSOS

## BAI02 Práticas de Processo, Entradas/Saídas e Atividades

Atividades								
Prática de Gestão	Entradas		Saídas					
<b>BAI02.04 Obter a aprovação de requisitos e soluções.</b> Coordenar as respostas das partes interessadas afetadas e, em etapas-chave determinadas, obter do patrocinador de negócios ou dono do produto aprovação e assinatura dos requisitos funcionais e técnicos, dos estudos de viabilidade, das análises de risco e das soluções recomendadas .	BAI01.09	<ul style="list-style-type: none"> <li>• Plano de Gestão de Qualidade</li> </ul>	<ul style="list-style-type: none"> <li>• Aprovações de patrocinadores em requisitos e soluções propostas</li> <li>• Revisões de qualidade aprovadas</li> </ul>	BAI03.02 BAI03.03 BAI03.04 APO11.02				
Atividades								
<p>01 Assegurar que o patrocinador de negócios ou dono do produto tome a decisão final no que diz respeito a escolha da solução, abordagem de aquisição e concepção de alto nível, de acordo com o caso de negócio. Coordenar as opiniões das partes interessadas envolvidas e obter as assinaturas das autoridades de negócio e técnica adequadas (ex. Dono do processo de negócio, arquiteto corporativo, gerente de operações, segurança) para a abordagem proposta.</p> <p>02 Obter revisões de qualidade ao longo e no final de cada etapa-chave do projeto, iteração ou lançamento para avaliar os resultados com os critérios originais de aceite. Tenha a assinatura de patrocinadores de negócios e outras partes interessadas em cada revisão de qualidade positiva.</p>								

## BAI02 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ITIL V3 2011	Desenho de Serviço, 4.1 Coordenação do Desenho

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI03 Gerenciar Identificação e Desenvolvimento de Soluções		Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b>		
Estabelecer e manter soluções identificadas em linha com os requisitos corporativos cobrindo concepção, desenvolvimento, aquisição/suprimento e parceria com fornecedores/vendedores. Gerenciar configuração, preparação de testes, execução de testes, gestão de requisitos e manutenção de processos de negócios, aplicações, informações/dados, infraestrutura e serviços.		
<b>Declaração de Propósito do Processo</b>		
Estabelecer soluções tempestivas e eficientes capazes de suportar os objetivos corporativos estratégicos e operacionais.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
Objetivos de TI	Métricas Relacionadas	
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>• Quantidade de interrupções de negócios relacionados a incidentes de serviços de TI</li> <li>• Percentual de partes interessadas de negócios satisfeita com as entregas dos serviços de TI atingindo os níveis de serviço acordados</li> <li>• Percentual de usuários satisfeitos com a qualidade do serviço de TI entregue</li> </ul>	
<b>Objetivos e Métricas do Processo</b>		
Objetivo do Processo	Métricas Relacionadas	
01 A concepção da solução, incluindo componentes relevantes, atende às necessidades corporativas, alinha-se com os padrões e cobre todos os riscos identificados.	<ul style="list-style-type: none"> <li>• Quantidade de redesenho de soluções por desalinhamento aos requisitos.</li> <li>• Tempo necessário para aprovação da entrega da concepção que atingiu as expectativas</li> </ul>	
02 A solução, conforme a concepção, está de acordo com os padrões corporativos, e possui controles adequados, segurança e auditabilidade.	<ul style="list-style-type: none"> <li>• Quantidade de exceções à solução observada durante as etapas de revisão</li> </ul>	
03 A solução é de qualidade aceitável e foi testada com sucesso.	<ul style="list-style-type: none"> <li>• Quantidade de erros identificados durante os testes</li> <li>• Tempo e esforço para completar as tarefas</li> </ul>	
04 Alterações aprovadas aos requisitos são corretamente incorporadas na solução.	<ul style="list-style-type: none"> <li>• Quantidade de alterações aprovadas rastreadas nos quais geraram novos erros</li> </ul>	
05 Atividades de manutenção atendem com sucesso as necessidades tecnológicas e de negócios.	<ul style="list-style-type: none"> <li>• Quantidade de pedidos de manutenção insatisfatórias</li> </ul>	

# COBIT® 5 : HABILITANDO PROCESSOS

BAI03 Tabela RACI

Prática de Gestão	Conselho de Administração	Dir. Executivo (Presidente) (CEO)	Dir. Financeiro (CFO)	Dir. de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Dir. de Riscos (CRO)	Dir. de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Dir. de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>BAI03.01</b> Desenhe soluções de alto-nível					R	I	R								C	C	I	C	C	A	C		C	C	C	C
<b>BAI03.02</b> Desenhe componentes de solução detalhados					R	I	R								C	C	I	C	A	C		C	C	C	C	
<b>BAI03.03</b> Desenvolva componentes de solução					R	I	R								C	C	I	C	A	C		C	C	C	C	
<b>BAI03.04</b> Adquira componentes de solução.					I	R	I	I							C	C	A	I	R	R	R	C	C	C	C	
<b>BAI03.05</b> Construa soluções.					R	I	R								C	C	I	C	A	C		C	C	C	C	
<b>BAI03.06</b> Efetue garantia de qualidade.					I	R	A	R							C	C	I	C	R	C		C	C	C	C	
<b>BAI03.07</b> Pepare-se para testes das soluções.					R	A	I								C	C	I	R	R	R	R	R	R	R	R	
<b>BAI03.08</b> Execute testes das soluções.					R	A	I								I	I	I	R	R	I	I	I	I	I	I	
<b>BAI03.09</b> Gerencie mudanças a requisites.					I	R	A	R							I	I	C	R	R	C		C	C	C	C	
<b>BAI03.10</b> Faça manutenção das soluções.					R		R								C	C	I	C	A	C		C	C	C	C	
<b>BAI03.11</b> Defina os serviços de TI e mantenha o porftólio de serviços.					I	I		I							I	I	R	I	C	C	A	I	I			

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI03 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.01 Especificar soluções de alto nível.</b> Desenvolver e documentar soluções de alto nível usando técnicas de desenvolvimento ágil ou em cascata previamente acordadas. Garantir o alinhamento com a estratégia de TI e a arquitetura corporativa. Reanalisar e atualizar as especificações quando questões significativas ocorrerem durante a definição de especificações detalhadas, nas fases de construção ou conforme a solução evoluir. Garantir que as partes interessadas participem ativamente na especificação e aprovem cada versão.	APO03.01	• Princípios de arquitetura	• Especificação aprovada do design de alto nível	BAI04.03 BAI05.01
	APO03.02	• Descrições de padrões de domínio e definição da arquitetura		
	APO04.03	• Pesquisa de possibilidades de inovação		
	APO04.04	• Avaliação de ideias de inovação		
	BAI02.01	• Confirmação de critérios de aceitação das partes interessadas • Repositório de definição de requisitos		
	BAI02.02	• Plano de aquisição/desenvolvimento de alto nível		

## Atividades

- 01 Estabelecer uma especificação de alto nível que traduz a solução proposta em processos de negócio, suportando serviços, aplicações, infraestrutura e repositórios de informações capazes de atingir os requerimentos de negócio e de arquitetura corporativa.
- 02 Envolver usuários apropriadamente qualificados e experientes e especialistas de TI no processo de especificação para garantir que a especificação provê uma solução que otimamente utiliza as capacidades de TI propostas para melhorar os processos de negócio.
- 03 Criar uma especificação em conformidade com os padrões de especificação da organização, num nível de detalhe que é apropriado para a solução e método de desenvolvimento e consistente com as estratégias de negócio, TI e corporativa, com a arquitetura corporativa, planos de segurança, leis, regulações e contratos.
- 04 Após a aprovação pela garantia de qualidade, submeter a especificação de alto nível final para as partes interessadas do projeto, dono do processo de negócio e patrocinador para aprovação com base em um critério pré-acordado. Essa especificação vai evoluir durante o projeto conforme o entendimento se aprimorar.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.02 Especificar componentes detalhados da solução.</b> Desenvolver, documentar e elaborar especificações detalhadas progressivamente usando técnicas de desenvolvimento ágil ou em cascata previamente acordadas, endereçando todos os componentes (processos de negócio e controles manuais e automáticos relacionados, aplicações de TI de apoio, serviços de infraestrutura, produtos de tecnologia e parceiros/fornecedores). Assegurar que a especificação detalhada inclui SLAs e OLAs internos e externos.	APO03.01	• Princípios de arquitetura	• Especificação detalhada aprovada	BAI04.03 BAI05.01
	APO03.02	• Modelo de arquitetura da informação • Definição de descrições de domínio e arquitetura		APO09.03 BAI04.02
	APO03.05	• Orientação para desenvolvimento de solução		
	APO04.06	• Avaliações de uso de abordagens inovadoras		
	BAI02.01	• Critérios de aceite confirmados das partes interessadas • Repositório de definição de requisitos		
	BAI02.02	• Relatório do estudo de viabilidade		
	BAI02.03	• Ações para mitigação de risco • Registro de riscos de requerimentos		
	BAI02.04	• Aprovação pelo patrocinador dos requisitos e soluções propostas		

# COBIT® : HABILITANDO PROCESSOS

## BAI03 Práticas de Processo, Entradas/Saídas e Atividades

Atividades
01 Definir progressivamente as atividades dos processos de negócio e fluxos de trabalho que precisam ser executados em conjunto com o novo sistema aplicativo para atingir os objetivos corporativos, incluindo a definição de atividades de controle manuais.
02 Definir os passos de processamento da aplicação, incluindo a especificação de tipos de transação e regras de negócio, controles automáticos, definições de dados e objetos de negócio, casos de uso, interfaces externas, restrições e outros requerimentos (ex: licenças, jurídico, padrões, internacionalização/localização).
03 Classificar as entradas e saídas de dados de acordo com os padrões corporativos de arquitetura. Especificar a coleta de dados fonte, documentando as entradas de dados (independentemente da fonte) e validações para processamento de transações, bem como os métodos de validação. Definir as saídas identificadas, incluindo as fontes de dados.
04 Definir interfaces de sistema/solução, incluindo quaisquer intercâmbios automatizados de dados.
05 Definir o armazenamento de dados, localização, recuperação e recuperabilidade.
06 Definir a redundância apropriada, recuperação e backup.
07 Definir a interface entre o usuário e o sistema de aplicação para que seja de uso fácil e autodocumentado.
08 Considerar o impacto que a necessidade da solução por performance de infraestrutura, sendo sensível ao número de ativos de informática, largura de banda e sensibilidade da informação.
09 Proativamente avaliar deficiências de definição (ex: inconsistências, falta de clareza, possíveis falhas) ao longo do ciclo de vida, identificando melhorias quando requerido.
10 Prover a habilidade para auditar transações e identificar causas raiz de erros de processamento.

Prática de Gestão	Entradas		Saídas	
De	Descrição	Descrição	Para	
<b>BAI03.03 Desenvolver os componentes da solução.</b> Desenvolver componentes da solução progressivamente de acordo com as especificações detalhadas seguindo padrões de desenvolvimento, documentação, requerimentos de garantia da qualidade e aprovações. Assegurar que todos os requisitos de controle nos processos de negócio, aplicações de TI e serviços de infraestrutura que os suportam, produtos de serviços e tecnologia e parceiros/fornecedores são endereçados.	BAI02.02	<ul style="list-style-type: none"> <li>• Relatório do estudo de viabilidade</li> </ul>	<ul style="list-style-type: none"> <li>• Documentação dos componentes da solução</li> </ul>	BAI04.03 BAI05.05 BAI08.03 BAI08.04
	BAI02.04	<ul style="list-style-type: none"> <li>• Aprovação dos requerimentos e soluções propostos pelo patrocinador</li> </ul>		

Atividades
01 Desenvolver processos de negócio, serviços de suporte, aplicações e infraestrutura e repositórios de informação com base em requerimentos de negócio, funcionais e técnicos pré-acordados.
02 Quando fornecedores terceirizados estiverem envolvidos no desenvolvimento da solução, assegurar que os padrões de manutenção, suporte, desenvolvimento e licenciamento estejam endereçados em obrigações contratuais.
03 Acompanhar requisições de mudança e revisões de definições, desempenho e qualidade, assegurando a participação ativa de todas as partes interessadas.
04 Documentar todos os componentes da solução de acordo com padrões definidos e manter controle de versão sobre todos os componentes desenvolvidos e documentação associada.
05 Avaliar o impacto de configuração e customização da solução no desempenho e eficiência de soluções adquiridas e a interoperabilidade com aplicações existentes, sistemas operacionais e outra infraestrutura. Adaptar os processos de negócio conforme requeridos para alavancar a capacidade da aplicação.
06 Assegurar que responsabilidades pelo uso de componentes de infraestrutura de acesso restrito ou alta segurança sejam claramente definidos e entendidos pelos que desenvolvem e integram componentes de infraestrutura. O seu uso deve ser monitorado e avaliado.

Prática de Gestão	Entradas		Saídas	
De	Descrição	Descrição	Para	
<b>BAI03.04 Adquirir componentes da solução.</b> Adquirir componentes da solução com base no plano de aquisição de acordo com os requisitos e especificações detalhadas, princípios e padrões de arquitetura, e com as políticas e procedimentos corporativos de compras e contratos, requisitos de garantia de qualidade e aprovações. Assegurar que todos os requisitos legais e contratuais sejam identificados e endereçados pelo fornecedor.	BAI02.04	<ul style="list-style-type: none"> <li>• Aprovação dos requisitos e soluções propostas pelo patrocinador.</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de aquisição aprovado</li> </ul>	APO10.03
				BAI09.01

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI03 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
01 Criar e manter um plano para aquisição de componentes de solução, considerando a flexibilidade futura para aumento de capacidade, custos de transição e atualizações durante a vida do projeto.				
02 Revisar e aprovar todos os planos de aquisição, considerando o risco, custos, benefícios e a conformidade técnica com os padrões de arquitetura corporativa.				
03 Avaliar e documentar o grau em que as soluções adquiridas requerem adaptações de processos de negócios para alavancar os benefícios da solução adquirida.				
04 Providenciar as aprovações requeridas em pontos-chave de decisão durante o processo de aquisição.				
05 Registrar o recebimento de todas as aquisições de software e infraestrutura no inventário de ativos.				

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.05 Construir soluções:</b> Instalar e configurar soluções e integrá-las com as atividades de processos de negócios. Implementar medidas de controle, segurança e auditabilidade durante a configuração e durante a integração do hardware e software de infraestrutura, para proteger os recursos e garantir a disponibilidade e integridade dos dados. Atualizar o catálogo de serviços para refletir as novas soluções.			• Componentes de solução integrados e configurados	BAI06.01

Atividades				
01 Integrar e configurar os componentes de solução de TI e de negócios e os repositórios de informação em linha com as especificações detalhadas e requisitos de qualidade. Considerar o papel dos usuários, partes interessadas e donos do processo na configuração de processos de negócios.				
02 Completar e atualizar os manuais operacionais e os processos de negócios, quando necessário, para considerar qualquer customização ou condições especiais para a implementação.				
03 Considerar todos os requisitos de controle da informação na integração e configuração de componentes, incluindo a implementação de controles de negócio, quando apropriado, em controles automatizados para que o processamento seja correto, completo, pontual, autorizado e auditável.				
04 Implementar trilhas de auditoria durante a configuração e integração de hardware e software de infraestrutura para proteger recursos e garantir a disponibilidade e integridade.				
05 Considerar quando o efeito de customizações e configurações cumulativas (incluindo mudanças de pequeno porte que não foram submetidas a especificações formais) requeiram uma reavaliação de alto nível da solução e funcionalidades associadas.				
06 Assegurar a interoperabilidade dos componentes da solução com testes, preferencialmente automatizados.				
07 Configurar os softwares de aplicação adquiridos para atender aos requisitos de processamento de negócios.				
08 Definir catálogos de serviço para públicos-alvo internos e externos com base nos requisitos de negócios.				

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.06 Executar a garantia de qualidade.</b> Desenvolver, obter recursos e executar um plano de garantia de qualidade alinhado com o sistema de garantia de qualidade para atingir a qualidade especificada na definição de requisitos e os procedimentos e padrões corporativos de qualidade.	APO11.01	• Resultados das revisões de efetividade do sistema de gestão da qualidade	• Plano de garantia de qualidade	APO11.04
	BAI01.09	• Plano de gestão da qualidade	• Resultados da revisão de qualidade, exceções e correções	APO11.04

Atividades				
01 Definir um plano e práticas de garantia de qualidade, como, por exemplo, a especificação de critérios de qualidade, processos de validação e verificação, definição de como a qualidade será revisada, qualificações necessárias aos revisores de qualidade e papéis e responsabilidades.				
02 Monitorar frequentemente a qualidade da solução com base em requisitos de projeto, políticas corporativas, aderência à metodologias de desenvolvimento, procedimentos de gestão da qualidade e critérios de aceite.				
03 Empregar a inspeção de código, práticas de desenvolvimento orientadas a testes, testes automatizados, integração contínua, walkthroughs e testes de aplicação quando apropriado. Reportar sobre resultados dos processos de monitoramento e teste para a equipe de desenvolvimento de sistema e para a gestão de TI.				
04 Monitorar todas as exceções de qualidade e endereçar todas as ações corretivas. Manter um registro com todas as revisões, resultados, exceções e correções. Repetir as revisões de qualidade, quando apropriado, com base na quantidade de retrabalho e ações corretivas.				

# COBIT® : HABILITANDO PROCESSOS

## BAI03 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.07 Preparar para teste da solução.</b> Estabelecer um plano de teste e ambientes necessários para testes unitários e integrados dos componentes da solução, incluindo os processos de negócio e serviços de suporte, aplicações e infraestrutura.			<ul style="list-style-type: none"> <li>• Plano de teste</li> <li>• Procedimentos de teste</li> </ul>	BAI07.03 BAI07.03
<b>Atividades</b>				
01 Criar um plano de teste integrado e práticas de acordo com o ambiente corporativo e planos estratégicos de tecnologia que possibilitem a criação de ambientes de teste e simulação para auxiliar a verificar que a solução operará com sucesso no ambiente produtivo, entregará os resultados pretendidos e que os controles são adequados.				
02 Criar um ambiente de teste que suporte o escopo completo da solução e reflita, o mais próximo possível, de condições reais de uso, incluindo processos e procedimentos de negócio, número de usuários, tipos de transação e condições de desenvolvimento.				
03 Criar procedimentos de teste alinhados com o plano e práticas e permitem a avaliação da operação da solução em condições reais de uso. Assegurar que os procedimentos de teste avaliam a adequacidade dos controles, com base em padrões corporativos que definem papéis, responsabilidades e critérios de teste e que são aprovadas pelas partes interessadas do projeto, pelo patrocinador e pelo proprietário do processo de negócio.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.08 Executar testes de solução.</b> Executar testes continuamente durante o desenvolvimento, incluindo testes de controle, de acordo com o plano de teste definido e práticas de desenvolvimento no ambiente apropriado. Assegurar a participação de proprietários de processos de negócio e usuários finais no time de teste. Identificar, logar e priorizar erros e problemas identificados durante o teste.	APOD4.05	<ul style="list-style-type: none"> <li>• Análise de iniciativas rejeitadas</li> </ul>	<ul style="list-style-type: none"> <li>• Registros de resultados de teste e trilhas de auditoria</li> <li>• Comunicação de resultados de teste</li> </ul>	BAI07.03 BAI07.03
<b>Atividades</b>				
01 Executar testes de soluções e seus componentes, com representantes dos processos de negócio e usuários finais. Assegurar que os testes sejam conduzidos somente nos ambientes de desenvolvimento e teste.				
02 Utilizar instruções de teste claras, como definido no plano de testes, e considerar a proporção adequada de testes automatizados e testes interativos com usuários.				
03 Executar todos os testes de acordo com práticas e o plano de teste incluindo a integração de processos de negócio e soluções de TI e requisitos não-funcionais (ex: segurança, interoperabilidade, usabilidade).				
04 Identificar, registrar e classificar erros (ex: menor, significativo e missão crítica) durante os testes. Repetir os testes até que todos os erros significativos tenham sido resolvidos. Assegurar que uma trilha de auditoria com os resultados de teste seja mantida.				
05 Registrar os resultados de teste e comunicar os resultados para as partes interessadas de acordo com o plano de teste.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.09 Gerenciar mudanças de requisitos.</b> Acompanhar o status de requisitos individuais (incluindo requisitos rejeitados) durante o ciclo de vida do projeto e gerenciar a aprovação de mudanças de requisitos.	APOD4.05 BAI02.01	<ul style="list-style-type: none"> <li>• Resultados e recomendações das provas de conceito</li> <li>• Registro das requisições de mudança de requisitos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de todas as requisições de mudança submetidas e aprovadas</li> </ul>	BAI06.03
<b>Atividades</b>				
01 Avaliar o impacto de todas as requisições de mudança no desenvolvimento da solução, o caso de negócios original e orçamento e categorizá-los e priorizá-los de acordo.				
02 Acompanhar as mudanças no requisitos, possibilitando o monitoramento, revisão e aprovação por todas as partes interessadas. Assegurar que os resultados do processo de mudança são completamente entendidos e acordados por todas as partes interessadas, o patrocinador e o proprietário do processo de negócio.				
03 Aplicar as requisições de mudança, mantendo a integridade da integração e configuração dos componentes da solução. Avaliar o impacto de qualquer atualização significativa da solução e classificar de acordo com critérios objetivos pré-acordados (como requisitos corporativos), com base nos resultados de análise do risco envolvido (como o impacto em sistemas, processos ou segurança existentes), justificativa do custo-benefício e outros requisitos.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI03 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.10 Manter soluções.</b> Desenvolver e executar um plano para manutenção da solução e dos componentes de infraestrutura. Incluir revisões periódicas das necessidades de negócio e requisitos operacionais.			<ul style="list-style-type: none"> <li>• Plano de manutenção</li> </ul>	APO08.05
			<ul style="list-style-type: none"> <li>• Componentes da solução atualizados e documentação relacionada</li> </ul>	BAI05.05

## Atividades

- 01 Desenvolver e executar um plano para manutenção dos componentes da solução que inclua revisões periódicas das necessidades de negócio e requisitos operacionais como gestão de correções, estratégias de atualização, mapeamento de vulnerabilidades e requisitos de segurança.
- 02 Avaliar a significância das atividades de manutenção propostas na funcionalidade, processos de negócio e especificação atuais da solução. Considerar o risco, impacto aos usuários e disponibilidade de recursos. Assegurar que os proprietários dos processos de negócio entendem o efeito de categorizar mudanças como manutenção.
- 03 Em caso de grandes mudanças nas soluções existentes que resultem em mudanças significativas nas especificações, funcionalidades e processos de negócio correntes, seguir o processo de desenvolvimento de novos sistemas. Para atualizações de manutenção, utilizar o processo de gestão de mudanças.
- 04 Assegurar que o padrão e o volume de atividades de manutenção são analisados periodicamente a fim de verificar atividades anormais, indicando problemas de qualidade e desempenho, custo-benefício de uma grande atualização, ou a substituição da solução ao invés da manutenção.
- 05 Para atualizações de manutenção, utilizar o processo de gestão de mudanças para controlar todas as requisições.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI03.11 Definir os serviços de TI e manter o catálogo de serviços.</b> Definir e acordar serviços de TI e opções níveis de serviço novos ou atualizados. Documentar definições de serviço e opções de nível de serviço novas ou atualizadas no catálogo de serviços.	EDM04.01	<ul style="list-style-type: none"> <li>• Princípios guia para alocação de recursos e competências</li> </ul>	<ul style="list-style-type: none"> <li>• Definições de serviço</li> </ul>	APO05.01 DSS01.03
	APO02.04	<ul style="list-style-type: none"> <li>• Descrição do custo benefício do ambiente alvo</li> <li>• Deficiências e mudanças necessárias para atingir a competência almejada</li> </ul>	<ul style="list-style-type: none"> <li>• Catálogo de serviços atualizado</li> </ul>	APO05.05
	APO06.02	<ul style="list-style-type: none"> <li>• Alocação de orçamento</li> </ul>		
	APO06.03	<ul style="list-style-type: none"> <li>• Comunicações do orçamento</li> <li>• Plano de orçamento de TI</li> </ul>		
	APO08.05	<ul style="list-style-type: none"> <li>• Definição de projetos de melhoria potenciais</li> </ul>		
	BAI10.02	<ul style="list-style-type: none"> <li>• Baseline de configuração</li> </ul>		
	BAI10.03	<ul style="list-style-type: none"> <li>• Baseline de aprovação de mudanças</li> </ul>		
	BAI10.04	<ul style="list-style-type: none"> <li>• Relatórios de status de configuração</li> </ul>		

## Atividades

- 01 Propor definições de serviços de TI novos ou alterados para assegurar que os serviços atingem seu propósito. Documentar as propostas de definição de serviços a serem desenvolvidos no catálogo.
- 02 Propor opções de nível de serviços novas ou alteradas (tempos de serviço, satisfação do usuário, disponibilidade, desempenho, capacidade, segurança, continuidade, conformidade e usabilidade) para assegurar que os serviços de TI estão prontos para uso. Documentar as opções de serviços propostas no catálogo.
- 03 Intefacear com a gestão de relacionamento com o negócio e gestão do catálogo para acordar as definições de serviço e opções de nível de serviço propostas.
- 04 Se as mudanças de serviço não forem aprovadas pelo aprovador competente, elaborar serviços de TI ou opções de nível de serviço novas ou melhoradas. Caso contrário, encaminhar a mudança no serviço para a gestão do catálogo para revisão do investimento.

## BAI03 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
Nenhum	

# COBIT® 5 : HABILITANDO PROCESSOS

BAI04 Gerenciar Disponibilidade e Capacidade	Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Balancear as necessidades atuais e futuras por disponibilidade, desempenho e capacidade com provisão de serviços eficiente. Incluir a avaliação de competências atuais, prevendo as necessidades futuras com base em requisitos de negócio, análise de impactos, e avaliação de riscos para planejar e implementar ações que se adequam aos requerimentos identificados.	
<b>Declaração de Propósito do Processo</b> Manter a disponibilidade do serviço, gestão eficiente dos recursos, e otimizar o desempenho do sistema através da previsão de requisitos de capacidade futuros.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>• Número de rupturas de negócios causadas por incidentes de serviços de TI</li> <li>• Percentual das partes interessadas de negócios satisfeitas com a entrega de serviços de TI que está dentro dos níveis de serviço pré-acordados</li> <li>• Percentual de usuários satisfeitos com a qualidade da entrega de serviços de TI</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>• Frequência de avaliações de otimizações de custo e da maturidade</li> <li>• Resultados das avaliações de tendência</li> </ul>
14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	<ul style="list-style-type: none"> <li>• Nível de satisfação dos usuários de negócios com a qualidade e a tempestividade (ou disponibilidade) de informações gerenciais</li> <li>• Quantidade de incidentes em processos de negócios causados pela indisponibilidade de informação</li> <li>• Proporção e extensão de decisões incorretas de negócios onde informações incorretas ou indisponíveis foram o fator chave</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 O plano de disponibilidade antecipa as expectativas de negócios sobre requisitos críticos de capacidade	<ul style="list-style-type: none"> <li>• Quantidade de atualizações não planejadas de capacidade, desempenho e disponibilidade</li> </ul>
02 Capacidade, desempenho e disponibilidade estão de acordo com os requisitos	<ul style="list-style-type: none"> <li>• Quantidade de picos de transações onde o desempenho alvo é superado</li> <li>• Quantidade de incidentes de disponibilidade</li> <li>• Quantidade de eventos onde a capacidade excedeu os limites planejados</li> </ul>
03 Problemas de disponibilidade, desempenho e capacidade são identificados e rotineiramente resolvidos	<ul style="list-style-type: none"> <li>• Quantidade e percentual de problemas não resolvidos de disponibilidade, desempenho e capacidade</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI04 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) / CEO	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Audit or	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Contingência dos Negócios	Oficial de Privacidade
BAI04.01 Avaliar a disponibilidade, desempenho e capacidade atuais e criar um padrão.					I													C		C	R		R	C	C	
BAI04.02 Avaliar o impacto no negócio						A												C		C	R		R	C	C	
BAI04.03 Planejamento para requisitos de serviços novos ou alterados.						R												C		C	A		R	C	C	
BAI04.03 Planejamento para requisitos de serviços novos ou alterados						R												C		C	A		R	C	C	
BAI04.05 Investigar e endereçar problemas de disponibilidade, desempenho e capacidade					I	R												I	R	C	A		R	I	I	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI04 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI04.01 Avaliar a disponibilidade, desempenho e capacidade atuais e criar um padrão.</b> Avaliar a disponibilidade, desempenho e capacidade de serviços e recursos para assegurar que a capacidade e performance estão disponíveis a um custo justificável para suportar as necessidades de negócio e entregar os níveis de serviço. Criar padrões de disponibilidade, desempenho e capacidade para comparação futura.	BAI02.01	• Reppositório de definição de requisitos	• Padrões de disponibilidade, desempenho e capacidade	Interno
	BAI02.03	• Registro de riscos de requisitos	• Avaliações dos níveis de serviço	APO09.05
<b>Atividades</b>				
01 Considerar nas avaliações (atuais e previstas) de disponibilidade, desempenho e capacidade de serviços e recursos: requisitos do cliente, prioridades de negócio, objetivos de negócio, impacto no orçamento, utilização de recursos, competências de TI e tendências da indústria.				
02 Monitorar o desempenho e utilização da capacidade atual contra limites definidos, quando necessário com o suporte de software automatizado.				
03 Identificar e acompanhar todos os incidentes causados por capacidade ou desempenho inadequados.				
04 Avaliar regularmente os níveis correntes de desempenho para todos os níveis de processamento (demandas de negócio, capacidade do serviço e capacidade do recurso) comparando-os contra tendências e níveis de serviços, levando em consideração mudanças no ambiente.				

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## BAI04 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI04.02 Avaliar o impacto no negócio.</b> Identificar os serviços importantes para a organização, mapear os serviços e recursos com os processos de negócio, e identificar dependências de negócio. Assegurar que o impacto de recursos indisponíveis é completamente acordado e aceito pelo cliente. Assegurar que, para funções vitais de negócio, os níveis de serviço relacionados à disponibilidade podem ser atingidos.	APO09.03	<ul style="list-style-type: none"> <li>• Acordos de nível de serviço e acordos de nível operacional</li> </ul>	<ul style="list-style-type: none"> <li>• Cenários de disponibilidade, desempenho e capacidade</li> </ul>	Interno
	BAI03.02	<ul style="list-style-type: none"> <li>• Revisão dos acordos de nível de serviço e acordos de nível operacional</li> </ul>	<ul style="list-style-type: none"> <li>• Avaliações de impacto no negócio relacionadas a disponibilidade, desempenho e capacidade</li> </ul>	

### Atividades

- 01 Identificar somente as soluções ou serviços que são críticos para os processos de gestão da disponibilidade e capacidade.
- 02 Mapear as soluções ou serviços selecionados com aplicações, e infraestrutura com os quais são dependentes para habilitar o foco em recursos críticos para o planejamento da disponibilidade.
- 03 Coletar dados sobre padrões de disponibilidade de logs de falhas passadas e monitoramento do desempenho. Utilizar ferramentas de modelagem para ajudar a prever falhas com base em tendências históricas de uso e expectativas da administração sobre novos ambientes ou condições de uso.
- 04 Criar cenários com base nos dados coletados, descrevendo situações de disponibilidade futuras para ilustrar a variedade de níveis de capacidade potenciais necessários para atingir o desempenho e disponibilidade objetivado.
- 05 Determinar a probabilidade de que o objetivo de disponibilidade e desempenho não seja atingido com base nos cenários.
- 06 Determinar o impacto dos cenários nas métricas de desempenho de negócio (ex.: receita, lucro, serviços ao cliente). Engajar a linha de serviços, líderes funcionais (especialmente finanças) e regionais para entender a avaliação de impacto destes.
- 07 Assegurar que os donos dos processos de negócio entendam e concordem com os resultados da análise. Dos proprietários de negócio, obter uma lista de riscos não aceitáveis que demandem uma resposta para reduzir o risco a níveis aceitáveis.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI04.03 Planejamento para requisitos de serviços novos ou alterados.</b> Planejar e priorizar as implicações de mudanças de necessidades de negócio e requisitos de serviço para a disponibilidade, desempenho e capacidade.	BAI02.01	<ul style="list-style-type: none"> <li>• Critérios de aceite confirmados pelas partes interessadas</li> </ul>	<ul style="list-style-type: none"> <li>• Melhorias priorizadas</li> </ul>	APO02.02
	BAI03.01	<ul style="list-style-type: none"> <li>• Especificações de alto nível aprovadas</li> </ul>	<ul style="list-style-type: none"> <li>• Planos de capacidade e desempenho</li> </ul>	
	BAI03.02	<ul style="list-style-type: none"> <li>• Especificações detalhadas aprovadas</li> </ul>		
	BAI03.03	<ul style="list-style-type: none"> <li>• Componentes de solução documentados</li> </ul>		

### Atividades

- 01 Revisar as implicações de disponibilidade e capacidade na análise de tendências de serviço.
- 02 Identificar as implicações na capacidade e disponibilidade de mudanças de necessidades de negócio e oportunidades de melhoria. Utilizar técnicas de modelagem para validar a disponibilidade, desempenho e planos de capacidade.
- 03 Priorizar as melhorias necessárias e criar planos de capacidade e disponibilidade de custo justificável.
- 04 Ajustar os planos de capacidade e disponibilidade e acordos de nível de serviço baseado em processos de negócios novos, propostos e/ou projetados e dando suporte a mudanças de serviços, aplicações e de infraestrutura, assim como revisões do desempenho atual e utilização da capacidade, incluindo níveis de carga de trabalho.
- 05 Assegurar que a administração compare a demanda atual de recursos com a oferta e demanda previstas para avaliar as técnicas de previsão atuais e fazer melhorias quando possível.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI04.04 Monitorar e revisar a disponibilidade e capacidade.</b> Monitorar, medir, analisar, reportar e revisar a disponibilidade, desempenho e a capacidade. Identificar desvios dos padrões estabelecidos. Revisar os relatórios de análise de tendência identificando ações onde necessário, e assegurando que todos os níveis de serviço estejam dentro das especificações.			<ul style="list-style-type: none"> <li>• Relatórios de desempenho, capacidade e disponibilidade</li> </ul>	MEA01.03

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI04 Práticas de Processo, Entradas/Saídas e Atividades

## Atividades

- 01 Estabelecer um processo para a coleta de dados para prover a administração com informações de monitoramento e reporte sobre as cargas disponibilidade, performance e capacidade de todos os recursos relacionados à informação.
- 02 Prover reportes regulares dos resultados de forma adequada para revisão por TI e pela administração do negócio e comunicação para a administração corporativa.
- 03 Integrar atividades de monitoração e reporte às atividades iterativas de gestão de capacidade (monitoramento, análise, ajuste e implementações)
- 04 Prover relatórios de capacidade para os processos de orçamento.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI04.05 Investigar e endereçar problemas de disponibilidade, desempenho e capacidade.</b> Encaminhar os desvios investigando e resolvendo os problemas de disponibilidade, desempenho e capacidade identificados.			<ul style="list-style-type: none"> <li>• Deficiências de desempenho e capacidade</li> <li>• Ações corretivas</li> <li>• Procedimentos de escalação de emergência.</li> </ul>	Interno APO02.02 DSS02.02

## Atividades

- 01 Obter orientação de manuais de produto de fornecedores para assegurar um nível apropriado de disponibilidade de desempenho para picos de processamento e carga de trabalho.
- 02 Identificar deficiência de capacidade e desempenho com base no monitoramento do desempenho atual e previsto. Utilizar as especificações conhecidas de disponibilidade, continuidade e recuperação para classificar recursos e permitir a priorização.
- 03 Definir ações corretivas (ex.: transferir carga de trabalho, priorização de tarefas e adição de recursos, quando problemas de capacidade e performance forem identificados).
- 04 Integrar ações corretivas requeridas nos processos de planejamento e gestão de mudanças apropriados.
- 05 Definir um procedimento de escalação para um procedimento de resolução rápido em caso de problemas de capacidade e performance.

## BAI04 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	6.3 Serviço e gerenciamento de continuidade e disponibilidade
ITIL V3 2011	Desenho de Serviço, 4.4 Gestão de Disponibilidade Desenho de Serviço, 4.5 Gestão de Capacidade

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

BAI05 Gerenciar Capacidade de Mudança Organizacional		Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Maximizar a probabilidade de implementações de mudanças organizacionais que afetem toda a corporação com sucesso, rapidamente, com risco reduzido, cobrindo o ciclo completo de mudanças e de todas as partes interessadas afetadas no negócio e em TI.		
<b>Declaração de Propósito do Processo</b> Preparar e comprometer as partes interessadas para mudanças no negócio e reduzir o risco de falhas.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
<b>Objetivos de TI</b>		<b>Métricas Relacionadas</b>
08 Uso adequado de aplicativos, informações e soluções tecnológicas	<ul style="list-style-type: none"> <li>• Percentual de proprietários de processo de negócio satisfeitos com os produtos de TI e serviços de suporte</li> <li>• Nível de entendimento pelos proprietários de processos de negócio de como soluções de tecnologia suportam os seus processos</li> <li>• Nível de satisfação dos usuários de negócio com treinamento e manuais de usuário</li> <li>• Valor presente mostrando o nível de satisfação do negócio com a qualidade e utilidade das soluções de negócio</li> </ul>	
13 Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	<ul style="list-style-type: none"> <li>• Quantidade de programas/projetos no prazo e dentro do orçamento</li> <li>• Percentual de partes interessadas satisfeitas com os programas/projetos</li> <li>• Quantidade de programas precisando de retrabalho significativo devido a falhas de qualidade</li> <li>• Custo de manutenção de aplicações contra o custo total de TI</li> </ul>	
17 Conhecimento, expertise e iniciativas para inovação dos negócios	<ul style="list-style-type: none"> <li>• Nível de conscientização de executivos de negócio e entendimento das possibilidades de inovações em TI</li> <li>• Nível de satisfação das partes interessadas com os níveis de pericia e ideias de inovação em TI</li> </ul>	
<b>Objetivos e Métricas do Processo</b>		
<b>Objetivo do Processo</b>		<b>Métricas Relacionadas</b>
01 Desejo de mudança das partes interessadas foi entendido.	<ul style="list-style-type: none"> <li>• Nível de desejo das partes interessadas pela mudança</li> <li>• Nível de envolvimento da alta administração</li> </ul>	
02 Time de implementação é competente e hábil para conduzir a mudança.	<ul style="list-style-type: none"> <li>• Avaliações de satisfação das partes interessadas sobre o time de implementação</li> <li>• Número de problemas com as competências ou capacidade</li> </ul>	
03 Mudanças desejadas são entendidas e aceitas pelas partes interessadas.	<ul style="list-style-type: none"> <li>• Comentários ou parecer sobre o nível de entendimento</li> <li>• Número de perguntas recebidas</li> </ul>	
04 Participantes tem poder para entregar a mudança.	<ul style="list-style-type: none"> <li>• Percentual de participantes com autoridade apropriada</li> <li>• Retorno dos participantes sobre o nível de empoderamento</li> </ul>	
05 Participantes são habilitados a operar, usar e manter a mudança.	<ul style="list-style-type: none"> <li>• Percentual de participantes treinados</li> <li>• Auto-avaliações dos participantes sobre as competências relevantes</li> <li>• Nível de satisfação dos participantes operando, usando e mantendo a mudança</li> </ul>	
06 A mudança é implementada e sustentada.	<ul style="list-style-type: none"> <li>• Percentual de usuários apropriadamente treinados para a mudança</li> <li>• Nível de satisfação dos usuários com a adoção da mudança</li> </ul>	

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI05 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>BAI05.01</b> Estabelecer o desejo de mudança.	R	A	C	C	R	C	R	R			C		R	C	C	R	C	C	C	C	C	C	C	C		
<b>BAI05.02</b> Formar um time de implementação efetivo.		I	I	C	A	C	C	R	R					C	C	C	R	R	C	C	C	C	C	C	C	
<b>BAI05.03</b> Comunicar a visão desejada.		A	C	C	R	I	R	I	I				I	I	I	R	I	I	I	I	I	I	I	I	I	
<b>BAI05.04</b> Empoderar participantes e identificar vitórias de curto prazo.				R	A	C	C	R	C				R	C	C	R	C	C	C	C	C	C	C	C	C	
<b>BAI05.05</b> Habilitar a operação e uso					C	A	R		R									R	C	R	R	R	R	R	R	R
<b>BAI05.06</b> Embutir novas abordagens		R	R	R	A	R		R										R	C	R	R	R	R	R	R	R
<b>BAI05.07</b> Manter as mudanças.	R	R	R	R	A	R		R										R	C	R	R	R	R	R	R	R

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI05 Práticas de Processo, Entradas/Saídas e Atividades				
Prática de Gestão		Entradas		Saídas
		De	Descrição	Descrição
<b>BAI05.01 Estabelecer o desejo de mudança.</b> Entender o escopo e o impacto de mudanças antecipadas e o desejo de mudar das partes interessadas. Identificar ações para motivar as partes interessadas a aceitar e querer fazer as mudanças acontecerem com sucesso.		APO11.03	<ul style="list-style-type: none"> <li>• Resultados da qualidade do serviço, incluindo a avaliação de clientes</li> </ul>	<ul style="list-style-type: none"> <li>• Comunicação de condutores de mudança</li> </ul>
		BAI02.01	<ul style="list-style-type: none"> <li>• Critérios de aceite confirmados pelas partes interessadas</li> <li>• Repertório de definição de requisitos</li> </ul>	<ul style="list-style-type: none"> <li>• Comunicações da alta administração demonstrando o compromisso com a mudança</li> </ul>
		BAI02.03	<ul style="list-style-type: none"> <li>• Ações de mitigação de risco</li> <li>• Registro de risco de requisitos</li> </ul>	
		BAI03.01	<ul style="list-style-type: none"> <li>• Especificação de alto nível aprovada</li> </ul>	
		BAI03.02	<ul style="list-style-type: none"> <li>• Especificação detalhada aprovada</li> </ul>	

# COBIT® 5 : HABILITANDO PROCESSOS

## BAI05 Práticas de Processo, Entradas/Saídas e Atividades

### Atividades

01 Avaliar o escopo e o impacto da mudança esperada, as partes interessadas afetadas, a natureza do impacto e o envolvimento necessário de cada grupo de partes interessadas, a prontidão e habilidade para adotar a mudança.

02 Identificar, alavancar e comunicar os pontos fracos, eventos negativos, riscos, insatisfação de clientes e problemas de negócio, bem como os benefícios iniciais, oportunidades futuras e recompensas, vantagens competitivas, como uma fundação para estabelecer o desejo pela mudança.

03 Publicar comunicados chaves do comitê executivo ou CEO para demonstrar o compromisso com a mudança.

04 Prover liderança visível da alta administração para estabelecer a direção e alinhar, motivar e inspirar as partes interessadas a desejarem a mudança.

### Prática de Gestão

### Entradas

### Saídas

#### BAI05.02 Formar um time de implementação efetivo.

Estabelecer um time de implementação efetivo reunindo os membros apropriados, adquirindo a confiança, e estabelecendo objetivos comuns e métricas de efetividade.

### De

### Descrição

### Descrição

### Para

- Critérios de aceite confirmados pelas partes interessadas.

- Time de implementação e papéis

BAI01.04

- Visão comum e objetivos

BAI01.02

### Atividades

01 Identificar e reunir um time central de implementação que inclua os membros apropriados do negócio e TI com a capacidade de despender o tempo necessário e contribuir com conhecimento, experiência, credibilidade e autoridade. Considerar a inclusão de partes externas como consultores para prover uma visão independente ou para endereçar lacunas de conhecimento. Identificar agentes de mudança em potencial em diferentes partes da corporação com quem o time central pode contar para suportar a visão e cascatare as mudanças.

02 Criar confiança entre o time central de implementação por meio de eventos cuidadosamente planejados com comunicação efetiva e atividades em conjunto.

03 Desenvolver uma visão comum e objetivos que suportem os objetivos corporativos.

### Prática de Gestão

### Entradas

### Saídas

#### BAI05.03 Comunicar a visão desejada.

Comunicar a visão desejada para a mudança na linguagem dos que serão afetados por ela. A comunicação deve ser feita pela alta administração e incluir o racional, os benefícios, a mudança, os impactos da realização da mudança, a visão, o cronograma e o envolvimento requerido das diversas partes interessadas.

### De

### Descrição

### Descrição

### Para

- Plano de comunicação da visão

BAI01.04

- Comunicação da visão

BAI01.05

### Atividades

01 Desenvolver o plano de comunicação da visão para endereçar os principais grupos de audiência, seus perfis comportamentais e requisitos de informação, canais de comunicação e princípios.

02 Entregar a comunicação em níveis apropriados da corporação de acordo com o plano.

03 Reforçar a comunicação através de múltiplas reuniões e repetições.

04 Verificar o entendimento da visão desejada e responder a quaisquer problemas destacados pela equipe.

05 Responsabilizar todos os níveis de liderança pela demonstração da visão.

### Prática de Gestão

### Entradas

### Saídas

#### BAI05.04 Empoderar participantes e identificar vitórias de curto prazo.

Empoderar aqueles com papéis de implantação assegurando que as responsabilidades sejam atribuídas, treinamentos são ministrados, estruturas organizacionais e processos de RH sejam alinhados. Identificar e comunicar vitórias de curto prazo que podem ser conquistadas e são importantes do ponto de vista de gestão de mudanças.

### De

### Descrição

### Descrição

### Para

- Estrutura Organizacional da Organização

- Objetivos de desempenho alinhados de RH

APO07.04

- Ganhos de curto prazo identificados

BAI01.04

- Comunicação dos benefícios

BAI01.06

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI05 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
01 Identificar as estruturas organizacionais compatíveis com a visão; se requerido, realizar mudanças para assegurar o alinhamento.				
02 Planejar as necessidades do pessoal para desenvolver as competências apropriadas e atitudes para sentir o empoderamento.				
03 Alinhar os processos de RH e os sistemas de mensuração (ex.: avaliação de performance, decisões de compensação, decisões de promoção, recrutamento e seleção) para suportar a visão				
04 Identificar e gerenciar líderes que continuem a resistir à mudança necessária.				
05 Identificar, priorizar e entregar oportunidades para vitórias de curto prazo. Essas podem ser relacionadas às áreas com dificuldades conhecidas ou fatores externos que devem ser endereçados urgentemente.				
06 Alavancar as vitórias de curto prazo conquistadas comunicando os benefícios aos impactados e mostrando que a visão está encaminhada. Afinar a visão, manter os líderes comprometidos e manter o impeto.				

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI05.05 Habilitar a operação e uso.</b> Planejar e implementar todos os aspectos de uso, técnicos e operacionais de forma que todos os que estão envolvidos no ambiente futuro possam exercer suas responsabilidades.	BAI03.03	• Componentes de solução documentados	• Plano de operação e uso	APO08.04 BAI08.04 DSS01.01 DSS01.02 DSS06.02
	BAI03.10	• Componentes de solução atualizados e documentação relacionada	• Resultados e medidas de sucesso	APO08.05 BAI07.07 BAI07.08 MEA01.03

Atividades				
01 Desenvolver um plano para operação e uso da mudança que comunica e constrói sobre as vitórias de curto prazo conquistadas, endereça aspectos comportamentais e culturais da transição ampla, e aumenta o comprometimento e engajamento. Assegurar que o plano cobre uma visão holística da mudança e provê documentação (ex.: procedimentos), mentoring, treinamento, instrução, transferência de conhecimentos, suporte pós-implementação e suporte contínuo.				
02 Implementar o plano de operação e uso. Definir e acompanhar as medidas de sucesso, incluindo medidas rígidas de negócio e de percepção que indiquem como as pessoas se sentem em relação à mudança, conduzindo ações de remediação quando necessário.				

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI05.06 Embutir novas abordagens.</b> Enravar novas abordagens acompanhando as mudanças implementadas, avaliando a efetividade do plano de operação e uso e sustentando a conscientização através da comunicação contínua. Tomar medidas corretivas quando apropriado, que podem incluir forçar cumprir com a conformidade.			• Resultados de auditorias de conformidade	MEA02.02 MEA03.03
			• Comunicações de conscientização	Interno
			• Resultados de avaliações de performance do RH	APO07.04

Atividades				
01 Celebrar as conquistas e implementar programas de recompensa e reconhecimento para reforçar a mudança.				
02 Utilizar sistemas de medição de desempenho para identificar causas raiz para baixa adoção de medidas corretivas.				
03 Tornar os proprietários de processos responsáveis pelas operações do dia-a-dia.				
04 Conduzir auditorias de conformidade para identificar as causas raiz da não adoção e ações corretivas recomendadas.				
05 Prover conscientização contínua pela comunicação frequente da mudança e de sua adoção.				

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI05.07 Manter as mudanças.</b> Sustentar as mudanças por meio de treinamento efetivo a novo pessoal, campanhas de comunicação contínua, comprometimento da alta administração, adoção de monitoramento e compartilhamento de lições aprendidas na corporação.			• Planos de transferência de conhecimento	BAI08.03 BAI08.04
			• Comunicação do comprometimento da administração	Interno
			• Revisões de uso operacional	MEA02.02

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## BAI05 Práticas de Processo, Entradas/Saídas e Atividades

### Atividades

- 01 Prover mentoring, treinamento, instrução e transferência de conhecimentos para novo pessoal para sustentar a mudança.
- 02 Sustentar e reforçar a mudança através da comunicação regular demonstrando o comprometimento da alta administração.
- 03 Conduzir revisões periódicas de operação e uso da mudança e identificar melhorias.
- 04 Capturar lições aprendidas relacionadas à implementação da mudança e compartilhar o conhecimento através da corporação.

## BAI05 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
	Kotter, John; Leading Change, Harvard Business School Press, USA, 1996

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI06 Gerenciar Mudanças		Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Gerenciar todas as mudanças de maneira controlada, incluindo mudanças normais e manutenções de emergência relacionadas aos processos de negócio, aplicações e infraestrutura. Isso inclui mudanças em padrões e procedimentos, análises de impacto, priorização e autorização, mudanças emergenciais, acompanhamento, reporte, fechamento e documentação.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
Objetivos de TI		Métricas Relacionadas
04 Gestão de risco organizacional de TI		<ul style="list-style-type: none"> <li>Percentual de processos de negócio críticos, serviços de TI e programas de negócio habilitados por TI cobertos pela avaliação de risco</li> <li>Quantidade de incidentes significativos relacionados à TI que não foram identificados na avaliação de riscos</li> <li>Percentual de avaliações de risco corporativas incluindo riscos relacionados à TI</li> <li>Frequência de atualizações do perfil de risco</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio		<ul style="list-style-type: none"> <li>Quantidade de interrupções em processos de negócio devido a incidentes de serviços de TI</li> <li>Percentual de partes interessadas do negócio satisfeitas com o fato de que a entrega de serviços de TI está de acordo com os níveis de serviço previamente acordados</li> <li>Percentual de usuários satisfeitos com a qualidade do serviço de TI</li> </ul>
10 Segurança da informação, infraestrutura de processamento e aplicativos		<ul style="list-style-type: none"> <li>Quantidade de incidentes de segurança causando perdas financeiras, interrupções de negócio e embaraço público</li> <li>Quantidade de serviços de TI com requisitos de segurança pendentes</li> <li>Tempo para conceder, modificar e remover privilégios de acesso, comparados com os acordos de nível de serviço</li> <li>Frequência de avaliações de segurança contra os últimos padrões e procedimentos</li> </ul>
<b>Objetivos e Métricas do Processo</b>		
Objetivo do Processo		Métricas Relacionadas
01 Mudanças autorizadas são efetuadas tempestivamente e com erros mínimos.		<ul style="list-style-type: none"> <li>Quantidade de retrabalho causado por mudanças que falharam</li> <li>Tempo e esforço reduzidos para realizar mudanças</li> <li>Quantidade e intervalo de tempo das requisições de mudança pendentes</li> </ul>
02 Avaliações de impacto revelam o efeito das mudanças em todos os componentes afetados.		<ul style="list-style-type: none"> <li>Percentual de mudanças mal sucedidas devido a análises de impacto inadequadas</li> </ul>
03 Todas as mudanças emergenciais são revisadas e autorizadas após a mudança.		<ul style="list-style-type: none"> <li>Percentual do total de mudanças que são emergenciais</li> <li>Número de mudanças emergenciais não autorizadas após a mudança</li> </ul>
04 Partes interessadas chave são mantidas informadas sobre todos os aspectos da mudança.		<ul style="list-style-type: none"> <li>Avaliações de satisfação sobre a comunicação pelas partes interessadas.</li> </ul>

# COBIT® 5 : HABILITANDO PROCESSOS

BAI06 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês: Diretivos (Projeto e Programa)	Escrítorio de Programas e Projetos (PMO)	Escrítorio de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>BAI06.01</b> Avaliar, Priorizar e Autorizar as requisições de mudança.					<b>A R</b>			<b>C</b>	<b>C</b>						<b>C</b>	<b>C</b>	<b>R</b>	<b>C</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>C</b>	<b>R</b>	<b>C</b>		
<b>BAI06.02</b> Gerenciar mudanças emergenciais.					<b>A I</b>				<b>C</b>							<b>C</b>	<b>C</b>	<b>R</b>	<b>I</b>	<b>R</b>	<b>R</b>		<b>I</b>	<b>C</b>		
<b>BAI06.03</b> Acompanhar e reportar o status					<b>C R</b>		<b>C</b>											<b>A</b>	<b>R</b>	<b>R</b>		<b>R</b>				
<b>BAI06.04</b> Fechar e documentar mudanças					<b>A R</b>		<b>R</b>	<b>C</b>								<b>C</b>	<b>C</b>	<b>R</b>	<b>C</b>	<b>R</b>	<b>R</b>	<b>I</b>	<b>I</b>			

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI06 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI06.01 Avaliar, Priorizar e Autorizar as requisições de mudança.</b> Avaliar todas as requisições de mudança para determinar o impacto nos processos de negócio e serviços de TI, e avaliar se a mudança vai afetar o ambiente operacional e introduzir riscos inaceitáveis. Assegurar que as mudanças são registradas, priorizadas, categorizadas, avaliadas, autorizadas, planejadas e agendadas.	BAI03.05	• Componentes de solução configurados e integrados	• Análises de impacto	Interno
	DSS02.03	• Requisições de serviço aprovadas	• Requisições de mudança aprovadas	BAI07.01
	DSS03.03	• Soluções propostas para erros conhecidos		
	DSS03.05	• Soluções sustentáveis identificadas	• Cronograma e plano de mudança	BAI07.01
	DSS04.08	• Mudanças de plano aprovadas		
	DSS06.01	• Recomendações e análises de causa raiz		

#### Atividades

- 01 Requisições formais de mudança para permitir aos donos de processos de negócio e TI a requisitar mudanças em processos de negócio, infraestrutura, sistemas ou aplicações. Assegurar que todas as mudanças são iniciadas somente através do processo de requisição de mudanças.
- 02 Categorizar todas as requisições de mudança (ex.: processos de negócio, infraestrutura, sistemas operacionais, redes, sistemas de aplicação, softwares de aplicação de prateleira adquiridos) e relacionar os itens de configuração por elas afetados.
- 03 Priorizar todas as requisições com base em requisitos de negócio e técnicos, recursos requeridos, e razões regulatórias, contratuais e legais para a mudança solicitada.
- 04 Planejar e avaliar todas as requisições de forma estruturada. Incluir análise de impacto em processos de negócio, infraestrutura, sistemas e aplicações, planos de continuidade de negócio e provedores de serviço para assegurar que todos os componentes afetados foram identificados. Avaliar a probabilidade de afetar adversamente o ambiente operacional e o risco de implementação da mudança. Considerar implicações de segurança, legais, contratuais e de conformidade da mudança requisitada. Considerar também as interdependências entre as mudanças. Envolver os proprietários de processo de negócio nos processos de avaliação,

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**BAI06 Práticas de Processo, Entradas/Saídas e Atividades**

**05 Formalmente aprovar** cada mudança pelos proprietários de processo de negócio, gestores de serviço e partes interessadas técnicas de TI, conforme apropriado. Mudanças que são de baixo risco e relativamente frequentes devem ser pré-aprovadas como mudanças padrão.

**06 Planejar e agendar** todas as mudanças aprovadas.

**07 Considerar o impacto** de provedores de serviço contratados (ex.: processamento de negócio terceirizado, infraestrutura, desenvolvimento de aplicações e serviços compartilhados) no processo de gestão de mudanças, incluindo a integração de processos de gestão de mudanças organizacionais com os processos de gestão de mudança de prestadores de serviço e o impacto em contratos e acordos de nível de serviço.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI06.02 Gerenciar mudanças emergenciais.</b> Cuidadosamente gerir mudanças emergenciais para minimizar incidentes futuros e assegurar que a mudança foi controlada e é implementada de forma segura. Verificar que as mudanças emergenciais são apropriadamente avaliadas e autorizadas após a mudança.			• Revisão pós-implementação de mudanças emergenciais	Interno

**Atividades**

**01 Assegurar** que um procedimento documentado existe para declarar, avaliar, aprovar e autorizar após a mudança e registro da mudança emergencial.

**02 Verificar** que toda a concessão de acesso emergencial para implementação de mudanças seja autorizada apropriadamente, documentada e revogada após a implementação.

**03 Monitorar** todas as mudanças emergenciais, conduzir revisões pós-implementação envolvendo todas as partes interessadas. A revisão deve considerar e iniciar ações corretivas com base em causas raiz como problemas com processos de negócio, desenvolvimento e manutenção de sistemas de aplicação, ambientes de teste e desenvolvimento, manuais e documentação e integridade de dados.

**04 Definir** o que constitui uma mudança emergencial.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI06.03 Acompanhar e reportar o status.</b> Manter um Sistema de acompanhamento e relatório para documentar as mudanças rejeitadas, comunicar o status das mudanças aprovadas, em andamento e completas. Assegurar que as mudanças aprovadas são implementadas conforme planejado.	BAI03.09	• Registro de todas as requisições de mudança aprovadas e implementadas	• Relatórios de status das requisições de mudança	BAI01.06 BAI10.03

**Atividades**

**01 Categorizar** as requisições de mudança no processo de acompanhamento (ex.: rejeitadas, aprovadas, mas não iniciadas, aprovadas em curso e fechadas).

**02 Implementar** relatórios de status das mudanças com métricas de desempenho para permitir a administração de revisar e monitorar tanto o status detalhado das mudanças como de forma geral (ex.: Análise de tempo das requisições de mudança). Assegurar que os relatórios de status têm trilhas de auditoria para que mudanças possam ser acompanhadas após sua concepção até um eventual cancelamento.

**03 Monitorar** mudanças em aberto para assegurar que todas as mudanças aprovadas são fechadas tempestivamente, dependendo da prioridade.

**04 Manter** um Sistema de acompanhamento e relatório para todas as requisições de mudança.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI06.04 Fechar e documentar mudanças.</b> Sempre que uma mudança for implementada, atualizar a documentação da solução e do usuário afetados de forma apropriada.			• Documentação da mudança	Interno

**Atividades**

**01 Incluir** mudanças na documentação (ex.: procedimentos operacionais de negócio e de TI, documentação de recuperação de desastres e continuidade de negócio, informações de configuração, documentação de aplicação, telas de ajuda e materiais de treinamento) dentro do procedimento de gestão de mudanças como parte integral da mudança.

**02 Definir** a retenção apropriada para a documentação da mudança e documentação do usuário.

**03 Submeter** a documentação ao mesmo nível de revisão que a própria mudança.

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## • BAI06 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	9.2 Gestão de Mudanças
ITIL V3 2011	Transição de Serviços, 4.2 Gestão de Mudanças

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

<b>BAI07 Gerenciar Aceitação e Transição da Mudança</b>		<b>Área: Gestão</b> <b>Domínio: Construir, Adquirir e Implementar</b>
<b>Descrição do Processo</b>		Aceitar formalmente e fazer novas soluções operacionais, incluindo planejamento da implementação, sistema e conversão de dados, testes de aceitação, comunicação, preparação para liberação, promoção para a produção de processos de negócios novos ou alterados e serviços de TI, suporte inicial de produção e a revisão pós implementação.
<b>Declaração de Propósito do Processo</b>		Implementar soluções de forma segura e em linha com as expectativas e resultados acordados.
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
Objetivos de TI	<b>Métricas Relacionadas</b>	
08 Uso adequado de aplicativos, informações e soluções tecnológicas	<ul style="list-style-type: none"> <li>Percentual de donos de processos de negócios satisfeitos com o suporte dos produtos de TI e serviços</li> <li>Nível de compreensão dos usuários de negócio sobre como as soluções de tecnologia suportam seus processos</li> <li>Nível de satisfação dos usuários de negócio com treinamentos e manuais de usuário</li> <li>Valor Presente Líquido (VPL) mostrando o nível de satisfação do negócio com a qualidade e utilidade das soluções de tecnologia</li> </ul>	
12 Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia	<ul style="list-style-type: none"> <li>Número de Incidentes em processos de negócio causados por erros de integração na tecnologia</li> <li>Número de mudanças em processos de negócio que precisaram ser atrasadas ou retrabalhadas por causa de problemas de integração da tecnologia</li> <li>Número de programas de negócio habilitados por TI atrasados ou que incorreram em custo adicional por problemas de integração da tecnologia</li> <li>Número de aplicações ou infraestruturas críticas operando em silos não integrados</li> </ul>	
<b>Objetivos e Métricas do Processo</b>		
Objetivo do Processo	<b>Métricas Relacionadas</b>	
01 Os testes de aceitação sejam aprovados pelas partes interessadas e levem em conta todos os aspectos dos planos de implementação e conversão.	<ul style="list-style-type: none"> <li>Percentual de partes interessadas satisfeitas com a integralidade do processo de teste</li> </ul>	
02 Liberações estão prontas para a promoção em produção com prontidão e suporte das partes interessadas.	<ul style="list-style-type: none"> <li>número e percentagem de liberações não prontas para o lançamento dentro do cronograma</li> </ul>	
03 Liberações são promovidas com sucesso, são estáveis e atingem as expectativas.	<ul style="list-style-type: none"> <li>Número ou percentagem de liberações que não conseguem se estabilizar dentro de um período aceitável</li> <li>Porcentagem de liberações causando indisponibilidade</li> </ul>	
04 As lições aprendidas para contribuir para liberações futuras.	<ul style="list-style-type: none"> <li>Número e percentagem de análises de causa raiz concluídas</li> </ul>	

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

BAI07 Tabela RACI

Prática de Gestão	Conselho de Administração	Dirutor Executivo (Presidente) (CEO)	Dirutor Financeiro (CFO)	Dirutor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escrítorio de Programas e Projetos (PMO)	Escrítorio de Gestão do valor da TI	Dirutor de Riscos (CRO)	Dirutor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Dirutor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
BAI 07.01 Estabelecer um plano de implementação					C R	A C		R					C C	R C R C				R R R R C								
<b>BAI07.02</b> Planejar processos de negócios, sistema e conversão de dados.					C R	A C	R						C C	R C R C				R R R R C								
<b>BAI07.03</b> Planejar testes de aceitação					A R	R I							C I	R R		I R R C										
<b>BAI07.04</b> Estabelecer um ambiente de teste.					A R	R I							I	R R		I R R C										
<b>BAI07.05</b> Realizar testes de aceitação					A R	R I							I	R R		I R R C										
<b>BAI07.06</b> Promover para a produção e gerir os lançamentos.					R	A I							I	R R		R I I I										
<b>BAI 07.07</b> Fornecer suporte de produção inicial.					R	A I							I	R R		R I I I										
<b>BAI07.08</b> Realizar uma revisão pós-implementação					R	A I							C C I	R R		R C I I										

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI07 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI 07.01 Estabelecer um plano de implementação.</b> Estabelecer um plano de implementação que abrange sistema e conversão de dados, critérios de aceitação de teste, comunicação, formação, preparação da liberação, a promoção da produção, apoio antecipado à produção, um plano de recuperação / reversão e uma revisão pós-implementação. Obter a aprovação de partes relevantes.	BAI01.09	<ul style="list-style-type: none"> <li>• Plano de gerenciamento da qualidade</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de implementação aprovado</li> </ul>	Interno
	BAI06.01	<ul style="list-style-type: none"> <li>• Plano de mudança e cronograma</li> <li>• Solicitações de mudança aprovadas</li> </ul>	<ul style="list-style-type: none"> <li>• Implementação do processo de recuperação e reversão</li> </ul>	Interno
<b>Atividades</b>				
01 Criar um plano de implementação que reflete a estratégia de implementação abrangente, a sequência das etapas de implementação, requisitos de recursos, interdependências, os critérios para a gestão da aceitação da implementação em produção, os requisitos de verificação da instalação, a estratégia de transição para apoio à produção e atualização de BCPs.				
02 Confirmar se todos os planos de execução são aprovados pelas partes interessadas técnicas e de negócios e revisado pela auditoria interna, conforme o caso.				
03 Obter o compromisso dos provedores de solução externos para o seu envolvimento em cada etapa da implementação.				
04 Identificar e documentar o processo de reversão e recuperação.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI07 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI07.02 Planejar processos de negócios, sistema e conversão de dados.</b> Preparar para os processos de negócios, dados de serviços de TI e migração da infraestrutura como parte de métodos de desenvolvimento da empresa, incluindo trilhas de auditoria e um plano de recuperação para falhas na migração.			• Plano de migração	DSS06.02
<b>Atividades</b>				
01 Definir um processo de negócio, um plano de migração da infraestrutura e serviços de TI. Considerar, por exemplo, hardware, redes, sistemas, software, dados de transações, arquivos mestres, backups e arquivos, interfaces com outros sistemas (internos e externos), possíveis requisitos de conformidade, procedimentos de negócios e documentação de sistemas, no desenvolvimento do plano.				
02 Considerar todos os ajustes necessários nos procedimentos, incluindo papéis e responsabilidades revistos e procedimentos de controle, no plano de conversão de processos de negócios				
03 Incorporar no plano de conversão de dados, métodos para coletar, converter e verificar dados a serem convertidos e identificar e resolver quaisquer erros encontrados durante a conversão. Incluir comparando os dados originais e convertidos para completude e integridade.				
04 Verificar se o plano de conversão de dados não requer alterações nos valores de dados a menos que absolutamente necessário por razões de negócios. Documentar mudanças feitas nos valores dos dados e assegurar a aprovação do proprietário dos dados de processos de negócios.				
05 Ensaiar e testar a conversão antes de tentar uma conversão em produção				
06 Considerar o risco de problemas de conversão, planejamento da continuidade de negócios e processos de recuperação do processo de negócios, plano de migração de dados e infraestrutura onde há gestão de riscos, necessidades de negócios ou requisitos de conformidade / regulatórios.				
07 Coordenar e verificar o calendário e a completude da conversão para que haja uma transição suave e contínua, sem perda de dados de transação. Quando necessário, na ausência de qualquer outra alternativa, congelar as operações em produção.				
08 Plano para fazer backup de todos os sistemas e dados obtidos no ponto antes da conversão. Manter trilhas de auditoria para permitir a reconversão e garantir que há um plano de recuperação que abrange a reversão da migração e retorno do processamento em caso de falha.				
09 Plano de retenção do backup e dados arquivados em conformidade com as necessidades do negócio e os requisitos regulatórios ou de conformidade.				
Prática de Gestão	Entradas		Saídas	
<b>BAI07.03 Planejar testes de aceitação.</b> Estabelecer um plano de teste com base em padrões da empresa que definem papéis, responsabilidades e critérios de entrada e saída. Garantir que o plano seja aprovado pelas partes interessadas.	De	Descrição	Descrição	Para
	BAI01.09	• Requisitos para a verificação independente dos resultados	• Plano de aceitação de teste aprovado	BAI01.04 BAI01.08
	BAI03.07	• Procedimentos de teste • Plano de teste		
	BAI03.08	• Comunicação do resultado do teste • Logs de trilhar de auditoria do resultado do teste		

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## BAI07 Práticas de Processo, Entradas/Saídas e Atividades

Atividades
01 Desenvolver e documentar o plano de teste, alinhado com o programa e o plano de qualidade do projeto e padrões organizacionais relevantes. Comunicar e consultar com os donos dos processos de negócios apropriados e as partes interessadas de TI.
02 Garantir que o plano de teste reflete uma avaliação de risco do projeto e que todos os requisitos funcionais e técnicos são testados. Com base na avaliação do risco de fracassos e as falhas do sistema em execução, o plano deve incluir requisitos de desempenho, stress, usabilidade, piloto e testes de segurança.
03 Garantir que o plano de teste aborda a necessidade potencial de acreditação interna ou externa de resultados do processo de teste (por exemplo, requisitos regulatórios financeiros).
04 Garantir que o plano de teste identifica os recursos necessários para a execução de testes e avaliação dos resultados. Exemplos de recursos incluem a construção de ambientes de teste e uso do tempo da equipe para o grupo de teste, incluindo a eventual substituição temporária de pessoal de teste em ambientes de produção ou de desenvolvimento. Garantir que os interessados sejam consultados sobre as implicações de recursos do plano de teste.
05 Garantir que o plano de teste identifique fases de ensaio adequadas às exigências operacionais e ao ambiente. Exemplos de tais fases de teste incluem teste de unidade, teste do sistema, teste de integração, teste de aceitação do usuário, teste de desempenho, teste de esforço, teste de conversão de dados, teste de segurança, teste de prontidão operacional, backup e teste de recuperação.
06 Verificar se o plano de teste considera a preparação para o teste (incluindo a preparação do local), requisitos de treinamento, instalação ou uma atualização de um ambiente de teste definido, planejamento / performance / documentação / retenção de casos de teste, erro e problemas na execução, correção e acionamento e formal aprovação.
07 Garantir que o plano de teste estabelece critérios claros para medir o sucesso da realização a cada fase de testes. Consultar os proprietários de processos de negócio e de TI na definição dos critérios de sucesso. Determinar que o plano estabelece procedimentos de remediação quando os critérios de sucesso não forem atendidos (por exemplo, em caso de falhas significativas na fase de testes, o plano fornece orientação sobre a possibilidade de avançar para a próxima fase, interromper o teste ou adiar a implementação).
08 Confirme que todos os planos de teste estão aprovados pelas partes interessadas, incluindo donos de processos de negócios e de TI, conforme o caso. Exemplos de tais agentes são gerentes de desenvolvimento de aplicações, gerentes de projeto e usuários finais de processos de negócio.

### Prática de Gestão

### Entradas

### Saídas

Prática de Gestão	De	Descrição	Descrição	Para
<b>BAI07.04 Estabelecer um ambiente de teste.</b> Definir e estabelecer um ambiente de teste seguro e representativo do processo de negócios planejado e das operações no ambiente de TI, desempenho e capacidade, segurança, controles internos, práticas operacionais, requisitos de qualidade de dados e privacidade e cargas de trabalho.			• Testar dados	Interno

### Atividades

01 Criar um banco de dados com dados de teste que são representativos do ambiente de produção. Higienizar os dados utilizados no ambiente de teste para o ambiente de produção de acordo com as necessidades do negócio e padrões organizacionais (por exemplo, considerar se conformidades ou requisitos regulamentares obrigam o uso de dados de higienizados).
02 Proteger os dados de teste sensíveis e resultados contra qualquer divulgação, incluindo o acesso, retenção, armazenamento e destruição. Considere o efeito da interação dos sistemas organizacionais com os de terceiros.
03 Coloque em prática um processo para permitir a retenção adequada ou eliminação dos resultados dos testes, mídia e outra documentação associada para permitir a avaliação adequada e posterior análise conforme exigido pelo plano de teste. Considere o efeito de requisitos regulamentares ou de conformidade.
04 Garantir que o ambiente de teste é representativo do futuro do negócio e do panorama operacional, incluindo procedimentos de processos de negócio e funções, o stress da carga de trabalho provável, sistemas operacionais, softwares aplicativos necessários, sistemas de gerenciamento de banco de dados e de rede e infraestrutura de computação encontrados no ambiente de produção.
05 Garantir que o ambiente de teste é seguro e capaz de interagir com sistemas de produção.

### Prática de Gestão

### Entradas

### Saídas

Prática de Gestão	De	Descrição	Descrição	Para
<b>BAI07.05 Realizar testes de aceitação.</b> Teste as mudanças de forma independente, em conformidade com o plano de teste definido antes da migração para o ambiente operacional de produção.			• Log dos resultados do teste • Avaliação dos resultados da aceitação	Interno BAI01.06

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI07 Práticas de Processo, Entradas/Saídas e Atividades

Atividades			
01 Revise o log categorizado de erros encontrados no processo de teste pela equipe de desenvolvimento, verificando-se que todos os erros foram corrigidos ou formalmente aceitos.			
02 Avaliar a aceitação final contra os critérios de sucesso e interpretar os resultados finais de testes de aceitação. Apresentá-los de uma forma que seja compreensível para donos de processos de negócio e de TI para que uma revisão e avaliação pode ter lugar.			
03 Aprovar a aceitação com assinatura formal por parte dos donos de processos de negócio, terceiros (conforme o caso) e partes interessadas de TI antes da promoção para a produção.			
04 Garantir que o teste de mudanças é realizada de acordo com o plano de testes. Garantir que o teste foi desenhado e realizado por um grupo de teste independente da equipe de desenvolvimento. Considerar a medida em que os proprietários de processos de negócio e usuários finais estão envolvidos no grupo de teste. Certifique-se de que o teste é realizado apenas dentro do ambiente de teste.			
05 Garantir que os testes e os resultados esperados estão em conformidade com os critérios de sucesso definidos e estabelecidos no plano de teste.			
06 Considerar o uso de instruções de teste claramente definidas (scripts) para implementar os testes. Garantir que o grupo de teste independente avalia e aprova cada script de teste para confirmar que ele aborda adequadamente os critérios de sucesso de ensaio previstos no plano de teste. Considerar o uso de scripts para verificar a medida em que o sistema atende os requisitos de segurança.			
07 Considerar o equilíbrio adequado entre os testes com scripts automatizados e testes com interação do usuário.			
08 Realizar testes de segurança em conformidade com o plano de teste. Medir a extensão das deficiências de segurança ou lacunas. Considere o efeito de incidentes de segurança desde a construção do plano de teste. Considerar o efeito sobre o acesso e controles de fronteira.			
09 Realizar testes de segurança em conformidade com o plano de teste. Medir a extensão das deficiências de segurança ou lacunas. Considere o efeito de incidentes de segurança desde a construção do plano de teste. Considerar o efeito sobre o acesso e controles de fronteira.			
10 Ao realizar testes, assegurar que os elementos recuperação e de reversão do plano de teste foram abordadas.			
11 Identificar, registrar e classificar erros (por exemplo, menores, significativos, de missão crítica) durante os testes. Garantir que uma trilha de auditoria de resultados do teste está disponível. Comunicar os resultados dos testes para as partes interessadas de acordo com o plano de teste para facilitar a correção de bugs e melhoria da qualidade.			

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
BAI07.06 Promover para a produção e gerir os lançamentos.			• Plano de liberações	BAI10.01
Promover o aceite da solução para os negócios e operações. Se for o caso, executar a solução como uma implementação piloto ou em paralelo com a solução antiga por um período definido e comparar o comportamento e resultados. Se ocorrerem problemas significativos, reverter para o ambiente original com base no plano recuperação de recuperação / recuperação. Gerenciar lançamentos de componentes da solução.			• Log de liberações	Interno

Atividades			
01 Preparar para a transferência de processos de negócio e serviços de apoio, aplicações e infra-estrutura de teste para o ambiente de produção de acordo com a gestão de mudança organizacional			
02 Determinar o grau de implementação piloto de processamento paralelo dos antigos e novos sistemas em linha com o plano de implementação.			
03 Atualizar prontamente o processo de negócios relevante e documentação do sistema e os documentos de informações de configuração e plano de contingência, conforme o caso.			
04 Garantir que todas as bibliotecas de mídia são atualizadas prontamente com a versão do componente da solução que está sendo transferido do teste para o ambiente de produção. Arquivar a versão existente e sua documentação de apoio. Garantir que a promoção para a produção de sistemas, software e infraestrutura está sob controle de configuração.			
05 No caso da distribuição de componentes da solução ser realizada eletronicamente, controlar a distribuição automatizada para garantir que os usuários são notificados e a distribuição ocorre apenas para destinos autorizados e identificados corretamente. Incluir no processo de liberação, os procedimentos de reversão para permitir que a distribuição de alterações seja revista em caso de uma avaria ou erro.			
06 No caso de distribuição de forma física, manter um registro formal dos itens que foram distribuídos, para quem, onde eles foram			

# COBIT® 5 : HABILITANDO PROCESSOS

## BAI07 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI 07.07 Fornecer suporte de produção inicial.</b> Fornecer apoio inicial aos usuários e operações de TI por um período de tempo para lidar com problemas e ajudar a estabilizar a nova solução.	APO11.03	<ul style="list-style-type: none"> <li>• Revisar os resultados de qualidade do serviço, incluindo feedback do cliente</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de suporte suplementar</li> </ul>	APO08.04 APO08.05 DSS02.04
	BAI05.05	<ul style="list-style-type: none"> <li>• Medidas de sucesso e resultados</li> </ul>		
<b>Atividades</b>				
01 Fornecer recursos adicionais, conforme necessário, para os usuários finais e pessoal de apoio até que o lançamento tenha se estabilizado.				
02 Fornecer recursos de sistemas de TI adicionais, conforme necessário, até que a liberação esteja em um ambiente operacional estável.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI07.08 Realizar uma revisão pós-implementação.</b> Conduzir uma revisão pós-implementação para confirmar a conclusão e os resultados, identificar as lições aprendidas e desenvolver um plano de ação. Avallar e verificar o desempenho real e os resultados do serviço novo ou modificado contra o desempenho e os resultados previstos (isto é, o serviço esperado pelo usuário ou cliente).	APO11.04	<ul style="list-style-type: none"> <li>• Os resultados dos controles de qualidade e auditorias</li> </ul>	<ul style="list-style-type: none"> <li>• Relatório de revisão pós-implementação</li> </ul>	BAI01.13 BAI01.14
	APO11.05	<ul style="list-style-type: none"> <li>• Causas raiz de falhas de qualidade na entrega</li> <li>• Resultados da solução e monitoramento da qualidade na entrega do serviço</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de ações corretivas</li> </ul>	BAI01.13 BAI01.14
	BAI05.05	<ul style="list-style-type: none"> <li>• Medidas de sucesso e resultados</li> </ul>		
<b>Atividades</b>				
01 Estabelecer procedimentos para garantir que a revisão pós-implementação identifique, avalie e informe a medida que:				
<ul style="list-style-type: none"> <li>• Requisitos da empresa foram cumpridos</li> <li>• Benefícios esperados foram realizados</li> <li>• O sistema é considerado utilitário</li> <li>• Expectativas internas e externas das partes interessadas sejam atendidas</li> <li>• Impactos inesperados sobre a empresa tenham ocorrido</li> <li>• Risco chave é mitigado</li> <li>• Os processos de gerenciamento de mudanças, de instalação e de acreditação foram realizados de forma eficaz e eficiente</li> </ul>				
02 Consulte donos processos de negócios e gerenciamento de TI na escolha técnica de métricas para a medição de sucesso e realização de requisitos e benefícios.				
03 Realizar a revisão pós-implementação, em conformidade com o processo de gestão de mudança organizacional. Envolver os donos dos processos de negócio e terceiros, conforme o caso.				
04 Considere os requisitos para a revisão pós-implementação decorrentes de negócios fora e TI (por exemplo, auditoria interna, ERM, compliance).				
05 Acordar e implementar um plano de ação para resolver questões identificadas na revisão pós-implementação. Envolver os donos dos processos de negócio e o gerenciamento técnico de TI no desenvolvimento do plano de ação.				

## BAI07 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	Processo de Gestão de Liberações
ITIL V3 2011	<ul style="list-style-type: none"> <li>• Transição de Serviço, 4.1 Planejamento e Apoio à Transição.</li> <li>• Transição de Serviço, 4.4 Gerenciamento de Liberações e Implantação.</li> <li>• Transição de Serviço, 4.5 Validação de Serviço e Testes.</li> <li>• Transição de Serviço, 4.6 Avaliação da Mudança.</li> </ul>
PMBOK	Garantia de qualidade PMBOK e processo de aceite para todos os produtos
PRINCE2	Planejamento de produto baseado no PRINCE2

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI08 Gerenciar Conhecimento		Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Manter a disponibilidade do conhecimento relevante, atual, validado e confiável para apoiar todas as atividades do processo e facilitar a tomada de decisão. Plano para a identificação, coleta, organização, manutenção, utilização e retirada do conhecimento.		
<b>Declaração de Propósito do Processo</b> Proporcionar o conhecimento necessário para suportar todos os funcionários em suas atividades de trabalho e para a tomada de decisão informada e melhoria da produtividade.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
Objetivos de TI	<b>Métricas Relacionadas</b>	
09 Agilidade de TI	<ul style="list-style-type: none"> <li>• Nível de satisfação dos executivos de negócios com a capacidade de resposta de TI às novas exigências</li> <li>• Número de processos críticos de negócio suportados por infraestrutura e aplicações up-to-date</li> <li>• Tempo médio para transformar objetivos estratégicos de TI em uma iniciativa acordada e aprovada</li> </ul>	
17 Conhecimento, experiência e iniciativas de inovação empresarial	<ul style="list-style-type: none"> <li>• Nível de conscientização dos executivos de negócio e compreensão das possibilidades de inovação de TI</li> <li>• Nível de satisfação das partes interessadas com níveis de inovação da especialização de TI e idéias</li> <li>• Número de iniciativas aprovadas resultantes de ideias inovadoras de TI</li> </ul>	
<b>Objetivos e Métricas do Processo</b>		
Objetivo do Processo	<b>Métricas Relacionadas</b>	
01 Fontes de informação são identificadas e classificadas	<ul style="list-style-type: none"> <li>• Porcentagem de categorias de informações abrangidas</li> <li>• Volume de informações classificadas</li> <li>• Percentagem de informações categorizados validadas</li> </ul>	
02 Conhecimento é utilizado e compartilhado	<ul style="list-style-type: none"> <li>• Porcentagem de conhecimento disponível realmente utilizados</li> <li>• Número de usuários treinados na utilização e compartilhamento do conhecimento</li> </ul>	
03 Compartilhamento do conhecimento é incorporado a cultura da empresa.	<ul style="list-style-type: none"> <li>• Nível de satisfação dos usuários</li> <li>• </li> </ul>	
04 O conhecimento é atualizado e melhorado para suportar os requisitos.	<ul style="list-style-type: none"> <li>• Frequência de atualização</li> </ul>	

# COBIT<sup>®</sup> 5: HABILITANDO PROCESSOS

BAI08 Tabela RACI

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BA108 Práticas de Processo, Entradas/Saídas e Atividades

BAI - Práticas de Processo, Entradas, Saídas e Atividades				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI 08.01 Consolidar e facilitar uma cultura de compartilhamento do conhecimento.</b> Conceber e implementar um esquema para nutrir e facilitar uma cultura de partilha de conhecimentos.			• Comunicações sobre o valor do conhecimento	APO01.04

## Atividades

- 01 Comunicar de forma proativa o valor do conhecimento para incentivar a criação de conhecimento, utilização, reutilização e partilha.
  - 02 Incentivar o compartilhamento e transferência de conhecimentos, identificando e alavancando fatores motivacionais.
  - 03 Criar um ambiente, ferramentas e artefatos que apoiem o intercâmbio e transferência de conhecimentos.
  - 04 Incorporar práticas de gestão do conhecimento em outros processos de TI.
  - 05 Ajusta expectativas da administração e demonstrar atitude apropriada em relação à utilidade do conhecimento e a necessidade de compartilhar o conhecimento da empresa.

### **Prática de Gestão**

Prática de Gestão	Entradas	Salidas		
	De	Descrição	Descrição	Para
<b>BAI08.02 Identificar e classificar as fontes de informação.</b> Identificar, validar e classificar diversas fontes de informação internas e externas necessárias para permitir a utilização e operação eficaz de processos	For a do COBIT	<ul style="list-style-type: none"> <li>• Requisitos de conhecimento e fontes</li> </ul>	<ul style="list-style-type: none"> <li>• Classificação das fontes de informação</li> </ul>	Interno

1

- | <b>Atividades</b>  |
|--|
| 01 Identificar os usuários potenciais do conhecimento, incluindo proprietários de informações que podem contribuir e aprovar conhecimento. Obter requisitos de conhecimentos e fontes de informação de usuários identificados.   |
| 02 Considerar os tipos de conteúdo (procedimentos, processos, estruturas, conceitos, políticas, regras, fatos, classificações), artefatos (documentos, registros, vídeo, voz), e informações estruturadas e não estruturadas (especialistas, mídias sociais, e-mail, correio de voz, RSS feeds). |
| 03 Classificar fontes de informação com base em um esquema de classificação de conteúdo (por exemplo, informações modeladas de   |

03 Classificar fontes de informação com base em um esquema de classificação de conteúdo (por exemplo, informações modelo de arquitetura). Mapear fontes de informação para o esquema de classificação.

04 Coletar, coligir e validar fontes de informação com base nos critérios de validação de informação (por exemplo, comprehensibilidade, relevância, importância, integridade, precisão, consistência, confidencialidade, vigência e confiabilidade).

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI08 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI08.03 Organizar e contextualizar informações em conhecimento.</b> Organizar informações com base em critérios de classificação. Identificar e criar relações significativas entre os elementos de informação e permitir a utilização das informações. Identificar os proprietários e definir e aplicar níveis de acesso aos recursos de conhecimento.	BAI03.03	• Componentes de solução documentados	• Reppositórios de conhecimentos publicados	APO07.03
	BAI05.07	• Planos de transferência de conhecimento		

## Atividades

- 01 Identificar atributos compartilhados e fontes de correspondência de informação, criando relações entre conjuntos de informação (marcação da informação).
- 02 Criar visões para conjuntos de dados relacionados considerando as partes interessadas e os requisitos organizacionais.
- 03 Conceber e implementar um sistema de gestão do conhecimento não estruturado e não disponível através de fontes formais (por exemplo, o conhecimento especializado).
- 04 Publicar e tornar o conhecimento acessível às partes interessadas com base em funções e mecanismos de acesso.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI08.04 Usar e compartilhar conhecimento.</b> Propagar conhecimento dos recursos disponíveis para as partes interessadas relevantes e comunicar a forma como estes recursos podem ser utilizados para atender a necessidades diferentes (por exemplo, resolução de problemas, aprendizagem, planejamento estratégico e tomada de decisão).	BAI03.03	• Componentes de solução documentados	• Banco de dados dos usuários do conhecimento	Interno
	BAI05.05	• Plano de utilização e operação		
	BAI05.07	• Planos de transferência do conhecimento	• Consciência do conhecimento e ações de formação	

## Atividades

- 01 Identificar os usuários de conhecimento em potencial por classificação conhecimento.
- 02 Transferir conhecimento para os usuários de conhecimento com base em uma análise de lacunas necessárias e técnicas de aprendizagem eficazes e ferramentas de acesso.
- 03 Educar e treinar os usuários no conhecimento disponível, no acesso ao conhecimento e uso de ferramentas de acesso.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI08.05 Avaliar e retirar informações.</b> Medir o uso e avaliar a existência e relevância das informações. Aposentar informações obsoletas			• Resultados da avaliação de uso do conhecimento	Interno
			• Regras para retirada do conhecimento	

## Atividades

- 01 Medir o uso e avaliar a utilidade, a relevância e o valor dos elementos do conhecimento. Identificar informações relacionadas que já não são relevantes para os requisitos de conhecimento da empresa.
- 02 Definir as regras para retirada e aposentadoria do conhecimento em conformidade.

## BAI08 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ITIL V3 2011	Transição de Serviço, 4.7 Gestão do Conhecimento

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

BAI09 Gerenciar Ativos	Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> Gerenciar ativos de TI através de seu ciclo de vida para se certificar de que a sua utilização proporciona valor ao custo ideal, eles permanecem operacionais (aptos para o uso), eles são contabilizados e fisicamente protegidos e aqueles bens que são fundamentais para suportar a capacidade de serviço são confiáveis e disponíveis. Gerenciar licenças de software para garantir que o número ideal é adquirido, mantidos e implementados em relação ao uso de negócios e o software instalado está em conformidade com os acordos de licenciamento.	
<b>Declaração de Propósito do Processo</b> Contabilizar todos os ativos de TI e otimizar o valor fornecido por esses ativos.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
06 Transparência dos custos de TI, benefícios e riscos	<ul style="list-style-type: none"> <li>• Porcentagem de investimento nos casos de negócios com custos e benefícios de TI claramente definidos e aprovados como esperado</li> <li>• Porcentagem de serviços de TI com custos operacionais claramente definidos e aprovados e benefícios esperados</li> <li>• Pesquisa de satisfação das partes interessadas chave quanto ao nível de transparência, compreensão e precisão das informações financeiras de TI</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>• Frequência da maturidade de capacidade e de custo de avaliações de otimização</li> <li>• Tendência dos resultados das avaliações</li> <li>• Níveis de satisfação dos executivos de negócio e TI com os custos e capacidades relacionados a TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 As licenças estão em conformidade e alinhadas com as necessidades do negócio.	<ul style="list-style-type: none"> <li>• Porcentagem de licenças utilizadas contra licenças pagas</li> </ul>
02 Ativos são mantidos em níveis ideais.	<ul style="list-style-type: none"> <li>• Número de ativos não utilizados</li> <li>• Custos de referência</li> <li>• Número de ativos obsoletos</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI09 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>BAI09.01</b> Identificar e registrar o ativo corrente		C		C											I	C	C	A	R	C						
<b>BAI09.02</b> Gerenciar ativos críticos.		C	I	C											C	C		R	R	A	R	C	C	C		
<b>BAI09.03</b> Gerenciar o ciclo de vida do ativo.					C												C	C	A	R	R					
<b>BAI09.04</b> Otimizar os custos dos ativos		R	I	C													A	R	R	R	R	R				
<b>BAI09.05</b> Gerenciar licenças				I	C										C	R	A	R	R	R	C					

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI09 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas			Saídas		
	De	Descrição	Descrição	Para		
<b>BAI09.01 Identificar e registrar o ativo corrente.</b> Manter um registro atualizado e preciso de todos os ativos de TI necessários para fornecer serviços e assegurar alinhamento com o gerenciamento de configuração e a gestão financeira.	BAI03.04	• Atualizações para inventário de ativos	• Registro de ativos	AP006.01 BAI10.03		
	BAI10.02	• Repertório de configuração	• Resultados dos controles de inventários físicos	BAI10.03 BAI10.04 DSS05.03		
			• Resultados das revisões de adequado ao uso	AP002.02		

## Atividades

- 01 Identificar todos os ativos em um registo de ativos que registra o status atual. Manter o alinhamento com os processos de gerenciamento de mudança e gerenciamento de configuração, o sistema de gerenciamento de configuração e os registros de contabilidade financeira.
- 02 Identificar os requisitos legais, regulamentares ou contratuais que precisam ser abordados durante o gerenciamento do ativo.
- 03 Verificar a existência de todos os ativos de propriedade realização de verificações de inventário físico e lógico regulares e de reconciliação, incluindo o uso de ferramentas de descoberta de software.
- 04 Verificar se os ativos estão adequados à finalidade (ou seja, em uma condição de ser útil).
- 05 Determinar em uma base regular se cada ativo continua a fornecer valor e, em caso afirmativo, estimar a vida útil estimado para a entrega de valor.
- 06 Garantir a contabilização de todos os ativos.

Prática de Gestão	Entradas			Saídas		
De	Descrição	Descrição	Para			
<b>BAI09.02 Gerenciar ativos críticos.</b> Identificar os ativos que são fundamentais no fornecimento da capacidade do serviço e tomar medidas para maximizar a sua confiabilidade e disponibilidade para apoiar as necessidades de				• Comunicação das indisponibilidades para manutenções planejadas	AP008.04	

# COBIT® 5 : HABILITANDO PROCESSOS

## BAI09 Práticas de Processo, Entradas/Saídas e Atividades

### Atividades

- 01 Identificar os ativos que são críticos no fornecimento da capacidade de serviços referenciando exigências em definições de serviços, SLAs e do sistema de gerenciamento de configuração.
- 02 Monitorar desempenho dos ativos críticos, examinando as tendências de incidentes e se necessário, tomar medidas para reparar ou substituir.
- 03 Em uma base regular, considerar o risco de falha ou necessidade de substituição de cada ativo crítico.
- 04 Manter a resiliência dos ativos críticos através da aplicação de manutenção preventiva regular, monitorar o desempenho e se necessário, proporcionar alternativas e / ou ativos adicionais para minimizar a probabilidade de fracasso.
- 05 Estabelecer um plano de manutenção preventiva para todo o hardware, considerando a análise custo benefício, as recomendações dos fornecedores, o risco de interrupção, pessoal qualificado e outros fatores relevantes.
- 06 Estabelecer contratos de manutenção envolvendo o acesso de terceiros às instalações de TI da organização no local ou fora do local das atividades (por exemplo, terceirização). Estabelecer contratos de serviços formais que contenham ou façam referência a todas as condições de segurança necessárias, incluindo processos de autorização de acesso, para garantir a conformidade com as políticas e normas de segurança da organização.
- 07 Comunicar aos clientes e usuários afetados o impacto esperado (por exemplo, restrições de desempenho) das atividades de manutenção.
- 08 Assegurar que os serviços de acesso remoto e perfis de usuário (ou outros meios utilizados para a manutenção ou diagnóstico) estão ativos somente quando necessário.
- 09 Incorporar tempo de inatividade planejado em um cronograma de produção global, e programar as atividades de manutenção para minimizar o impacto negativo sobre os processos de negócios.

### Prática de Gestão

### Entradas

### Saídas

Prática de Gestão	Entradas	Descrição	Descrição	Para
<b>BAI09.03 Gerenciar o ciclo de vida do ativo.</b> Gerenciar ativos da compra ao descarte para assegurar que os ativos são utilizados de forma tão eficaz e eficiente quanto possível e são contabilizados e fisicamente protegidos.	De		<ul style="list-style-type: none"> <li>• Solicitações aquisição de ativos autorizadas</li> <li>• Revisões do registro de ativos</li> <li>• Desativação de ativos autorizados</li> </ul>	Interno BAI10.03 BAI10.03
<b>Atividades</b>				

- 01 Adquirir todos os ativos com base nas solicitações aprovadas e em conformidade com as políticas e práticas de aquisição da empresa.
- 02 Fonte, receber, verificar, testar e gravar todos os ativos de uma maneira controlada, incluindo a rotulagem física, conforme necessário.
- 03 Aprovar pagamentos e concluir o processo com os fornecedores de acordo com as condições contratuais acordadas.
- 04 Implantar ativos seguindo o ciclo de vida de implementação padrão, incluindo gerenciamento de mudanças e testes de aceitação.
- 05 Alocar recursos para os usuários com a aceitação de responsabilidades e assinaturas, conforme o caso.
- 06 Realocar os ativos, sempre que possível, quando eles não são mais necessários devido a uma mudança de função de usuário, a redundância dentro de um serviço ou desativação de um serviço.
- 07 Descartar ativos quando eles não servem a nenhum propósito útil devido à desativação dos serviços relacionados, tecnologias obsoletas ou a falta de usuários.
- 08 Descartar ativos de forma segura considerando, por exemplo, a exclusão permanente de quaisquer dados registrados em dispositivos de mídia e potencial de danos ao meio ambiente.
- 09 Planejar, autorizar e implementar atividades relacionadas com a desativação, mantendo registros apropriados para atender a necessidades de regulamentação e negócios em andamento.

### Prática de Gestão

### Entradas

### Saídas

Prática de Gestão	Entradas	Descrição	Descrição	Para
<b>BAI09.04 Otimizar os custos dos ativos.</b> Analisa periodicamente a base de ativos em geral para identificar maneiras de otimizar os custos e manter o alinhamento com as necessidades do negócio.	De		<ul style="list-style-type: none"> <li>• Resultados de revisões de otimização de custos</li> <li>• Oportunidades para reduzir custos de ativos ou aumentar o valor</li> </ul>	APO02.02 APO02.02

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## BAI09 Práticas de Processo, Entradas/Saídas e Atividades

Atividades
01 Em uma base regular, revisar a base de ativos no geral, considerando se ela está alinhado com os requisitos de negócio.
02 Avaliar os custos de manutenção, considerar racionalidade e identificar opções de menor custo incluindo, se necessário, substituição por novas alternativas.
03 Revisar garantias e considerar o valor monetário e estratégias de substituição para determinar as opções de menor custo.
04 Revisar a base em geral para identificar oportunidades de padronização, fornecimento individual e outras estratégias que podem reduzir os custos de aquisição, suporte e manutenção.
05 Utilizar as estatísticas capacidade e utilização para identificar ativos subutilizados ou redundantes que poderiam ser considerados para a eliminação ou substituição para reduzir os custos.
06 Analisar o estado geral para identificar oportunidades para alavancar as tecnologias emergentes ou estratégias de fornecimento alternativo para reduzir custos ou aumentar o valor para o negócio.

## Prática de Gestão

## BAI09.05 Gerenciar licenças.

Gerenciar licenças de software de modo que o número ideal de licenças é mantido para suportar os requisitos de negócios e o número de licenças possuídas é suficiente para cobrir o software instalado em uso.

## Entradas

## De

## Descrição

## Descrição

## Para

- Registo das licenças de software BAI10.02
- Os resultados das auditorias licenças instaladas MEA03.03
- Plano de acção para ajustar os números de licenças e alocações APO02.05

## Atividades

01 Manter um registo de todas as licenças de software adquiridas e acordos de licença associados.
02 Em uma base regular, realizar uma auditoria para identificar todas as instâncias dos softwares licenciados instalados.
03 Comparar o número de instâncias de software instalados com o número de licenças possuídas.
04 Quando as instâncias são mais baixos do que o número possuídas, decidir se há necessidade de manter ou cessar o uso de licenças, considerando o potencial de economizar com manutenção desnecessária, treinamento e outros custos.
05 Quando as instâncias são mais elevados do que o número possuídas, considerar em primeiro lugar a oportunidade de desinstalar instâncias que não são mais necessários ou justificado, quando e se necessário, adquirir licenças adicionais para cumprir com o contrato de licenciamento.
06 Em uma base regular, considerar se melhor valor pode ser obtido pela atualização de produtos e licenças associadas.

## BAI09 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ITIL V3 2011	Transição de Serviço 4.3 Gerenciamento de Ativos de Serviço e Configuração

# COBIT® 5 : HABILITANDO PROCESSOS

BAI10 Gerenciar Configuração	Área: Gestão Domínio: Construir, Adquirir e Implementar
<b>Descrição do Processo</b> <p>Definir e manter as descrições e relações entre recursos chave e capacidades necessárias para entregar e habilitar serviços de TI, incluindo a coleta de informações de configuração, o estabelecimento de linhas de base, verificação e informações de configuração de auditoria, e atualizar o repositório de configuração.</p>	
<b>Declaração de Propósito do Processo</b> <p>Fornecer informações suficientes sobre os ativos de serviços para permitir o serviço seja efetivamente gerenciado, avaliar o impacto das mudanças e lidar com incidentes de serviço.</p>	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo das não conformidade de TI, incluindo acordos e multas e o impacto da perda de reputação</li> <li>Número de questões de não conformidade relacionadas a TI comunicadas à direção que causaram comentário público ou constrangimento</li> <li>Número de não cumprimento de questões relativas aos acordos contratuais com prestadores de serviços de TI</li> <li>Abrangência das avaliações de conformidade</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência da maturidade da capacidade e de custo de avaliações de otimização</li> <li>Tendência dos resultados das avaliações</li> <li>Níveis de satisfação dos executivos de negócios e de TI com os custos e capacidades relacionados a TI</li> </ul>
14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	<ul style="list-style-type: none"> <li>Nível de satisfação dos usuários de negócios com qualidade e pontualidade (ou disponibilidade) das informações gerenciais</li> <li>Número de incidentes de processos de negócios causadas por falta de disponibilidade de informações</li> <li>Relação e extensão das decisões de negócios errôneas onde a informação errada ou não disponível era um fator chave</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Re却tório de configuração é preciso, completo e atualizado.	<ul style="list-style-type: none"> <li>Número de desvios entre o re却tório de configuração e configuração atual</li> <li>Número de discrepâncias relativas a informações de configuração incompletas ou em falta</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

BAI10 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Controle da Qualidade dos Negócios	Oficial de Privacidade
<b>BAI10.01</b> Estabelecer e manter um modelo de configuração.				C												C C C I A R R										
<b>BAI 10.02</b> Estabelecer e manter um repositório de configuração e linha de base																	C R A R R									
<b>BAI10.03</b> Manter e controlar os itens de configuração.																	A C R R R C									
<b>BAI10.04</b> Produzir relatórios de status e configuração.				I												I I C C A R I										
<b>BAI10.05</b> Verificar e avaliar a integridade do repositório de configuração.				I												R R R A R										

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

BAI10 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI10.01 Estabelecer e manter um modelo de configuração.</b> Estabelecer e manter um modelo lógico dos serviços, bens e infraestrutura e como gravar itens de configuração (ICs) e as relações entre eles. Inclua os ICs considerados necessários para gerenciar os serviços de forma eficaz e para fornecer uma descrição confiável simples de um serviço.	BAI07.06	• Plano de liberação	• Escopo do modelo de gestão de configuração • Modelo de configuração lógico	Interno
<b>Atividades</b>				
01 Definir e chegar a acordo sobre o escopo e o nível de detalhe para o gerenciamento de configuração (isto é, quais os serviços, ativos e infraestrutura itens configuráveis para incluir).				
02 Estabelecer e manter um modelo lógico para a gestão de configuração incluindo informações sobre os tipos de itens de configuração, os atributos dos itens de configuração, tipos de relacionamento, atributos do relacionamento e códigos de status.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI 10.02 Estabelecer e manter um repositório de configuração e linha de base.</b> Estabelecer e manter um repositório do gerenciamento de configuração e criar linhas de base de configuração controladas.	BAI09.05	• Registo de licenças de software	• Repositório de configuração • Linha de base de configuração	BAI09.01 DSS02.01 BAI03.11

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## BAI10 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>BAI10.03 Manter e controlar os itens de configuração.</b> Manter um repositório atualizado dos itens de configuração povoado com as mudanças.	BAI06.03	<ul style="list-style-type: none"> <li>Relatórios de status de Solicitação de Mudança</li> </ul>	<ul style="list-style-type: none"> <li>Repositório de atualização com itens de configuração</li> </ul>	DSS02.01
	BAI09.01	<ul style="list-style-type: none"> <li>Resultados dos controles de inventário físico</li> <li>Registro de ativos</li> </ul>	<ul style="list-style-type: none"> <li>Mudanças aprovadas para a linha de base</li> </ul>	BAI03.11
	BAI09.03	<ul style="list-style-type: none"> <li>Desativação de ativos autorizados</li> <li>Revisões do registro de ativos</li> </ul>		
Atividades				
01 Identificar e classificar itens de configuração e popular o repositório.				
02 Criar, revisar e acordar formalmente sobre linhas de base de configuração de um serviço, aplicação ou infraestrutura.				
<b>BAI10.04 Produzir relatórios de status e configuração.</b> Definir e produzir relatórios de configuração em alterações do estado dos itens de configuração.	Prática de Gestão	Entradas		Saídas
		De	Descrição	Para
	BAI09.01	<ul style="list-style-type: none"> <li>Resultados dos controles de inventários físicos</li> </ul>	<ul style="list-style-type: none"> <li>Relatórios de status de configuração</li> </ul>	BAI03.11 DSS02.01
Atividades				
01 Identificar as alterações de status nos itens de configuração e relatar contra a linha de base.				
02 Combinar todas as alterações de configuração com requisições de mudança aprovadas para identificar quaisquer alterações não autorizadas. Relatar alterações não autorizadas à gestão da mudança.				
03 Identificar os requisitos de apresentação de relatórios de todas as partes interessadas, incluindo conteúdo, frequência e mídia. Produzir relatórios de acordo com as necessidades identificadas.				
Prática de Gestão				
<b>BAI10.05 Verificar e avaliar a integridade do repositório de configuração.</b> Revisar periodicamente o repositório de configuração e verificar a integralidade e exatidão contra a meta desejada.	Prática de Gestão	Entradas		Saídas
		De	Descrição	Para
			<ul style="list-style-type: none"> <li>Resultados da verificação física dos itens de configuração</li> <li>Desvios de licença</li> <li>Resultado das revisões de integridade do repositório</li> </ul>	<p>Interno</p> <p>MEA03.03</p> <p>Interno</p>
Atividades				
01 Verifica periodicamente itens de configuração atuais contra o repositório de configuração, comparando configurações físicas e lógicas e usando ferramentas de descoberta apropriadas conforme a necessidade.				
02 Reportar e rever todos os desvios para correções ou ações aprovadas para remover quaisquer ativos não autorizados.				
03 Verificar periodicamente se todos os itens de configuração físicos com definidos no repositório, existem fisicamente. Relatar quaisquer desvios para a gestão.				
04 Ajustar e revisar periodicamente a meta de integridade do repositório de configuração com base na necessidade do negócio.				
05 Comparar periodicamente o grau de integridade e precisão contra as metas e tomar medidas corretivas, se necessário, para melhorar a qualidade dos dados do repositório.				

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	9.1 Gestão de Configuração
ITIL V3 2011	Transição de Serviço 4.3 Gerenciamento de Ativos de Serviço e Configuração

CAPÍTULO 5  
CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## ENTREGAR, SERVIÇO E SUPORTE (DSS)

- 01 Gerenciar Operações.**
- 02 Gerenciar Solicitações e Incidentes de Serviços.**
- 03 Gerenciar Problemas.**
- 04 Gerenciar Continuidade.**
- 05 Gerenciar Serviços de Segurança.**
- 06 Gerenciar Controles de Processos de Negócio.**

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

DSS01 Gerenciar Operações		Área: Gestão Domínio: Entregar, Serviço e Suporte
<b>Descrição do Processo</b> Coordenar e executar as atividades e procedimentos operacionais necessários para entregar serviços de TI internos e terceirizados, incluindo a execução de procedimentos operacionais padrão pré-definidos e as atividades de monitoração necessárias.		
<b>Declaração de Propósito do Processo</b> Entregar resultados operacionais de serviços de TI conforme planejado.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
<b>Objetivos de TI</b>		<b>Métricas Relacionadas</b>
04 Gestão de risco organizacional de TI		Percentual de processos críticos de negócio, serviços de TI e programas de negócio relacionados à TI cobertos pela avaliação de riscos. Número significativo de incidentes relacionados à TI que não foram na avaliação de riscos. Percentual de avaliações de riscos corporativos incluindo riscos relacionados à TI Frequência de atualização do perfil de risco.
07 Prestação de serviços de TI em consonância com os requisitos de negócio		Número de interrupções de negócio devido a incidentes nos serviços de TI Percentual de partes interessadas do negócio satisfeitas com a entrega de serviços de TI, de acordo com os níveis de serviço acordados. Percentual de usuários satisfeitos com a qualidade da entrega de serviços de TI
11 Otimização de ativos, recursos e capacidades de TI		Frequência de avaliação da maturidade da capacidade e otimização de custos Tendências dos resultados das avaliações Nível de satisfação dos executivos do negócio e de TI com os custos e capacidades relacionados à TI.
<b>Objetivos e Métricas do Processo</b>		
<b>Objetivo do Processo</b>		<b>Métricas Relacionadas</b>
01 Atividades operacionais são executadas conforme requisitadas e agendadas.		Número de procedimentos operacionais não padrão executadas. Número de incidentes causados por problemas operacionais.
02 Operações são monitoradas, medidas, reportadas e remediadas.		Proporção de eventos comparados com o número de incidentes. Percentual dos tipos de eventos operacionais críticos cobertos por sistemas de detecção automática

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

DSS01 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>DSS01.01</b> Executar procedimentos operacionais.																			<b>A</b>	<b>C</b>	<b>C</b>	<b>C</b>				
<b>DSS01.02</b> Gerenciar serviços terceirizados.										<b>I</b>							<b>A</b>		<b>R</b>							
<b>DSS01.03</b> Monitorar a infraestrutura de TI.				<b>I</b>	<b>C</b>					<b>I</b>						<b>C</b>	<b>I</b>	<b>C</b>	<b>A</b>	<b>C</b>	<b>C</b>					
<b>DSS01.04</b> Gerenciar o ambiente.						<b>I</b>				<b>C</b>	<b>A</b>				<b>C</b>	<b>C</b>	<b>C</b>	<b>I</b>	<b>C</b>	<b>R</b>	<b>I</b>	<b>R</b>	<b>I</b>			
<b>DSS01.05</b> Gerenciar as instalações.						<b>I</b>			<b>C</b>	<b>A</b>				<b>C</b>	<b>C</b>	<b>C</b>	<b>I</b>	<b>C</b>	<b>R</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>			

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

DSS01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS01.01 Executar procedimentos operacionais.</b> Manter e executar procedimentos e tarefas operacionais com confiabilidade e consistência.	BAI05.05	<ul style="list-style-type: none"> <li>• Plano de operação e uso</li> </ul>	<ul style="list-style-type: none"> <li>• Agenda operacional</li> <li>• Registro de Backup</li> </ul>	Interna Interna
<b>Atividades</b>				
01 Desenvolver e manter procedimentos operacionais e atividades relacionadas para suporte a todos os serviços entregues.				
02 Manter um cronograma de atividades operacionais, executar as atividades, e gerenciar o performance e rendimento das atividades programadas.				
03 Verificar se todos os dados esperados para processamento são recebidos e processados completamente, com precisão e em tempo hábil. Entregar saídas de acordo com as exigências da empresa. Apoio reativação e necessidades de reprocessamento. Certificar de que os usuários recebam as saídas corretas de maneira segura e em tempo hábil.				
04 Assegurar que as normas de segurança aplicáveis são satisfeitas para o recebimento, processamento, armazenamento e saída de dados de uma forma que atenda aos objetivos corporativos, a política de segurança da empresa e os requisitos regulamentares.				
05 Agendar, executar e registrar backups de acordo com as políticas e procedimentos estabelecidos.				
Prática de Gestão	Entradas		Saídas	
<b>DSS01.02 Gerenciar serviços de TI terceirizados.</b> Gerenciar a operação dos serviços terceirizados de TI para manter a proteção das informações e confiabilidade da prestação de serviços.	De	Descrição	Descrição	Para
	APO09.03	<ul style="list-style-type: none"> <li>• Acordos de nível operacional (OLAs)</li> <li>• Acordos de nível de serviço (SLAs)</li> </ul>	<ul style="list-style-type: none"> <li>• Planos de garantias independentes</li> </ul>	MEA02.06
	BAI05.05	<ul style="list-style-type: none"> <li>• Plano de operação e uso</li> </ul>		

# COBIT® : HABILITANDO PROCESSOS

DSS01 Práticas de Processo, Entradas/Saídas e Atividades							
Atividades							
01 Assegurar que os requisitos corporativos para a segurança dos processos de informação são aderentes e em conformidade com os contratos e Acordos de nível de serviço (SLAs) com terceiros para hospedagem ou prestação de serviços.							
02 Assegurar que as operações de negócio da empresa, os requisitos de processamentos de TI e prioridades para entrega dos serviços são aderentes e em conformidade com contratos e Acordos de nível de serviço (SLAs) com terceiros para hospedagem ou prestação de serviços.							
03 Integrar processos internos e críticos de gerenciamento de TI com os de prestadores de serviços terceirizados, que abrange, por exemplo, planejamento de desempenho e capacidade, gerenciamento de mudanças, gerenciamento de configuração, solicitação de serviço e gerenciamento de incidentes, gerenciamento de problemas, gerenciamento de segurança, continuidade de negócios, e o monitoramento do desempenho dos processos e relatórios.							
04 Planejar para a auditoria independente e assegurar ambientes operacionais de provedores terceirizados para confirmar que os requisitos acordados sejam devidamente tratados.							
Prática de Gestão		Entradas		Saídas			
<b>DSS01.03 Monitorar a infraestrutura de TI.</b> Monitorar a infraestrutura de TI e eventos relacionados. Armazenar informações cronológicas suficientes sobre registros de operações para permitir a reconstrução, revisão e análise das sequências de operações no tempo e outras atividades circundantes ou operações de apoio.	BAI03.11	• Definições de Serviços	• Regras de monitoração de ativos e condições de eventos • Registros de Eventos • Registro de Incidentes	Descrição Para			
				DSS02.01 DSS02.02			
				Interna			
				DSS02.02			
Atividades							
01 Registros de eventos, identificando o nível de informação a ser gravado com base na ponderação de risco e desempenho.							
02 Identificar e manter uma lista de ativos de infraestrutura que precisam ser monitorados, com base na criticidade do serviço e a relação entre os itens de configuração e os serviços que deles dependem.							
03 Definir e implementar regras que identifica e registra eventos de violações de limites e condições. Encontrar um equilíbrio entre a geração de eventos menores espúrios e eventos significativos de modo que os registros de eventos não sejam sobrecarregados com informações desnecessárias.							
04 Produzir registros de eventos e retê-los por um período adequado para auxiliar em futuras investigações.							
05 Estabelecer procedimentos para monitorar os registros de eventos e realizar revisões regulares.							
06 Assegurar que os registros de incidentes sejam criados em tempo hábil quando o monitoramento identificar desvios nos limites definidos.							
Prática de Gestão		Entradas		Saídas			
<b>DSS01.04 Gerenciar o ambiente.</b> Manter as medidas de proteção contra fatores ambientais. Instalar equipamentos e dispositivos especializados para monitorar e controlar o ambiente.	De	Descrição	Descrição	Para			
				APO01.08 APO01.08			
Atividades							
01 Identificar as catástrofes naturais e provocadas pelo homem que podem ocorrer na área dentro da qual as instalações de TI estão localizadas. Avaliar o efeito potencial dessas catástrofes sobre as instalações de TI.							
02 Identificar como os equipamentos de TI, incluindo equipamentos móveis e remotos, são protegidos contra ameaças ambientais. Certificar que a política limita ou proíbe comer, beber e fumar em áreas sensíveis, e proíbe o armazenamento de artigos de papelaria e outros suprimentos que representam um risco de incêndio dentro de salas de informática.							
03 Situar e construir TI facilidades para minimizar e mitigar a suscetibilidade a ameaças ambientais.							
04 Monitorar regularmente e manter os dispositivos que detectam proativamente ameaças ambientais (por exemplo, fogo, água, fumaça, umidade).							
05 Responder a alarmes ambientais e outras notificações. Documentar e testar procedimentos, que devem incluir priorização de alarmes e contato com as autoridades de resposta a emergências locais e treinar pessoal nestes procedimentos.							
06 Comparar medidas e planos de contingência com as exigências da política de seguros e relatar os resultados. Tratar os pontos em não conformidade tempo hábil.							
07 Assegurar que os ambientes de TI são construídos e projetados para minimizar o impacto do risco ambiental (por exemplo, roubo, ar, fogo, fumaça, água, vibração, terror, vandalismo, produtos químicos, explosivos). Considerar zonas específicas de segurança e / ou células à prova de fogo (por exemplo, localização de ambientes de produção e desenvolvimento / servidores longe um do							

outro).

- 08 Manter os locais de TI e salas de servidores limpo e em condições de segurança em todos os momentos (por exemplo, sem bagunça, sem caixas de papel ou cartão, que não haja caixotes de lixo cheios, que o ambiente esteja sem produtos químicos ou materiais inflamáveis).

172

Personal Copy of: Sr. Felipe Soares de Oliveira

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

#### DSS01 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS01.05 Gerenciar instalações.</b> Gerenciar instalações, incluindo equipamentos de energia e de comunicação, de acordo com as leis e reguladores, requisitos técnicos e de negócio, especificações do fornecedor e com as diretrizes de saúde e segurança.			<ul style="list-style-type: none"><li>Reportes de Avaliação das instalações</li><li>Conscientização sobre Saúde e Segurança</li></ul>	MEA01.03 MEA01.03 Interna
<b>Atividades</b>				
01 Examinar os requisitos das instalações de TI para a proteção contra oscilações de energia e interrupções, em conjunto com outros requisitos de planejamento de continuidade de negócios. Providenciar equipamento adequado para fornecimento ininterrupto de energia (por exemplo, baterias, geradores) para apoiar o planejamento de continuidade de negócios.				
02 Testar regularmente os mecanismos da fonte de alimentação ininterrupta de energia e assegurar que a energia pode ser transferida para o fornecimento de contingência sem qualquer efeito significativo nas operações de negócios.				
03 Certificar que as instalações que contenham os sistemas de TI têm mais de uma fonte para as instalações dependentes (por exemplo, energia, telecomunicações, água, gás). Separar a entrada física de cada utilidade.				
04 Verificar se o cabeamento externo para o site de TI está localizado no subsolo ou tem proteção alternativa adequada. Determinar que o cabeamento dentro do site de TI seja contido dentro de conduites seguros e que os armários de fiação sejam de acesso restrito ao pessoal autorizado. Proteger corretamente o cabeamento contra danos causados por fogo, fumaça, água, interceptação e interferência.				
05 Assegurar que o cabeamento físico e as conexões (dados e telefone) são estruturados e organizados. Estruturas de cabeamento e conduites devem ser documentadas (por exemplo, plano de 'blueprint' e diagramas de fiação).				
06 Analisar os sistemas de alta disponibilidade das instalações para redundância e requisitos de proteção contra falhas para o cabeamento (externo e interno).				
07 Assegurar que os ambientes de TI e suas instalações estejam em continua conformidade com as leis de saúde e segurança aplicáveis, e de acordo com os regulamentos, diretrizes e especificações dos fornecedores.				
08 Educar o pessoal regularmente a respeito das leis de saúde e segurança, regulamentos e orientações relevantes. Educar o pessoal em simulações de incêndio e salvamento para garantir o conhecimento e tomada de ações em caso de incêndio ou de incidentes semelhantes.				
09 Registrar, monitorar, gerenciar e resolver incidentes de instalações de acordo com o processo de gerenciamento de incidentes de TI estabelecido. Deixar disponíveis os relatórios sobre os incidentes nas instalações nas situações em que a divulgação é requerida por leis e reguladores.				
10 Assegurar que as instalações de TI e seus equipamentos sejam mantidos de acordo com os intervalos de manutenção e especificações recomendadas pelos fornecedores. A manutenção deve ser realizada somente por pessoas autorizadas.				
11 Analisar as alterações físicas feitas nas instalações de TI ou dependências para reavaliar o risco do ambiente (por exemplo, incêndio ou danos causados pela água). Relatar os resultados desta análise para a gestão de continuidade dos negócios e gerenciamento das instalações.				

#### DSS01 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ITIL V3 2011	Operação de Serviços, 4.1 Gerenciamento de Eventos

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

DSS02 Gerenciar Solicitações e Incidentes de Serviços	Área: Gestão Domínio: Entregar, Serviço e Suporte
<b>Descrição do Processo</b>	
Fornecer resposta rápida e eficaz às solicitações dos usuários e resolver todos os tipos de incidentes. Restaurar o serviço normal; registrar e atender a solicitações de usuários; e registrar, investigar, diagnosticar, escalar e resolver incidentes.	
<b>Declaração de Propósito do Processo</b>	
Alcançar maior produtividade e minimizar as interrupções através de rápida resolução de consultas dos usuários e incidentes.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Porcentual de processos críticos de negócio, serviços de TI e programas de negócio habilitados por TI que são abrangidos pela avaliação de risco</li> <li>Número de incidentes significativos relacionados com TI que não foram identificados na avaliação de risco</li> <li>Porcentual de avaliações de risco, incluindo riscos relacionados com TI</li> <li>Frequência de atualização do perfil de riscos</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de interrupções nos negócios devido a incidentes em serviços de TI</li> <li>Porcentual de partes interessadas do negócio satisfeitas pela entrega de serviços de TI de acordo com os níveis de serviços acordados</li> <li>Porcentual de usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Os serviços relacionados com TI estão disponíveis para uso.	<ul style="list-style-type: none"> <li>Número e percentual de incidentes que causam interrupção de processos críticos de negócios</li> <li>Tempo médio entre incidentes de acordo com serviços de TI habilitados</li> </ul>
02 Os incidentes são resolvidos de acordo com os níveis de serviço acordados.	<ul style="list-style-type: none"> <li>Porcentual de incidentes resolvidos dentro do período de tempo acordado / aceitável.</li> </ul>
03 As solicitações de serviço são tratadas de acordo com os níveis de serviço acordados e visando a satisfação dos usuários.	<ul style="list-style-type: none"> <li>Nível de satisfação dos usuários com relação ao pedidos serviço atendidos.</li> <li>A média de tempo para lidar com cada tipo de solicitação de serviço</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

DSS02 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>DSS02.01</b> Definir esquemas de classificação de registros de incidentes e de serviços.				C					I	I							A	C	R	R		R	C	C	C	
<b>DSS02.02</b> Registrar, classificar e priorizar as solicitações e incidentes.					I				I	I											A	R			I	
<b>DSS02.03</b> Verificar, aprovar e atender as solicitações de serviços.					R												I	R	R	A						
<b>DSS02.04</b> Investigar, diagnosticar e atribuir incidentes.					R				I	I						I	I	I	C	R	A	C				
<b>DSS02.05</b> Resolver e recuperar operações após incidentes.					I				I	I						C	C	I	R	R	A	R		C		
<b>DSS02.06</b> Fechar requisições de serviços e incidentes.					I				I	I						I	I	I	I	A	I	R	I		I	
<b>DSS02.07</b> Rastrear situações e gerar reportes.					I				I	I						I	I	I	I	A	R	I				

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

DSS02 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
<b>DSS02.01 Definir esquemas de classificação de Incidentes e solicitações de serviços.</b> Definir esquemas e modelos para classificação de incidente e solicitações de serviços.	De APO09.03 APO09.03	Descrição • Acordos de nível de serviço (SLAs)	Descrição • Esquemas e modelos de classificação de requisições de serviços e incidentes	Para Internacional
	BAI10.02 BAI10.02	• Reppositório de Configuração	• Regras para escalonamento de incidentes	Internacional
	BAI10.03 BAI10.03	• Repositório atualizado com itens de configuração	• Critérios para registro de problemas	
	BAI10.04 BAI10.04	• Reportes de situação da configuração		
	DSS01.03 DSS01.03	• Regras de monitoramento de ativos e condições de eventos		
	DSS03.01 DSS03.01	• Esquema de classificação de problemas		
	DSS04.03	• Ações de resposta e		

Personal Copy of: Sr. Felipe Soares de Oliveira

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## DSS02 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
Prática de Gestão	Entradas	Saídas		
<b>DSS02.02 Registrar, classificar e priorizar as solicitações e incidentes.</b> Identificar, registrar e classificar as solicitações de serviço e incidentes, e atribuir uma prioridade de acordo com a criticidade de negócios e acordos de serviço.	APO09.03 APO09.03 BAI04.05 BAI04.05 DSS01.03 DSS01.03 DSS05.07 DSS05.07	<ul style="list-style-type: none"> <li>• Acordos de nível de serviço (SLAs)</li> <li>• Procedimento de escalonamento de emergências</li> <li>• Registros de incidentes</li> <li>• Regras de monitoramento de ativos e condições de eventos</li> <li>• Registros de incidentes de segurança</li> </ul>	<ul style="list-style-type: none"> <li>• Registros de incidentes e solicitação de serviços</li> <li>• Incidentes e Solicitações de Serviços classificadas e priorizadas</li> </ul>	Interna APO08.03 APO09.04 APO13.03
Atividades				
01 Registrar todas as solicitações de serviço e incidentes, gravando todas as informações relevantes para que possam ser tratadas de forma eficaz e que um registro histórico completo possa ser mantido.				
02 Para ativar a análise de tendências, classificar as solicitações de serviço e incidentes, identificando o tipo e categoria.				
03 Priorizar solicitações de serviço e incidentes com base na definição de impacto aos negócios e urgência do serviço descrita no Acordos de Níveis de Serviço (SLA).				
Prática de Gestão	Entradas	Saídas		
<b>DSS02.03 Verificar, aprovar e atender às solicitações de serviços.</b> Selecionar os procedimentos de solicitação adequados e verificar se as solicitações de serviço atendem os critérios definidos. Obter a aprovação, se necessário, e preencher os pedidos.	De APO12.06	Descrição <ul style="list-style-type: none"> <li>• Causa raiz dos riscos relacionados</li> </ul>	Descrição <ul style="list-style-type: none"> <li>• Solicitações de serviços aprovadas</li> <li>• Solicitações de serviços atendidas</li> </ul>	Para BAI06.01 Interna
Atividades				
01 Verificar o direito de emitir solicitações de serviço utilizando, sempre que possível, um fluxo de processo pré-definido e mudanças padrão.				
02 Obter a aprovação financeira e funcional ou autorização, se necessário, ou aprovações pré-definidas para mudanças padrão previamente acordadas.				
03 Cumprir as solicitações executando o procedimento de pedido selecionado, utilizando, sempre que possível, menus de autoajuda automatizados e modelos de solicitação pré-definidos para itens mais frequentemente solicitados				
Prática de Gestão	Entradas	Saídas		
<b>DSS02.04 Investigar, diagnosticar e atribuir incidentes.</b> Identificar e registrar os sintomas de incidentes, determinar as possíveis causas e atribuir para resolução.	De BAI07.07	Descrição <ul style="list-style-type: none"> <li>• Plano suplementar de suporte</li> </ul>	Descrição <ul style="list-style-type: none"> <li>• Sintomas de incidents</li> <li>• Registro de problema</li> </ul>	Para Interna
Atividades				
01 Identificar e descrever sintomas relevantes para estabelecer as causas mais prováveis dos incidentes. Referenciar fontes de conhecimento disponíveis (incluindo erros e problemas conhecidos) para identificar possíveis resoluções de incidentes (soluções temporárias e / ou soluções permanentes).				
02 Se um problema relacionado ou erro conhecido ainda não existir e se o incidente satisfaz critérios de registo de problema previamente acordados, registrar um novo problema.				
03 Atribuir incidentes a funções especializadas se uma experiência mais profunda for necessária, e envolver o nível de gerenciamento apropriado, onde e se necessário.				
Prática de Gestão	Entradas	Saídas		
<b>DSS02.05 Resolver e recuperar incidentes.</b> Documentar, aplicar e testar as soluções definitivas ou alternativas identificadas e executar ações para restaurar o serviço relacionados à TI.	De APO12.06 DSS03.03 DSS03.04	Descrição <ul style="list-style-type: none"> <li>• Planos de Resposta a Riscos relacionados a incidentes</li> <li>• Registro de erros conhecidos</li> <li>• Comunicação de</li> </ul>	Descrição <ul style="list-style-type: none"> <li>• Resoluções de incidents</li> </ul>	Para DSS03.04

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## DSS02 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
DSS02.06 Fechar solicitações de serviço e incidentes. Verificar se a resolução de incidente e / ou solicitação foi satisfatória e fechar o pedido.	DSS03.04	<ul style="list-style-type: none"> <li>• Registro de problemas fechados</li> </ul>	<ul style="list-style-type: none"> <li>• Solicitações de serviços e incidents fechados</li> <li>• Confirmação do usuário para atendimento ou resolução satisfatórios</li> </ul>	APO08.03 APO09.04 DSS03.04  APO08.03
Atividades				
01 Selecionar e aplicar as resoluções de incidente mais apropriadas (solução temporária e / ou solução permanente).				
02 Registrar se foram utilizadas soluções alternativas para resolução de incidentes.				
03 Executar ações de recuperação, se necessário.				
04 Documentar a resolução de incidente e avaliar se essa pode ser usada como uma fonte de conhecimento futuro.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
DSS02.07 Acompanhar o estado e produzir relatórios. Monitorar, analisar e relatar incidentes e tendências de atendimento de solicitações para fornecer informações para o processo de melhoria contínua.	APO09.03 DSS03.01 DSS03.02 DSS03.05	<p>APO09.03 DSS03.01 DSS03.02 DSS03.05</p> <p>Acordos de nível operacional (OLAs) Relatório de Status de Problemas Relatório de Resolução de Problemas Relatórios de monitoramento de resolução de problemas.</p>	<p>Relatório de estado de incidentes e tendências.</p>	APO08.03 APO09.04 APO11.04 APO12.01 MEA01.03  APO08.03 APO09.04 APO11.04 MEA01.03
Atividades				
01 Monitorar e rastrear escalonamentos de incidentes e resoluções e solicitar procedimentos para resolução ou conclusão.				
02 Identificar as partes interessadas de informação e suas necessidades de dados ou relatórios. Identificar frequência e meios de comunicação.				
03 Analisar incidentes e solicitações de serviço por categoria e tipo, para estabelecer tendências e identificar padrões de problemas recorrentes, violações de Acordos de Níveis de Serviço (SLA) ou ineficiências. Usar as informações como entrada para o planejamento de melhoria contínua.				
04 Produzir e distribuir relatórios oportunamente ou fornecer acesso controlado aos dados on-line.				

## DSS02 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	6.1 Gerenciamento do Nível de Serviço 8.2 Gerenciamento de Incidentes
ISO 27002	103 Gerenciamento de Incidente de Segurança da Informação
ITIL V3 2011	Operação de Serviços, 4.2 Gerenciamento de Incidentes Operação de Serviços, 4.3 Atendimento a Requisições

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

DSS03 Gerenciar Problemas	Área: Gestão Domínio: Entregar, Serviço e Suporte
<b>Descrição do Processo</b> Identificar e classificar os problemas e suas causas raízes e fornecer resolução oportuna para evitar incidentes recorrentes. Fornecer recomendações para melhorias.	
<b>Declaração de Propósito do Processo</b> Aumentar a disponibilidade, melhorar níveis de serviço, reduzir custos e melhorar a conveniência e satisfação do cliente pela redução do número de problemas operacionais.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Porcentagem de processos críticos de negócios, serviços de TI e serviços habilitados por TI abrangidos pela avaliação de risco</li> <li>Número de incidentes significativos relacionados com TI que não foram identificados na avaliação de risco</li> <li>Porcentagem de avaliações de risco, incluindo riscos relacionados com TI</li> <li>Frequência de atualização do perfil de risco</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de interrupções nos negócios devido a incidentes de serviço de TI</li> <li>Porcentagem de partes interessadas no negócio satisfeitas com a entrega de serviços de acordo com os níveis de serviço acordados</li> <li>Porcentagem de usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI	<ul style="list-style-type: none"> <li>Frequência de avaliações da maturidade e de otimizações de custo</li> <li>Tendência dos resultados das avaliações</li> <li>Níveis de satisfação de executivos de negócios e de TI com os custos e capacidades relacionados a TI</li> </ul>
14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	<ul style="list-style-type: none"> <li>Nível de satisfação dos usuários de negócios com a qualidade e oportunidade (ou disponibilidade) das informações para gestão</li> <li>Número de incidentes de processos de negócios causados por falta de disponibilidade de informações</li> <li>Relação e extensão de decisões empresariais errôneas onde a informação errônea ou não disponível foi um fator chave</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Problemas relacionados a TI são resolvidos de forma que não ocorram novamente.	<ul style="list-style-type: none"> <li>Diminuição do número de incidentes recorrentes causados por problemas não resolvidos</li> <li>Porcentagem de incidentes graves para os quais problemas foram registrados</li> <li>Porcentagem de soluções temporárias definidas para problemas em aberto</li> <li>Porcentagem de problemas registrados como parte da atividade de gestão proativa de problemas</li> <li>Número de problemas para os quais uma solução satisfatória que abordasse as causas que foram encontradas</li> </ul>

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

DSS03 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CFO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade	
<b>DSS03.01</b> Identificar e Classificar Problemas.				I C						I I				I I R	C R R			A C									
<b>DSS03.02</b> Investigar e Diagnosticar Problemas.										I I							C C A		R R								
<b>DSS03.03</b> Identificar Erros Conhecidos.																		A		R R							
<b>DSS03.04</b> Resolver e Encerrar Problemas.				I C					I I				C C I C C R				C C R	A									
<b>DSS03.05</b> Executar Gerenciamento Proativo de Problemas.				C																							

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

DSS03 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS03.01 Identificar e classificar problemas.</b> Definir e implementar critérios e procedimentos para relatar problemas identificados, incluindo a classificação, categorização e priorização de problemas.	APO12.06	• Causas Raiz relacionadas a Riscos	• Esquema de Classificação de Problemas	DSS02.01
	DSS02.01	• Critérios para Registro de Problemas	• Reportes de Situação de Problemas	DSS02.07
	DSS02.04	• Registro de problema	• Registro de Problema	Interna

**Atividades**

- 01 Identificar problemas através da correlação de relatórios de incidentes, logs de erros e outros recursos de identificação de problemas. Determinar níveis de prioridade e categorização para tratar de problemas em tempo hábil com base no risco do negócio e definição de serviço.
- 02 Lidar com todos os problemas, formalmente, com acesso a todos os dados pertinentes, incluindo informações do sistema de gestão da mudança e de configuração / ativos de TI e detalhes de incidentes.
- 03 Definir grupos de apoio adequados para ajudar com a identificação do problema, análise de causa raiz e determinação solução para apoiar a gestão problema. Determinar grupos de apoio com base em categorias pré-definidas, tais como hardware, rede, software, aplicativos e software de suporte.
- 04 Definir níveis de prioridade por meio de consultas ao negócio para assegurar que a identificação do problema e a causa raiz são tratados em tempo hábil de acordo com o Acordo De Nível De Serviço (SLAS) acordado. Basear os níveis de prioridade no impacto nos negócios e urgência.
- 05 Reportar o estado dos problemas identificados para a central de atendimento para que os clientes e a gestão de TI possam ser mantidos informados.
- 06 Manter um único catálogo de gerenciamento de problemas para registrar e relatar os problemas identificados e estabelecer trilhas de auditoria de processos de gerenciamento de problemas, incluindo o estado de cada problema (ou seja, aberto, reabrir, em

# COBIT® : HABILITANDO PROCESSOS

## DSS03 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS 03.02 Investigar e diagnosticar problemas.</b> Investigar e diagnosticar problemas usando especialistas no assunto para avaliar e analisar a causa raiz dos problemas.	APO12.06	<ul style="list-style-type: none"> <li>• Causas Raiz relacionadas a Riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Causas Raiz de Problemas</li> </ul>	Interna
			<ul style="list-style-type: none"> <li>• Reportes de Resolução de Problemas</li> </ul>	DSS02.07

### Atividades

- 01 Identificar problemas que podem ser erros conhecidos, comparando dados de incidentes com o banco de dados de erros conhecidos e suspeitos (por exemplo, os que forem comunicados pelos fornecedores externos) e classificar problemas como erros conhecidos.
- 02 Associar os itens de configuração afetados com o erro estabelecido / conhecido.
- 03 Produzir relatórios para comunicar o progresso na resolução de problemas e para monitorar o impacto contínuo de problemas não resolvidos. Monitorar o estado do processo de tratamento de problema em todo o seu ciclo de vida, incluindo a entrada a partir de mudança e gerenciamento de configuração.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS 03.03 Levantar erros conhecidos.</b> Assim que as causas dos problemas são identificadas, criar registros de erros conhecidos e uma solução adequada, e identificar possíveis soluções.			<ul style="list-style-type: none"> <li>• Registros de Erros Conhecidos</li> </ul>	DSS02.05
			<ul style="list-style-type: none"> <li>• Propostas de Solução para Erros Conhecidos</li> </ul>	BAI06.01

### Atividades

- 01 Assim que as causas dos problemas forem identificadas, criar registros de erros conhecidos e desenvolver uma solução alternativa adequada.
- 02 Identificar, avaliar, priorizar e processar (através de gestão de mudança) soluções para erros conhecidos com base em uma análise custo-benefício, impacto nos negócios e urgência.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS03.04 Resolver e Encerrar Problemas.</b> Identificar e iniciar soluções que endereçam a causa raiz e caso seja necessário levantando solicitações de mudança para resolver os erros através do processo de gestão de mudança estabelecido. Assegurar que o pessoal afetado esteja ciente das ações tomadas e dos planos desenvolvidos para prevenir a ocorrência de futuros incidentes.	DSS02.05	<ul style="list-style-type: none"> <li>• Resolução de Incidentes</li> </ul>	<ul style="list-style-type: none"> <li>• Encerrar registros de problemas</li> </ul>	DSS02.06
			<ul style="list-style-type: none"> <li>• Encerrar Requisições de Serviço e Incidentes</li> </ul>	<ul style="list-style-type: none"> <li>• Comunicação de Conhecimento Adquirido</li> </ul>

### Atividades

- 01 Fechar registros de problemas, quer após a confirmação da eliminação bem sucedida do erro conhecido ou após um acordo com o negócio sobre como lidar alternativamente com o problema.
- 02 Informar ao Service Desk sobre a programação de encerramento do problema, por exemplo, a programação para corrigir os erros conhecidos, a possível solução alternativa ou o fato de que o problema permanecerá até que uma mudança seja implementada, e as consequências da abordagem adotada. Mantenha os usuários afetados e os clientes informados conforme o caso conforme apropriado.
- 03 Durante todo o processo de resolução, obter reportes regulares de gestão da mudança sobre o progresso na resolução de problemas e erros.
- 04 Monitorar o impacto contínuo de problemas e erros conhecidos sobre os serviços.
- 05 Rever e confirmar o sucesso de resoluções de problemas maiores.
- 06 Certificar-se de que o conhecimento aprendido a partir da revisão seja incorporado numa reunião de revisão de serviço com o cliente de negócio.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS03.05 Executar o gerenciamento proativo de problemas.</b> Coletar e analisar dados operacionais (especialmente registros de incidentes e mudanças) para identificar			<ul style="list-style-type: none"> <li>• Reportes do Monitoramento da Resolução de Problemas</li> </ul>	DSS02.07

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

#### DSS03 Práticas de Processo, Entradas/Saídas e Atividades

Atividades	
01	Capturar informações relacionadas a problemas com mudanças e incidentes de TI e comunicá-las aos principais interessados. Esta comunicação pode assumir a forma de reportes e reuniões periódicas entre responsáveis pelos incidentes, problemas, mudanças e processos de gerenciamento de configuração para considerar problemas recentes e ações corretivas potenciais.
02	Garantir que os proprietários e gestores de processos de incidentes, problemas, mudanças e gerenciamento de configuração se encontram regularmente para discutir problemas conhecidos e futuras mudanças planejadas.
03	Para habilitar a empresa a monitorar os custos totais de problemas, capturar os esforços de mudança resultantes de atividades do processo de gerenciamento de problemas (por exemplo, correções para problemas e erros conhecidos) e relatá-los.
04	Produzir relatórios para monitorar a resolução de problemas em relação aos requisitos de negócios e Acordos de nível de serviço (SLAs). Garantir a cascata adequado de problemas, ou seja, o envolvimento de um nível superior de gestão de acordo com os critérios acordados, entrar em contato com fornecedores externos, ou referenciar ao conselho consultivo de alterações para aumentar a prioridade de um pedido urgente de mudança (RFC) para implementar uma solução alternativa temporária.
05	Para otimizar o uso dos recursos e reduzir soluções alternativas, acompanhar as tendências problemáticas.
06	Identificar e iniciar soluções sustentáveis (correções permanentes) que tratem a causa raiz, e levantar as solicitações de mudança através dos processos de gestão de mudança estabelecidos.

#### DSS03 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	8.3 Gerenciamento de Problema
ITIL V3 2011	Operação de Serviços, 4.4 Gerenciamento de Problemas

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

DSS04 Gerenciar Continuidade	Área: Gestão Domínio: Entregar, Serviço e Suporte
<b>Descrição do Processo</b> Estabelecer e manter um plano para permitir que o negócio e a TI possam responder a incidentes e interrupções, a fim de continuar a operação de processos de negócios críticos e os serviços de TI necessários, e manter a disponibilidade de informações em um nível aceitável para a empresa.	
<b>Declaração de Propósito do Processo</b> Continuar as operações críticas de negócios e manter a disponibilidade de informações em um nível aceitável para a empresa em caso de uma perturbação significativa.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Porcentagem de processos críticos de negócio, serviços de TI e programas de negócio habilitados por TI abrangidos pela avaliação de risco</li> <li>Número de Incidentes relacionados com TI significativos que não foram identificados na avaliação de risco</li> <li>Frequência de atualização do perfil de risco</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>Número de interrupções nos negócios devido a incidentes em serviços de TI</li> <li>Porcentagem de partes interessadas no negócio satisfeitas em que a entrega de serviços atende níveis de serviço acordados</li> <li>Porcentagem de usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	<ul style="list-style-type: none"> <li>Nível de satisfação dos usuários de negócios quanto à qualidade e oportunidade</li> <li>(ou disponibilidade) da informação para gestão</li> <li>Número de incidentes de processos de negócios causados por falta de disponibilidade de informações</li> <li>Relação e extensão das decisões empresariais erradas onde a informação errada ou não disponível foi um fator chave</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Informações críticas para os negócios estão disponíveis para o negócio alinhadas com os níveis mínimos exigidos de serviço.	<ul style="list-style-type: none"> <li>Porcentagem de serviços de TI que atendem aos requisitos de tempo de disponibilidade</li> <li>Porcentagem da restauração bem sucedida e oportuna a partir dos backups ou mídia alternativa</li> <li>Porcentagem de mídia de backup transferida e armazenada de forma segura</li> </ul>
02 Resiliência suficiente está implementada para os serviços críticos.	<ul style="list-style-type: none"> <li>Número de sistemas críticos ao negócio não cobertos pelo plano</li> </ul>
03 Testes de continuidade de serviços verificam a efetividade do plano.	<ul style="list-style-type: none"> <li>Número de exercícios e testes que atingem os objetivos de recuperação</li> <li>Frequência dos testes</li> </ul>
04 Um plano atualizado de continuidade reflete os requisitos atuais de negócios.	<ul style="list-style-type: none"> <li>Porcentagem de melhorias ao plano que foram efetivamente refletidas no plano</li> <li>Porcentagem de questões identificadas que foram posteriormente contempladas no plano</li> </ul>
05 Partes internas e externas foram treinadas no plano de continuidade.	<ul style="list-style-type: none"> <li>Porcentagem de partes interessadas internas e externas que tenham recebido treinamento</li> <li>Porcentagem de questões identificadas que foram posteriormente abordadas nos materiais de treinamento</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

DSS04 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>DSS04.01</b> Definir a política de continuidade de negócios, seus objetivos e escopo.				A C R						C					C C R	R C R					R C R					
<b>DSS04.02</b> Manter uma estratégia de continuidade.				A C R				I				C C R				C C R								R		
<b>DSS04.03</b> Desenvolver e implementar uma resposta de continuidade de negócio.					I R							I C C R													A	
<b>DSS04.04</b> Exercitar, testar e revisar o Plano de Continuidade de Negócio (BCP).					I R							I R R													A	
<b>DSS04.05</b> Revisar, manter e melhorar o plano de continuidade.				A I R			I					R													R	
<b>DSS04.06</b> Conduzir treinamento no plano de continuidade.					I R							R													A	
<b>DSS04.07</b> Gerenciar preparativos para backup.																										R
<b>DSS04.08</b> Conduzir revisões pós-retomada de operações.				C R			I					R C C R R													A	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

DSS04 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas	Saídas	
	De	Descrição	Para
<b>DSS04.01 Definir a política, objetivos e escopo da continuidade de negócios.</b> Definir a política de continuidade de negócios e escopo alinhados com os objetivos da empresa e das partes interessadas.	APO09.03	<ul style="list-style-type: none"> <li>• Acordos de nível de serviço (SLAs)</li> </ul>	<ul style="list-style-type: none"> <li>• Política e objetivos para a Continuidade de Negócios</li> <li>• Cenários de Incidentes Disruptivos</li> <li>• Avaliação das Capacidades e Diferenças da Continuidade</li> </ul>
			AP001.04 Internas Internas

## Atividades

- 01 Identificar os processos de negócios internos e terceirizados e as atividades de serviço que são críticas para as operações empresariais ou necessárias para se atender obrigações legais e / ou contratuais.

02 Identificar as principais partes interessadas e os papéis e responsabilidades para a definição e acordo sobre a política de continuidade e seu escopo.

03 Definir e documentar os objetivos e escopo mínimos acordados para a continuidade do negócio e incorporar a necessidade de planejamento contínuo na cultura da empresa.

04 Identificar os processos essenciais de suporte ao negócio e serviços de TI relacionados.

# COBIT<sup>®</sup> : HABILITANDO PROCESSOS

## DSS04 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas	Saídas	
<b>DSS04.02 Manter uma estratégia de continuidade.</b> Avaliar as opções de gerenciamento de continuidade de negócios e escolher uma estratégia viável e efetiva de custos que irá garantir a recuperação da empresa e a continuidade em face de um desastre ou outro incidente grave ou interrupção.	De APO12.06	Descrição	Descrição
		• Causas Raiz Relacionadas a Riscos	• Análises de Impacto de Negócio
		• Comunicações de Impacto em Riscos	• Requisitos de Continuidade Interna
<b>Atividades</b>		• Opções Estratégicas Aprovadas	APO02.05

- 01 Identificar potenciais cenários susceptíveis de dar origem a eventos que podem causar incidentes perturbadores significativos.
- 02 Realizar uma análise de impacto nos negócios para avaliar o impacto ao longo do tempo de uma interrupção de funções críticas do negócio e do efeito que uma ruptura teria sobre os negócios.
- 03 Estabelecer o tempo mínimo necessário para recuperar um processo de negócio e de suporte de TI com base em um prazo aceitável de interrupção dos negócios e falta de máximo tolerável.
- 04 Avaliar a probabilidade de ameaças que podem causar perda de continuidade de negócios e identificar medidas que irão reduzir a probabilidade e o impacto através de uma melhor prevenção e aumento da resiliência.
- 05 Analisar os requisitos de continuidade para identificar as possíveis opções estratégicas e opções técnicas.
- 06 Determinar as condições e os responsáveis pelas decisões chave que farão com que os planos de continuidade sejam acionados.
- 07 Identificar as necessidades de recursos e custos para cada opção técnica estratégica e fazer recomendações estratégicas.
- 08 Obter aprovações pelos executivos de negócios para as opções estratégicas selecionadas.

Prática de Gestão	Entradas	Saídas	
<b>DSS04.03 Desenvolver e implementar uma resposta a continuidade de negócio.</b> Desenvolver um Plano de Continuidade de Negócio (BCP) baseado na estratégia que documenta os procedimentos e informações prontas para uso em um incidente para capacitar a empresa a continuar suas atividades críticas.	De APO09.03	Descrição	Descrição
		• Acordos de nível operacional (OLAs)	• Ações e Comunicações de Resposta a Incidentes DSS02.01 • Plano de Continuidade de Negócio (BCP) Interna

- 01 Definir as ações de resposta a incidentes e comunicações a serem acionadas em caso de ruptura. Definir papéis e responsabilidades relacionadas, incluindo a prestação de contas pela política e implementação.
- 02 Desenvolver e manter Planos de Continuidade de Negócio (BCPs) operacionais contendo os procedimentos a serem seguidos para permitir a operação contínua dos processos críticos de negócios e / ou em regime de processamento temporário, incluindo links para planos de prestadores de serviços terceirizados.
- 03 Assegurar que os principais fornecedores e parceiros terceiros tenham planos de continuidade eficazes implementados. Obter evidências auditadas, conforme necessário.
- 04 Definir as condições e procedimentos de recuperação que permitem retomada do processamento de negócios, incluindo a atualização e a reconciliação das bases de dados de informação para preservar a integridade das informações.
- 05 Definir e documentar os recursos necessários para suportar os procedimentos de continuidade e recuperação, considerando-se as pessoas, instalações e infra-estrutura de TI.
- 06 Definir e documentar requisitos de backup de informações necessários para suportar os planos, incluindo planos e documentos em papel, bem como arquivos de dados, e considerar a necessidade de segurança e local de armazenamento externo.
- 07 Determinar habilidades necessárias para os indivíduos envolvidos na execução do plano e dos procedimentos.
- 08 Distribuir os planos e documentação de suporte de forma segura para partes interessadas devidamente autorizadas e verificar que eles são acessíveis em todos os cenários de desastres.

Prática de Gestão	Entradas	Saídas	
<b>DSS04.04 Exercício, testar e rever o Plano de Continuidade de Negócio (BCP).</b> Testar as providências de continuidade em uma base regular para exercer os planos de recuperação contra resultados predeterminados e para permitir que soluções inovadoras sejam desenvolvidas e	De	Descrição	Descrição
			• Objetivos dos testes Interna
			• Execícios de testes Interna
• Resultados dos testes e recomendações Interna			

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**DSS04 Práticas de Processo, Entradas/Saídas e Atividades**

Atividades				
01 Definir objetivos para exercitar e testar os sistemas de negócio, técnicos, logísticos, administrativos, processuais e operacionais do plano para verificar a integridade do Plano de Continuidade de Negócio (BCP) no atendimento a riscos do negócio.				
02 Definir e acordar com os interessados exercícios que são realistas, validar procedimentos de continuidade, e incluem funções e responsabilidades e acordos de retenção de dados que causam o mínimo de perturbação para os processos de negócios.				
03 Atribuir funções e responsabilidades para a realização de exercícios de plano de continuidade e testes.				
04 Agendar exercícios e atividades de testes conforme definido no plano de continuidade.				
05 Conduzir um exercício após o exercício do plano que informe e analise para considerar o objetivo.				
06 Desenvolver recomendações para melhoria do Plano de Continuidade de Negócio (BCP) Atual baseados nos resultados da reunião.				

**Prática de Gestão**

DSS04.05 Revisar, manter e melhorar o plano de continuidade.	De	Descrição	Saídas	
			Descrição	Para
			<ul style="list-style-type: none"> <li>• Resultados de Revisões do Plano</li> <li>• Alterações Recomendadas para os planos</li> </ul>	Interna  Interna

**Atividades**

01 Revisar o plano de continuidade e capacidade em uma base regular em relação a quaisquer suposições feitas e objetivos operacionais e estratégicos de negócios atual.
02 Considere se pode ser necessária uma revisão da avaliação de impacto é necessária, dependendo da natureza da mudança.
03 Recomendar e comunicar mudanças na política, planos, procedimentos, infra-estrutura e os papéis e responsabilidades para a aprovação gerencial e processamento através do processo de gestão de mudança.
04 Revisar o plano de continuidade em uma base regular para considerar o impacto das mudanças novas ou maiores para: organização, processos de negócios, acordos de outsourcing, tecnologias, infraestrutura, sistemas operacionais e sistemas de aplicação.

**Prática de Gestão**

DSS04.06 Conduzir formação para o plano de continuidade.	De	Descrição	Saídas	
			Descrição	Para
			<ul style="list-style-type: none"> <li>• Requerimentos de treinamentos</li> <li>• Monitoramento dos Resultados de Habilidades e Competências</li> </ul>	APO07.03  APO07.03

**Atividades**

01 Definir e manter os requisitos e planos de formação para aqueles que realizam o planejamento de continuidade, avaliações de impacto, as avaliações de risco, meios de comunicação e resposta a incidentes. Certificar que os planos de formação consideram a frequência os mecanismos de treinamentos.
02 Desenvolver competências com base em treinamento prático incluindo a participação em exercícios e testes.
03 Monitorar habilidades e competências com base nos resultados de exercícios e ensaios.

# COBIT® : HABILITANDO PROCESSOS

## DSS04 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS04.07 Gerenciar mecanismos de backup.</b> Manter a disponibilidade de informações críticas de negócios.			<ul style="list-style-type: none"> <li>• Resultados de testes com dados de backup</li> </ul>	Interna
<b>Atividades</b>				
01 Fazer backup de sistemas, aplicações, dados e documentação de acordo com um cronograma definido, considerando:				
<ul style="list-style-type: none"> <li>• Frequência (mensal, semanal, diária, etc.)</li> <li>• Modo de backup (por exemplo, o espelhamento de disco para backups em tempo real vs. DVD-ROM para retenção a longo prazo)</li> <li>• Tipo de backup (por exemplo, complete vs. incremental)</li> <li>• Tipo de mídia</li> <li>• Backups automatizados on-line</li> <li>• Tipos de dados (por exemplo, voz, óptico)</li> <li>• Criação de registros (logs)</li> <li>• Dados de computação críticos para o usuário final (por exemplo, planilhas)</li> <li>• Localização física e lógica das fontes de dados</li> <li>• Direitos de acesso e segurança</li> <li>• Criptografia</li> </ul>				
02 Certificar que os sistemas, aplicativos, dados e documentação mantida ou processados por terceiros são adequadamente apoiados por backups ou garantidos de outra forma. Considerar exigir retorno de backups de terceiros. Considere arranjos de custódia ou depósito.				
03 Definir os requisitos para armazenamento no local e fora dos dados de backup conforme os requisitos de negócios. Considere a acessibilidade necessária para fazer backup de dados.				
04 Implementação da sensibilização a respeito e formação para o Plano de Continuidade de Negócio (BCP).				
05 Testar periodicamente e atualizar os dados arquivados e de backup.				
Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS04.08 Conduzir revisão pós-retomada após interrupção.</b> Avaliar a adequação do BCP após a recuperação eficaz de processos e serviços de negócios no evento de uma interrupção.			<ul style="list-style-type: none"> <li>• Relatório de revisão após recuperação</li> <li>• Mudanças aprovadas para os planos</li> </ul>	Interna  BAI06.01
<b>Atividades</b>				
01 Avaliar a adesão ao Plano de Continuidade de Negócio (BCP) documentado.				
02 Determinar a eficácia do plano, recursos de continuidade, papéis e responsabilidades, habilidades e competências, a resiliência do incidente, infraestrutura técnica e estruturas organizacionais e relacionamentos.				
03 Identificar os pontos fracos ou omissões no plano e capacidades e fazer recomendações para melhoria.				
04 Obter a aprovação da gerência para quaisquer alterações ao plano e aplicar através do processo de controle de mudanças empresa.				

## DSS04 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
BS 25999:2007	Padrão de Continuidade de Negócio
ISO/IEC 20000	6.3 Gerenciamento de Continuidade de Serviços e Disponibilidade
ISO/IEC 27002:2011	104 Gerenciamento da Continuidade do Negócio
ITIL V3 2011	Desenho do Serviço, 4.6 Gerenciamento da Continuidade do Serviço de TI.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

DSS05 Gerenciar os Serviços de Segurança		Área: Gestão Domínio: Entregar, Serviço e Suporte
<b>Descrição do Processo</b>		
Proteger a informação da empresa para manter um nível aceitável de risco de segurança da informação, em linha com a política de segurança. Estabelecer e manter papéis e privilégios de acesso para segurança da informação e realizar monitoramento de segurança.		
<b>Declaração de Propósito do Processo</b>		
Minimizar o impacto de vulnerabilidades e incidentes operacionais de segurança da informação para o negócio.		<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>
Objetivos de TI	Métricas Relacionadas	
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos.	<ul style="list-style-type: none"> <li>Custo de inconformidade com TI, incluindo acordos e multas, e o impacto de perdas reputacionais.</li> <li>Número de inconformidade relacionadas a TI em relatórios emitidos ao conselho ou causando comentário públicos ou constrangimento.</li> <li>Número de pontos de inconformidades relacionados à acordos contratuais com fornecedores de serviços de TI.</li> <li>Cobertura da avaliação de conformidade.</li> </ul>	
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Programas habilitadores de TI cobertos pela avaliação de risco.</li> <li>Número de incidentes significativos relacionados a TI que não foram identificados na avaliação de risco.</li> <li>Percentual de avaliação de risco da empresa incluindo risco relacionados a TI.</li> <li>Frequência de atualização do perfil de risco.</li> </ul>	
10 Segurança da informação, infraestrutura de processamento e aplicativos	<ul style="list-style-type: none"> <li>Número de incidentes de segurança que causam perdas financeiras, interrupção dos negócios ou constrangimento público.</li> <li>Número de serviços de TI com requisitos de segurança pendentes.</li> <li>Tempo para conceder, mudar e remover acessos privilegiados, comparado ao nível de serviço acordado.</li> <li>Frequência de avaliação de segurança contra os últimos padrões e diretrizes.</li> </ul>	
<b>Objetivos e Métricas do Processo</b>		
Objetivo do Processo	Métricas Relacionadas	
01 Segurança de rede e da comunicação atende as necessidades do negócio.	<ul style="list-style-type: none"> <li>Número de vulnerabilidades descobertas.</li> <li>Número de violações ao Firewall.</li> </ul>	
02 Informações processadas, armazenadas e transmitidas por dispositivos 'endpoint' é protegida	<ul style="list-style-type: none"> <li>Percentual de indivíduos recebendo treinamento de conscientização relacionados ao uso de dispositivos 'endpoint'.</li> <li>Número de incidentes envolvendo dispositivos 'endpoint'.</li> <li>Número de dispositivos não autorizados detectados na rede ou no ambiente de usuários finais.</li> </ul>	
03 Todos usuários estão unicamente identificados e possuem diretos de acessos em conformidade com seus papéis no negócio.	<ul style="list-style-type: none"> <li>Média de tempo entre mudança e atualização das contas.</li> <li>Número de contas (contra número de usuários/funcionários autorizados).</li> </ul>	
04 Medidas físicas vem sendo implementadas para proteger a informação contra acessos não autorizados, danos e interferência quando está sendo processada, armazenada ou transmitidas.	<ul style="list-style-type: none"> <li>Percentual de testes periódicos nos dispositivos de segurança do ambiente</li> <li>Classificação média da avaliação da segurança física.</li> <li>Número de incidentes relacionados a segurança física.</li> </ul>	
05 Informação eletrônica é devidamente segura quando armazenada, transmitida e destruída.	<ul style="list-style-type: none"> <li>Número de incidentes relacionados a acesso não autorizado à informação</li> </ul>	

# COBIT® 5 : HABILITANDO PROCESSOS

DSS04 Tabela RACI

	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Conselho de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade	
<b>DSS05.01</b> Proteger contra software malicioso.		R	I								C	A			R	C	C	C	I	R	R		I	R			
<b>DSS05.02</b> Gerenciar a segurança das conexões de rede e conectividade				I		C	A							C	C	C	I	R	R			I	R				
<b>DSS05.03</b> Gerenciar a segurança dos endpoints				I		C	A							C	C	C	I	R	R			I	R				
<b>DSS05.04</b> Gerenciar identidade de usuários e acessos lógicos.				R		C	A							I	C	C	C	I	C	R		I	R	C			
<b>DSS05.05</b> Gerenciar acesso físicos aos ativos de TI				I		C	A							C	C	C	I	C	R			I	R	I			
<b>DSS05.06</b> Gerenciar documentos sensíveis e dispositivos de saída.							I							C	C	A		R									
<b>DSS05.07</b> Monitorar a infraestrutura por eventos de segurança.			I	C			I	A						C	C	C	I	C	R		I	R	I	I			

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

DSS05 Práticas de Processo, Entradas/Saídas e Atividades

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS05.01 Proteger contra malware.</b> Implementar e manter medidas preventivas, detentivas e corretivas (especialmente atualizações de patches de segurança e de antivírus) em toda a empresa para proteger os sistemas de informação e tecnologia de software malicioso (por exemplo, vírus, worms, spyware, spam).			<ul style="list-style-type: none"> <li>• Política de prevenção de software malicioso</li> <li>• Avaliação de ameaças em potencial</li> </ul>	APO01.04  APO12.02 APO12.03

## Atividades

- 01 Realizar conscientização sobre software malicioso e aplicar procedimentos para prevenção e responsabilidades.
- 02 Instalar e ativar ferramentas de proteção contra software malicioso em todas as instalações de processamento, com arquivos de definição atualizados conforme exigido (de forma automática ou semi-automática).
- 03 Distribuir todos os softwares de proteção a partir de um ponto central (versão e nível de patch) usando gerenciamento de configuração e mudanças centralizados.
- 04 Rever e avaliar novas potenciais ameaças regularmente (ex.: avaliando boletins de fabricantes e assessorias de segurança).
- 05 Filtrar e monitorar automaticamente novas ameaças e alertas de segurança fornecidas por fabricantes e assessorias de segurança.

05 Filtrar tráfego de entrada, como email e downloads, para proteção contra informações não solicitadas (ex.: spyware, e-mails de phishing)

06 Conduzir periodicamente, treinamento sobre malware em emails e uso da internet. Treinar os usuários a não instalar software compartilhado ou não aprovado.

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

Prática de Gestão	Entradas		Saídas		
	De	Descrição	Descrição	Para	
<b>DSS05.02 Gerenciar a segurança da rede e conectividade.</b> Use medidas de segurança e procedimentos de gerenciamento para proteger a informação sobre todos os métodos de conectividade	APO01.06	• Diretrizes para classificação de dados	• Política de segurança em conectividade	APO01.04	
	APO09.03	• SLAs	• Resultados de testes de invasão	MEA02.08	
<b>Atividades</b>					
01 Baseado em avaliações de risco e requisitos de negócio, estabelecer e manter uma política para segurança de conectividade.					
02 Permitir que somente dispositivos autorizados tenham acesso à informações corporativas e à rede. Configure estes dispositivos para forçar a entrada de senha					
03 Implementar mecanismos de filtragem, como firewalls e software de detecção de intrusão, com políticas apropriadas para controlar o tráfego de entrada e saída.					
04 Criptografar informações em trânsito de acordo com sua classificação.					
05 Aplicar protocolos de segurança aprovados a conectividade de rede.					
06 Configurar equipamentos de rede de maneira segura.					
07 Estabelecer mecanismos confiáveis para suportar a transmissão e recepção segura de informações					
08 Executar testes de invasão periodicamente para determinar a adequabilidade da proteção da rede					
09 Executar testes de segurança de Sistema periodicamente para determinar a adequabilidade da proteção dos sistemas					
Prática de Gestão	Entradas		Saídas		
	De	Descrição	Descrição	Para	
<b>DSS05.03 Gerenciar a segurança dos endpoints.</b> Garantir que endpoints (por exemplo, laptop, desktop, servidor e outros softwares ou dispositivos móveis e de rede) estejam protegidos a um nível igual ou maior que os requisitos de segurança definidos para as informações processadas, armazenadas ou transmitidas.	APO03.02	• Modelo de arquitetura da informação	• Políticas de segurança para dispositivos endpoint	APO01.04	
	APO09.03	• OLAs • SLAs			
	BAI09.01	• Resultados de verificações de inventário			
	DSS06.06	• Relatórios de violações			
<b>Atividades</b>					
01 Configurar sistemas operacionais de maneira segura.					
02 Implementar mecanismos de travamento.					
03 Encriptar informações armazenadas de acordo com sua classificação.					
04 Gerenciar acessos e controle remoto.					
05 Gerenciar configurações de rede de maneira segura.					
06 Implementar filtragem de tráfego de rede em dispositivos endpoint.					
07 Proteger a integridade dos sistemas.					
08 Prover proteção física aos dispositivos endpoint.					
09 Descartar dispositivos de endpoint de forma segura.					
Prática de Gestão	Entradas		Saídas		
	De	Descrição	Descrição	Para	
<b>DSS05.04 Gerenciar identidade de usuários e acesso lógico.</b> Certificar-se que todos os usuários tenham direitos de acesso a informações de acordo com suas necessidades de negócios e coordenar com as unidades de negócios que gerem os seus próprios direitos de acesso dentro de processos de negócios.	APO01.02	• Definição de papéis e responsabilidades relacionados a TI	• Direitos de usuários aprovados	Interno	
	APO03.02	• Modelo de arquitetura da informação	• Resultados de revisões de contas e privilégio de usuários	Interno	

# COBIT® : HABILITANDO PROCESSOS

## DSS05 Práticas de Processo, Entradas/Saídas e Atividades

### Atividades

- 01 Manter os direitos de acesso de usuários de acordo com os requisitos funcionais de negócio e de processo. Alinhar a gestão de identidades e direitos de acesso às funções e responsabilidades definidas, com base nos princípios de least-privilege, need-to-have e need-to-know.
- 02 Identificar unicamente toda atividade de processamento de informação por papéis funcionais, coordenando com as unidades de negócio para garantir que todos os papéis estejam consistentemente definidos, incluindo papéis pelas áreas de negócio, dentro de suas aplicações de negócio.
- 03 Autenticar todo acesso a ativos de informação baseado em sua classificação de segurança, coordenando com as unidades de negócio que gerenciam a autenticação em aplicações usadas em processos de negócio para garantir que controles de autenticação foram administrados corretamente.
- 04 Administrar todas as mudanças de direitos de acesso (criação, modificações e exclusões) para que tenham efeito no tempo apropriado baseado somente em transações documentadas e aprovadas por pessoal designado de gerenciamento.
- 05 Segregar e gerenciar contas de usuários privilegiados.
- 06 Realizar regularmente a revisão de todas as contas e privilégios relacionados.
- 07 Certificar-se que todos os usuários (internos, externos e temporários) e a sua atividade em sistemas de TI (aplicações de negócios, infraestrutura de TI, operações de sistema, desenvolvimento e manutenção) são exclusivamente identificáveis. Identificar exclusivamente todas as atividades de processamento de informações por usuário.
- 08 Manter uma trilha de auditoria de acesso à informação classificada como altamente sensível.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS05.05 Gerenciar o acesso físico aos ativos de TI.</b> Definir e implementar procedimentos de concessão, limitação e revogação do acesso às instalações, edifícios e áreas, de acordo com as necessidades do negócio, inclusive em emergências. O acesso às instalações, edifícios e áreas devem ser justificados, autorizados, registrados e monitorados. Isto deve aplicar-se a todas as pessoas que entram nas instalações, incluindo funcionários, funcionários temporários, clientes, fornecedores, visitantes ou qualquer outro terceiro.			<ul style="list-style-type: none"> <li>• Solicitações de acesso aprovadas</li> <li>• Registros de acesso</li> </ul>	<p>Interno</p> <p>DSS06.03</p>

### Atividades

- 01 Gerenciar as solicitações e concessões de acesso aos recursos de computação. Pedidos formais de acesso devem ser preenchidos, e autorizados pela gestão do site de TI, e os registros mantidos. Os formulários devem identificar especificamente as áreas em que o indivíduo é concedido acesso.
- 02 Garantir que os perfis de acesso continuem atualizados. Associe o acesso às instalações de TI (salas de servidores, edifícios, áreas ou zonas) a funções de trabalho e responsabilidades
- 03 Registrar e monitorar todos os pontos de entrada a instalações de TI. Registre todos os visitantes e fornecedores às instalações.
- 04 Instruir todos os funcionários a apresentar uma identificação visível em todos os momentos. Impedir a emissão de identificações ou crachás sem a devida autorização.
- 05 Exigir que visitantes sejam acompanhados todo o tempo, enquanto no local. Se um indivíduo desacompanhado, desconhecido ou sem identificação pessoal é identificado, alertar o pessoal de segurança.
- 06 Restringir o acesso a sites de TI sensíveis, estabelecendo restrições de perímetro, tais como cercas, paredes e dispositivos de segurança nas portas interiores e exteriores. Certifique-se de que os dispositivos registrem a entrada e disparem um alarme em caso de acesso não autorizado. Exemplos de tais dispositivos incluem crachás ou cartões-chave, teclados para senha, circuito fechado de televisão e scanners biométricos.
- 07 Conduza treinamentos de conscientização sobre segurança física regularmente

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>DSS05.06 Gerenciar documentos sensíveis e dispositivos de saída.</b> Estabelecer proteções físicas salvaguardas, práticas de contagem e gerenciamento de inventário sobre	APO03.02	<ul style="list-style-type: none"> <li>• Modelo de arquitetura da informação</li> </ul>	<ul style="list-style-type: none"> <li>• Inventário de documentos e dispositivos sensíveis</li> </ul>	<p>Interno</p>

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

#### DSS05 Práticas de Processo, Entradas/Saídas e Atividades

Atividades				
01 Estabelecer procedimentos para governar a recepção, uso, remoção e eliminação de formulários especiais e dispositivos de saída, dentro e fora da empresa.				
02 Atribuir privilégios de acesso a documentos sensíveis e dispositivos de saída com base nos princípios de least-privilege, equilibrando riscos e requisitos e de negócios.				
03 Estabelecer um inventário de documentos sensíveis e dispositivos de saída, e realizar reconciliações regulares.				
04 Estabelecer salvaguardas físicas adequadas sobre formulários especiais e dispositivos sensíveis.				
05 Destruir informações sensíveis e proteger os dispositivos de saída (por exemplo, desmagnetização da mídia eletrônica, a destruição física de dispositivos de memória, disponibilizando trituradoras ou cestos de papel com trava para destruir formulários especiais e outros documentos confidenciais).				
Prática de Gestão		Entradas		Saídas
<b>DSS05.07 Monitorar a infraestrutura por eventos relacionados à segurança.</b> Usando ferramentas de detecção de intrusão, monitorar a infraestrutura por acesso não autorizado e garantir que todos os eventos são integrados ao monitoramento geral de eventos e gerenciamento de incidentes.	De	Descrição	Descrição	Para
			• Registros de eventos de segurança	Interno
			• Características dos incidents de segurança	Interno
			• Tickets de incidents de segurança	DSS02.02
Atividades				
01 Registrar eventos de segurança relatados por ferramentas de monitoramento de segurança da infraestrutura, identificando o nível de informação a ser gravado com base na ponderação do risco. Retê-los por um período adequado para auxiliar em futuras investigações.				
02 Definir e comunicar a natureza e as características dos potenciais incidentes relacionados com a segurança para que eles possam ser facilmente reconhecidos e seus impactos entendidos, para permitir uma resposta proporcional.				
03 Rever regularmente os registros de eventos em busca de potenciais incidents.				
04 Manter um procedimento para a coleta de provas, de acordo com regras forenses locais e garantir que todos os funcionários estão cientes das exigências.				
05 Certifique-se que os tickets de incidentes de segurança são criados em tempo hábil quando o monitoramento identifica potenciais incidentes de segurança.				

#### DSS05 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 27002:2011	Código de práticas para o gerenciamento de segurança da informação
NIST SP800-53 Rev 1	Controles de Segurança Recomendados para Sistemas de Informações do Governo Federal dos EUA
ITIL V3 2011	Operação de Serviços, 4.5 Gerenciamento de Acessos

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

DSS06 Gerenciar Controles do Processo de Negócio	Área: Gestão Domínio: Entregar, Serviço e Suporte
<b>Descrição do Processo</b>	
Definir e manter controles de processo de negócios para garantir que as informações relacionadas e processadas dentro da organização ou em ambiente terceirizado satisfaçam todos os requisitos relevantes para controle das informações. Identificar requisitos relevantes de controle de informações, gerenciar e operar controles adequados para garantir que as informações e seu processamento satisfaçam estes requisitos.	
<b>Declaração de Propósito do Processo</b>	
Manter a integridade e segurança das informações e dos ativos de informação manipulados dentro na empresa ou em ambiente terceirizado referente aos processos de negócios.	
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>	
Objetivos de TI	Métricas Relacionadas
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>• Porcentagem de processos críticos de negócios, serviços de e programas de negócio habilitados por TI abrangidos pela avaliação de risco</li> <li>• Número de incidentes significativos relacionados com TI que não foram identificados na avaliação de risco</li> <li>• Porcentagem de avaliações de risco que incluem riscos relacionados com TI</li> <li>• Frequência de atualização do perfil de risco</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio	<ul style="list-style-type: none"> <li>• Número de interrupções nos negócios devido a incidentes em serviço de TI</li> <li>• Porcentagem de interessados de negócios, satisfeitos com a entrega de serviços de TI dentro dos níveis de serviço acordados</li> <li>• Porcentagem de usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
<b>Objetivos e Métricas do Processo</b>	
Objetivo do Processo	Métricas Relacionadas
01 Cobertura e eficácia de controles-chave para atingir os requisitos de negócio para o processamento de informações estão completos	<ul style="list-style-type: none"> <li>• Porcentagem de inventário completo dos processos críticos e controles-chave</li> <li>• Porcentagem de cobertura dos controles-chave dentro dos planos de teste</li> <li>• Número de incidentes e apontamentos de auditoria indicando falha dos controles-chave</li> </ul>
02 O inventário de papéis, responsabilidades e direitos de acesso está alinhado com necessidades de negócio autorizadas	<ul style="list-style-type: none"> <li>• Porcentagem de papéis de processo de negócios com direitos de acesso e níveis de autoridade atribuídos</li> <li>• Porcentagem de papéis de processos de negócios com clara separação das funções</li> <li>• Número de incidentes e apontamentos de auditoria devido a violações de acesso ou separação de direitos</li> </ul>
03 Transações de negócio são mantidas completamente e de acordo com o requerido nos logs	<ul style="list-style-type: none"> <li>• Porcentagem de completude do log de transações rastreável</li> <li>• Número de incidentes em que o histórico de transações não pode ser recuperado</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

DSS06 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>DSS06.01</b> Alinhar as atividades de controle incorporadas em processos de negócios com os objetivos empresariais.	C C C A R									I I				C C C				C C C			C C C		C C C		C	
<b>DSS06.02</b> Controlar o processamento de informações.	R R R A R									I I				C C C				C C C			C C C		C C C			
<b>DSS06.03</b> Gerenciar papéis, responsabilidades, privilégios de acesso e níveis de autoridade.		R A R								I		I	C C C				C C R			C C C		C C C		C		
<b>DSS06.04</b> Gerenciar erros e exceções.			I I A										C C I				C R			C C C		C C C				
<b>DSS06.05</b> Garantir a rastreabilidade de eventos de informação e registros.			C A							I		I	C C C				C C C			C C C		C C C				
<b>DSS06.06</b> Proteja ativos de informação	C C C A									I I				C C C				C C C			C C C		C C C			

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

## DSS06 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas	Saídas	
Prática de Gestão	De	Descrição	Para
<b>DSS06.01</b> Alinhar atividades de controle incorporadas em processos de negócios com objetivos empresariais.  Continuamente avaliar e monitorar a execução das atividades de processos de negócios e controles relacionados, com base no risco empresarial, para assegurar que os controles de processamento estão alinhados com as necessidades do negócio.	APO01.06	<ul style="list-style-type: none"> <li>• Procedimentos de integridade de dados</li> <li>• Orientações para classificação de dados</li> </ul>	<ul style="list-style-type: none"> <li>• Resultados das revisões de eficácia de processamento</li> <li>• Análise de causa raiz e recomendações</li> </ul>
<b>Atividades</b>			
01 Identificar e documentar atividades de controle em processos-chave de negócios para satisfazer exigências dos controles estratégicos, operacionais, relatórios e objetivos de conformidade 02 Priorizar atividades de controle baseado no risco inerente ao negócio e identificar controles-chave. 3.Garantir que atividades de controles-chave tenham um dono 04 Monitorar continuamente as atividades de controle em uma base fim-a-fim para identificar oportunidades de melhoria. 05 Melhorar continuamente a concepção e operação dos controles de negócios.			
Prática de Gestão	Entradas	Saídas	
<b>DSS06.02</b> Controlar o processamento de	De	Descrição	Para

**informações.**  
Operar a execução das atividades de processos de negócios e controles relacionados, com base no risco empresarial, a garantir que o processamento da informação é válida, completa, precisa, oportuna e segura (ou seja, reflete o uso do negócio legítimo e

BAI05.05	• Plano de uso e operação	• Relatórios de controle de processamento	Interno
BAI07.02	• Plano de migração		

# COBIT® : HABILITANDO PROCESSOS

## DSS06 Práticas de Processo, Entradas/Saídas e Atividades.

autorizado).

### Atividades

- 01 Criar transações por indivíduos autorizados segundo procedimentos estabelecidos, incluindo, quando apropriado, a segregação adequada de deveres em relação à origem e aprovação dessas transações.
- 02 Autenticar a origem de transações e verificar se ele/ela tem a autoridade para originar a transação.
- 03 Realizar transações em tempo hábil. Verifique se as transações são precisas, completas e válidas. Validar dados de entrada e edição ou, quando aplicável, enviar de volta para a correção o mais próximo do ponto de origem sempre que possível.
- 04 Corrija e reenvie os dados que foram erroneamente cadastrados sem comprometer os níveis de autorização da transação original. Quando necessário para a reconstrução, reter os documentos fontes originais pela quantidade adequada de tempo.
- 05 Manter a integridade e validade dos dados durante todo o ciclo de processamento. Certifique-se de que a detecção de transações errôneas não interrompe o processamento de transações válidas.
- 06 Manter a integridade dos dados durante interrupções inesperadas no processamento de negócios e confirmar a integridade dos dados após o processamento de falhas.
- 07 Tratar as saídas de forma autorizada, entregar ao destinatário apropriado e proteger as informações durante a transmissão. Verificar a exatidão e integridade da saída.
- 08 Antes de passar os dados da transação entre as aplicações internas e funções de negócio/operacionais (dentro ou fora da empresa), para verificar endereçamento adequado, a autenticidade da origem e a integridade do conteúdo. Manter a autenticidade e integridade durante a transmissão ou transporte.

### Prática de Gestão

### Entradas

### Saídas

Prática de Gestão	De	Descrição	Descrição	Para
<b>DSS06.03 Gerenciar funções, responsabilidades, privilégios de acesso e níveis de autoridade.</b> Gerenciar as funções de negócios, responsabilidades, níveis de autoridade e segregação de funções necessárias para apoiar os objetivos do processo de negócios. Autorizar o acesso a quaisquer ativos de informação relacionados com os processos de informação de negócios, incluindo aqueles sob a custódia do negócio, TI e terceiros. Isto assegura que a empresa sabe onde os dados estão e quem está a lidar com dados em seu nome.	EDM04.02	• Responsabilidades atribuídas para o gerenciamento de recursos	• Papéis e responsabilidades alocadas	APO01.02
	APO11.01	• Papéis de QMS, responsabilidades e direitos de decisão	• Níveis de autoridade alocados	APO01.02
	APO13.01	• Declaração de escopo do ISMS	• Direitos de acesso alocados	APO07.04
	DSS05.05	• Registros de acesso		

### Atividades

- 01 Atribuir funções e responsabilidades com base em descrições de trabalho aprovados e as atividades de processos de negócios alocadas.
- 02 Atribuir níveis de autoridade para aprovação de transações, os limites e quaisquer outras decisões relativas ao processo de negócio, com base em papéis de trabalho aprovados.
- 03 Atribuir direitos de acesso e privilégios com base em apenas o que é necessário para executar as atividades de trabalho, com base em papéis de trabalho pré-definidas. Remover ou revisar direitos de acesso imediatamente se o papel do trabalho muda ou um membro da equipe deixa a área de processo de negócio. Revise periodicamente para garantir que o acesso é apropriado para as atuais ameaças, riscos, tecnologias e necessidades de negócio.
- 04 Atribuir funções para as atividades sensíveis para que haja uma clara separação de funções.
- 05 Fornecer sensibilização e formação sobre papéis e responsabilidades regularmente para que todos compreendam as suas responsabilidades; a importância dos controles; e a integridade, confidencialidade e privacidade das informações da empresa em todas as suas formas.
- 06 Revisar periodicamente definições de controle de acesso, registros e relatórios de exceção para assegurar que todos os privilégios de acesso são válidos e alinhados com os funcionários atuais e suas funções atribuídas.

### Prática de Gestão

### Entradas

### Saídas

Prática de Gestão	De	Descrição	Descrição	Para
<b>DSS06.04 Gerenciar erros e exceções.</b> Gerenciar exceções de processos de negócios e erros e facilitar a sua correção. Incluir escalada de erros e exceções de processos de negócios e a execução de medidas corretivas definidas. Isso fornece garantia de precisão e integridade do processo de informações de negócios.			• Evidencia de correção de erro e remediação	MEA02.04
			• Relatórios de erro e análise de causa raiz	Interno

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**DSS06 Práticas de Processo, Entradas/Saídas e Atividades.**

Atividades				
01 Definir e manter procedimentos para atribuir a propriedade, corrigir erros, substituir os erros e lidar com condições de que saiam dos limites estabelecidos.				
02 Revisar erros, exceções e desvios				
03 Acompanhar, corrigir, aprovar e reenviar documentos-fonte e transações				
04 Manter evidências das ações corretivas				
05 Relatar em tempo hábil erros de processo referentes a informações de negócios relevantes para realizar análise de causa raiz e tendências.				

**Prática de Gestão****DSS06.05 Garantir a rastreabilidade dos eventos de informação e registros.**

Garantir que informações de negócios podem ser associadas ao evento de negócios que as origina e a suas as partes responsáveis. Isso permite a rastreabilidade das informações através do seu ciclo de vida e processos relacionados. Isso garante que a informação que impulsiona o negócio é confiável e foi processada de acordo com os objetivos definidos

**Entradas****De****Saídas****Descrição****Para****Descrição****Interno****• Requisitos de retenção****• Registro de transações****Interno****Atividades**

01 Definir os requisitos de retenção, com base em requisitos de negócios, para atender às necessidades de conformidade, operacionais e relatórios financeiros.

02 Capturar informações de origem, evidências de suporte e registros de transações.

03 Eliminar informações de origem, evidências de suporte e registro das transações de acordo com a política de retenção.

**Prática de Gestão****DSS06.06 Proteger ativos de informação.**

Garantir ativos de informação acessíveis pelo negócio através de métodos aprovados, incluindo informações em formato electrónico (tais como métodos que criam novos ativos sob qualquer forma, dispositivos de mídia portáteis, aplicações de usuários e dispositivos de armazenamento), informações em suporte físico (como documentos de origem ou de relatórios de saída) e informações em trânsito. Isto beneficia o negócio, fornecendo salvaguarda fim-a-fim das informações.

**Entradas****De****Saídas****Descrição****Para****Descrição****DSS05.03****Atividades**

01 Aplicar a classificação de dados e políticas de uso aceitável, políticas de segurança e procedimentos para proteger ativos de informação sob o controle do negócio.

02 Prover conscientização e treinamento de uso aceitável.

03 Restringir o uso, distribuição e acesso físico a informações de acordo com sua classificação.

04 Identificar e implementar processos, ferramentas e técnicas para verificar conformidade.

05 Relatar a negócios e outras partes interessadas sobre as violações e desvios.

**DSS06 Orientação Relacionada**

Padrão Relacionado	Referência Detalhada
Nenhum	

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

---

Página intencionalmente deixada em branco

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## MONITORAR, AVALIAR E ANALISAR (MEA)

- 01. Monitorar, avaliar e analisar o desempenho e conformidade.**
- 02 Monitorar, avaliar e analisar o sistema de controle interno.**
- 03 Monitorar, avaliar e analisar a conformidade com os requisitos externos.**

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

MEA01 Monitorar, avaliar e analisar o desempenho e conformidade		Área: Gestão Domínio: Monitorar, Avaliar e Analisar
<b>Descrição do Processo</b> Coletar, validar e avaliar objetivos e metas de negócios, TI e de processos. Monitorar como os processos estão sendo executados em relação às metas e métricas de desempenho e conformidade acordados, e fornecer relatórios sistemáticos e oportunos.		
<b>Declaração de Propósito do Processo</b> Fornecer transparência do desempenho e conformidade e direcionar ao atingimento de objetivos.		
<b>O processo suporta a realização de um conjunto primário de objetivos de TI:</b>		
<b>Objetivos de TI</b>		<b>Métricas Relacionadas</b>
04 Gestão de risco organizacional de TI		<ul style="list-style-type: none"> <li>• Porcentagem de processos críticos de negócio, serviços de TI e programas de negócios habilitados por TI abrangidos pela avaliação de risco</li> <li>• Número de incidentes significativos relacionados com TI que não foram identificados na avaliação de risco</li> <li>• Porcentagem de avaliações de risco, que incluem riscos relacionados com TI</li> <li>• Frequência de atualização do perfil de risco</li> </ul>
07 Prestação de serviços de TI em consonância com os requisitos de negócio		<ul style="list-style-type: none"> <li>• Número de interrupções nos negócios devido a incidentes de serviço</li> <li>• Porcentagem de partes interessadas no negócio satisfeitas com a entrega de dentro dos níveis de serviço acordados</li> <li>• Porcentagem de usuários satisfeitos com a qualidade da prestação de serviços de TI</li> </ul>
11 Otimização de ativos, recursos e capacidades de TI		<ul style="list-style-type: none"> <li>• Frequência das avaliações de maturidade, de capacidade e otimização de custo</li> <li>• Tendência dos resultados da avaliação</li> <li>• Níveis de satisfação de negócios e executivos de TI relacionados a custos e capacidades de TI</li> </ul>
15 Conformidade de TI com as políticas internas		<ul style="list-style-type: none"> <li>• Número de incidentes relacionados com a não conformidade com a política</li> <li>• Porcentagem de interessados que entenderam as políticas</li> <li>• Porcentagem de políticas apoiadas por normas vigentes e práticas de trabalho</li> <li>• Frequência de revisão e atualização de políticas</li> </ul>
<b>Objetivos e Métricas do Processo</b>		
<b>Objetivo do Processo</b>		Métricas relacionadas
01 Objetivos e métricas são aprovados pelas partes interessadas.		<ul style="list-style-type: none"> <li>• Porcentagem de metas e métricas aprovadas pelas partes interessadas</li> </ul>
02 Processos são medidos em relação às metas e métricas acordados.		<ul style="list-style-type: none"> <li>• Porcentagem de processos, com metas e métricas definidas</li> </ul>
03 A abordagem organizacional de monitoramento, avaliação e informação é eficaz e operacional.		<ul style="list-style-type: none"> <li>• Porcentagem de processos com eficácia das metas e métricas revistos e melhorados</li> <li>• Percentagem de processos críticos monitorados</li> </ul>
04 Metas e métricas são integrados nos sistemas de monitoramento empresa.		<ul style="list-style-type: none"> <li>• Porcentagem de metas e métricas alinhadas ao sistema de monitoramento corporativo</li> </ul>
05 Relatórios de desempenho e conformidade de processos são útil e tempestivos.		<ul style="list-style-type: none"> <li>• Porcentagem de relatórios de desempenho entregues conforme o programado</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

MEA01 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do Valor da TI	Diretor de Riscos (CFO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>MEA01.01</b> Estabelecer uma abordagem de monitoração.	A	R	R	R	I	C		I			C	C	C	R	I	C	C	C	I	C	I	I	I	I		
<b>MEA01.02</b> Definir metas de desempenho e conformidade.	I	I	I	A	R			I			C	C	C	R	R	I	R	I	I	I	I	I	I	I		
<b>MEA01.03</b> Coletar e processar dados de desempenho e conformidade.				C	R			I			C		A	R	R	I	R	I	I	I	I	I	I	I		
<b>MEA01.04</b> Analisar e reportar o desempenho.				A	R			C			C	C	C	C	C	R	R	C	R	C	C	C	C	C		
<b>MEA01.05</b> Garantir a aplicação de medidas corretivas.	I	I	I	I	C	R		C			C	C	C	A	C	R	R	C	R	C	C	C	C	C		

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 101. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

MEA01 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Para	Descrição	Para
<b>MEA01.01 Estabelecer uma abordagem de monitoramento.</b> Envolver-se com as partes interessadas para estabelecer e manter uma abordagem de monitoramento para definir os objetivos, escopo, método para medir a solução de negócios, entrega de serviços e de contribuição para os objetivos da empresa. Integrar esta abordagem com o sistema de gerenciamento de desempenho corporativo.	EDM05.01	<ul style="list-style-type: none"> <li>• Princípios de relatórios e de comunicações</li> <li>• Avaliação de requisitos de relatórios corporativos</li> <li>• Regras para avaliação e aprovação de relatórios obrigatórios</li> <li>• Avaliação da eficácia de relatórios</li> </ul>	• Requisitos de monitoramento	Interno
			• Métricas e metas de monitoramento aprovadas	Interno
	EDM05.03			

## Atividades

- 01 Identificar as partes interessadas (por exemplo, gestores, proprietários e usuários de processo).
- 02 Envolver-se com as partes interessadas e comunicar os requisitos e objetivos da empresa para o monitoramento, agregando e relatórios, usando definições comuns (por exemplo, glossário da empresa, metadados e taxonomia), baselining e benchmarking.
- 03 Alinhar e continuamente manter o monitoramento e a abordagem de avaliação com a abordagem empresarial e as ferramentas a serem utilizados para a coleta de dados e geração de relatórios corporativos (por exemplo, aplicações de business intelligence).
- 04 Acordar sobre as metas e métricas (por exemplo, conformidade, desempenho, valor, risco), taxonomia (classificação e relações entre objetivos e métricas) e de retenção de dados (provas).
- 05 Acordar sobre a gestão do ciclo de vida e processo de controle de mudanças para o monitoramento e relatórios. Incluir

05 Acordar sobre a gestão do ciclo de vida e processo de controlo de mudanças para o monitoramento e relatórios. Incluir oportunidades de melhoria para relatórios, métricas, abordagem, baselining e benchmarking.
06 Solicitar, priorizar e alocar recursos para o monitoramento (considere adequação, eficiência, eficácia e confidencialidade).
07 Periodicamente validar a abordagem utilizada e identificar novas ou alterações nas partes interessadas, requisitos e recursos.

# COBIT® 5 : HABILITANDO PROCESSOS

## MEA01 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
MEA01.02 Definir metas de desempenho e conformidade.	De	Descrição	Descrição	Para
Trabalhar com as partes interessadas para definir, periodicamente, rever, atualizar e aprovar metas de desempenho e conformidade, no âmbito do sistema de medição de desempenho.	APO01.07	<ul style="list-style-type: none"> <li>• Metas de desempenho e métricas para rastreamento de melhoria de processos</li> </ul>	<ul style="list-style-type: none"> <li>• Alvos de monitoramento</li> </ul>	APO Todos BAI Todos MEA Todos
<b>Atividades</b>				
01 Definir e rever periodicamente com as partes interessadas as metas e métricas para identificar quaisquer itens em falta significativas e definir razoabilidade das metas e tolerâncias.				
02 Comunicar as alterações propostas para as metas e tolerâncias (relativas às métricas) de desempenho e conformidade com as principais partes interessadas de due diligence (por exemplo, jurídica, auditoria, RH, ética, conformidade, finanças).				
03 Publicar alvos e tolerâncias alteradas aos usuários destas informações.				
04 Avaliar se os objetivos e métricas são adequados, ou seja, específicos, mensuráveis, alcançáveis, relevantes e com prazos (SMART).				
Prática de Gestão	Entradas		Saídas	
MEA01.03 Coletar e processar dados de desempenho e conformidade.	De	Descrição	Descrição	Para
Coletar e processar tempestivamente dados precisos alinhados com abordagens empresariais.	APO01.07 APO05.04 APO09.04 APO10.05 BAI01.06 BAI04.04 BAI05.05 DSS01.05 DSS02.07	<ul style="list-style-type: none"> <li>• Avaliações de capacidade de processo</li> <li>• Relatórios de desempenho da carteira de investimento</li> <li>• Relatórios de desempenho de nível de serviço</li> <li>• Resultados da revisão de controle da conformidade do fornecedor</li> <li>• Resultados de avaliações de desempenho do programa</li> <li>• Relatórios de desempenho e disponibilidade</li> <li>• Medidas de sucesso e resultados</li> <li>• Relatórios de avaliação de instalações</li> <li>• Relatório de status de cumprimento de requisitos e tendências            • Relatório de status de incidentes e tendências</li> </ul>	<ul style="list-style-type: none"> <li>• Dados de monitoramento processados</li> </ul>	Interno
<b>Atividades</b>				
01 Coletar dados a partir de processos definidos - automatizados, sempre que possível.				
02 Avaliar a eficiência (esforço em relação à visão fornecida) e adequação (utilidade e significado) e validar a integridade (precisão e completude) dos dados coletados.				
03 Agregar dados para suportar a coleta das métricas acordadas.				
04 Alinear dados agregados à abordagem de reporte e objetivos corporativos.				
05 Use ferramentas e sistemas para processamento e formatação adequados dos dados para análise.				

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

## MEA01 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA01.04 Analisar e reportar o desempenho.</b> Periodicamente revisar e reportar o desempenho contra metas, usando um método que forneça uma visão geral e sucinta do desempenho de TI e que se encaixe dentro do sistema de monitoramento corporativo.			• Relatórios de desempenho	EDM01.03 APO Todos BAI Todos DSS Todos MEA Todos

## Atividades

- 01 Desenhar relatórios de desempenho do processo concisos, fáceis de entender e adaptadas às diversas necessidades de gestão e audiências. Facilitar, a tomada efetiva e oportuna de decisão (por exemplo, scorecards, relatórios de semáforo) e garantir que a causa e efeito entre os objetivos e métricas são comunicadas de forma compreensível.
- 02 Comparar os valores de desempenho com as metas internas e benchmarks e, quando possível, com referências externas (indústria e os principais concorrentes).
- 03 Recomendar alterações às metas e métricas, quando apropriado.
- 04 Distribua relatórios às partes interessadas.
- 05 Analisar a causa dos desvios contra alvos, iniciar ações corretivas, atribuir responsabilidades de remediação, e acompanhamento. Em momentos apropriados, rever todos os desvios e procurar a causa raiz, onde for necessário. Documentar os problemas para obter mais orientações se o problema persistir. Documentar os resultados.
- 06 Sempre que possível, ligar o cumprimento de metas de desempenho ao sistema de recompensa organizacional.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA01.05 Garantir a implementação de ações corretivas.</b> Ajudar as partes interessadas na identificação, abertura e acompanhamento de ações corretivas para resolver anomalias.	EDM05.02	• Orientações para escalação	• Ações de remediação e atribuições	APO Todos BAI Todos DSS Todos MEA Todos
	APO01.08	• Ações de remediação de inconformidades	• Status e resultado de ações	EDM01.03

## Atividades

- 01 Revisar respostas, opções e recomendações da gerência para abordar problemas e principais desvios.
- 02 Garantir que a atribuição de responsabilidade pela ação corretiva é mantida.
- 03 Acompanhar os resultados de ações acordadas.
- 04 Comunicar os resultados às partes interessadas

## MEA01 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
ISO/IEC 20000	6.2 Relatórios de Serviço
ITIL V3 2011	Melhoria Contínua de Serviço, 4.1 O Processo de Melhoria em 7 Passos

# COBIT® 5 : HABILITANDO PROCESSOS

**MEA02 Monitorar, Avaliar e Analisar o Sistema de Controles Internos**

**Área: Gestão**

**Domínio: Monitorar, Avaliar e Analisar**

## Descrição do processo

Continuamente monitorar e avaliar o ambiente de controle, incluindo auto avaliações e análises de garantia independentes. Habilitar os gestores para identificar deficiências de controle e ineficiências e para iniciar ações de melhoria. Planejar, organizar e manter padrões para as atividades de avaliação e controle de segurança interna.

## Declaração de Propósito processo

Obter transparéncia para as principais partes interessadas sobre a adequação do sistema de controles internos e, assim, proporcionar confiança em operações, a confiança na realização dos objectivos da empresa e uma compreensão adequada do risco residual

### O processo suporta a realização de um conjunto primário de objetivos de TI:

Objetivos de TI	Métricas Relacionadas
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custo da não-conformidade de TI, incluindo punições e multas, e o impacto da perda de reputação</li> <li>Número de não conformidades relacionadas a TI comunicados à direção ou que causaram comentário público ou constrangimento</li> <li>Número de problemas de conformidade relativas aos acordos contratuais com prestadores de serviços de TI</li> <li>Cobertura das avaliações de conformidade</li> </ul>
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Porcentagem de processos críticos de negócio, serviços de TI e programas de negócios habilitados por TI abrangidos pela avaliação de risco</li> <li>Número de incidentes significativos relacionados com TI que não foram identificados na avaliação de risco</li> <li>Porcentagem de avaliações de risco, que incluem riscos relacionados com TI</li> <li>Frequência de atualização do perfil de risco</li> </ul>
15 Conformidade de TI com as políticas internas	<ul style="list-style-type: none"> <li>Número de incidentes relacionados com a não conformidade com a política</li> <li>Porcentagem de interessados que entenderam as políticas</li> <li>Porcentagem de políticas apoiadas por normas vigentes e práticas de trabalho</li> <li>Frequência de revisão e atualização de políticas</li> </ul>

### Objetivos e Métricas do Processo

Objetivos do Processo	Métricas Relacionadas
1.Processos, recursos e informações atendendo aos requisitos de sistema de controles internos da empresa.	<ul style="list-style-type: none"> <li>Porcentagem de processos com cumprimento de metas de produção assegurada dentro da tolerância</li> <li>Porcentagem de processos assegurada como compatível com os objetivos de controlo interno</li> </ul>
02 Todas as iniciativas de garantia são planejadas e executadas de forma eficaz.	<ul style="list-style-type: none"> <li>Porcentagem de iniciativas de garantia seguindo padrões de programas de garantia aprovados</li> </ul>
03 Garantia independente de que o sistema de controle interno é eficaz e operacional é fornecido.	<ul style="list-style-type: none"> <li>Porcentagem de processos que receberam revisão independente</li> </ul>
04 O controle interno é estabelecido e deficiências são identificados e relatadas	<ul style="list-style-type: none"> <li>Número de pontos fracos identificados por relatórios de qualificação e de certificação externos</li> <li>Número de grandes violações de controles internos</li> <li>Tempo entre a ocorrência de deficiência de controle interno e seu relato</li> </ul>

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

MEA02 Tabela RACI

Prática de Gestão	Conselho de Administração	Diretor Executivo (Presidente) (CEO)	Diretor Financeiro (CFO)	Diretor de Operações (COO)	Executivo de Negócios	Responsável pelo Processo de Negócios	Comitê Executivo Estratégico	Comitês Diretivos (Projeto e Programa)	Escritório de Programas e Projetos (PMO)	Escritório de Gestão do valor da TI	Diretor de Riscos (CRO)	Diretor de Segurança da Informação (CSO)	Conselho de Arquitetura	Comitê de Riscos da Organização	Chefe de RH	Conformidade	Auditor	Diretor de TI (CIO)	Chefe de Arquitetura	Chefe de Desenvolvimento	Chefe de Operações de TI	Chefe de Administração de TI	Gerente de Serviços	Gerente de Segurança da Informação	Gerente de Continuidade dos Negócios	Oficial de Privacidade
<b>MEA02.01</b> Monitorar os controles internos.	I	C	I	C	R				R	R					R	R	A	I	R	C		C	C	C	R	
<b>MEA02.02</b> Revisar a eficácia dos controles de processos de negócios.	I	I	R	I	A	R	I			I	I				R	R	C				C	C	C			
<b>MEA02.03</b> Realizar auto avaliações dos controles.	I	C	I	C	R			R	R						R	R	A	I	R	R	R	R	R	R	R	
<b>MEA02.04</b> Identificar e reportar deficiências nos controles.	I	C	I	C	R			R	I	I					R	R	A	I	R	R	R	R	R	R	R	
<b>MEA02.05</b> Assegurar que os provedores de garantias são independentes e qualificados					R										A	A	R									
<b>MEA02.06</b> Planejar iniciativas de garantia	A			C	R			C							C	C	R	C	C	C	C	C	C	C	C	
<b>MEA02.07</b> Definir o escopo de ações de garantia				R	R	R		C							C	A	R	C	C	C	C	C	C	C	C	
<b>MEA02.08</b> Executar iniciativas de garantia	I	I		C	R			C	I	I					C	A	R	C	C	C	C	C	C	C	C	

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11 Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

MEA02 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.01 Monitorar os controles internos.</b> Continuamente monitorar, avaliar e melhorar ambiente de TI e estrutura de controle para atender os objetivos da organização.	APO12.04	• Resultados de avaliações de riscos de terceiros	• Resultados do monitoramento e revisão dos controles internos	EDM01.03 APO Todos BAI Todos DSS Todos MEA Todos
	APO13.03	• Relatórios de auditoria do ISMS	• Resultados de benchmarking e outras avaliações	EDM01.03 APO Todos BAI Todos DSS Todos MEA Todos
	Referência externa ao COBIT	• Padrões Internacionais e boas práticas		

# COBIT® 5 : HABILITANDO PROCESSOS

## MEA02 Práticas de Processo, Entradas/Saídas e Atividades.

Atividades
01 Realizar atividades de monitoramento e avaliação de controles internos com base em padrões de governança organizacionais e estruturas e práticas aceitas pela indústria. Incluir o monitoramento e avaliação da eficiência e eficácia das revisões de supervisão gerencial.
02 Considerar avaliações independentes do sistema de controlo interno (por exemplo, auditoria interna ou entre pares).
03 Identificar os limites do sistema de controles internos de TI (por exemplo, considere como os controles da TI organizacional levam em conta terceirizados e/ou atividades, desenvolvimento e produção off-shore).
04 Garantir que as atividades de controle são realizadas e as exceções são imediatamente comunicadas, acompanhadas e analisadas, e as ações corretivas apropriadas sejam priorizadas e implementadas de acordo com o perfil de gestão de risco (por exemplo, classificar certas exceções como um risco chave e outros como a não chave).
05 Manter o sistema de controles internos de TI, considerando mudanças em curso no mundo dos negócios e riscos de TI, o ambiente de controle organizacional, negócios relevantes e processos de TI e riscos de TI. Se existem lacunas, avaliar e recomendar mudanças.
06 Avaliar regularmente o desempenho do sistema de controles de TI, comparando a normas e boas práticas aceitas pela indústria. Considerar a adoção formal de uma abordagem de melhoria contínua para monitoração dos controles internos.
07 Avaliar o status dos controles internos dos prestadores de serviços externos e confirmar que estes cumprem com os requisitos legais, regulamentares e obrigações contratuais.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.02 Revisar a eficácia dos controles de processo de negócio.</b> Rever o funcionamento dos controles, incluindo uma revisão da monitoração e provas de teste, para assegurar que os controles inseridos nos processos de negócio funcionam eficazmente. Incluir atividades para manter evidência da operação eficaz de controles através de mecanismos como testes periódicos de controles, monitoramento contínuo de controles, avaliações independentes, centros de comando e controle e centros de operações de rede. Isto fornece ao negócio a garantia de eficácia dos controles para atender aos requisitos relacionados ao negócio, regulamentares e responsabilidade social.	BAI05.06	• Resultados de auditorias de conformidade	• Evidencia de eficácia de controles	Interno
	BAI05.07	• Revisões de uso operacional		

Atividades
01 Entender e priorizar riscos conforme os objetivos organizacionais.
02 Identificar os controles-chave e desenvolver uma estratégia adequada para a validação de controles.
03 Identificar informações que indicam convincentemente se o ambiente de controles internos está funcionando de forma eficaz.
04 Desenvolver e implementar procedimentos eficientes para determinar se a informação persuasiva baseia-se nos critérios de informação.
05 Manter evidência de eficácia dos controles.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.03 Realizar auto avaliações de controles.</b> Incentivar gestores e donos de processos para assumir a responsabilidade pela melhoria dos controles através de um programa contínuo de auto avaliação para avaliar a integridade e eficácia do controle de gestão sobre os processos, políticas e contratos.			• Planos e critérios de auto avaliação	APO Todos BAI Todos DSS Todos MEA Todos
			• Resultados de auto avaliações	Interno
			• Resultados das revisões de auto avaliações	EDM01.03 APO Todos BAI Todos DSS Todos MEA Todos

## CAPÍTULO 5

## CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

**MEA02 Práticas de Processo, Entradas/Saídas e Atividades.**

Atividades			
01 Manter planos, escopo e identificar critérios de avaliação para a realização de auto avaliação. Planejar a comunicação dos resultados do processo de auto avaliação para a área de negócios, TI e gestão geral e do conselho. Considerar as normas de auditoria interna no desenho das auto avaliações.			
02 Determinar a frequência das auto avaliações periódicas, tendo em conta a eficácia e a eficiência global de monitoração contínua.			
03 Atribuir a responsabilidade da auto avaliação a indivíduos apropriados para assegurar a objetividade e competência.			
04 Prover revisões independentes para assegurar a objetividade da auto avaliação e permitir o compartilhamento de boas práticas de controle interno de outras empresas.			
05 Comparar os resultados das auto avaliações contra os padrões da indústria e boas práticas.			
06 Resumir e relatar os resultados da auto avaliação e benchmarking para acções correctivas.			
07 Definir uma abordagem acordada, consistente para a realização de auto avaliação de controles e em coordenação com os auditores internos e externos.			

Prática de Gestão	Entradas		Saídas		
	De	Descrição	Descrição	Para	
<b>MEA 02.04 Identificar e reportar deficiências de controle.</b>  Identificar deficiências de controle e analisar e identificar as suas causas subjacentes. Escalar deficiências de controle e informar as partes interessadas.	APO11.05	• Causa raiz de falhas na entrega de qualidade	• Deficiências de controles	APO Todos BAI Todos DSS Todos MEA Todos	
	APO12.06	• Causa raiz relacionadas com os riscos			
	DSS06.01	• Análise de causa raiz e recomendações • Resultado do processamento de revisões de eficácia	• Ações de remediação		
	DSS06.04	• Evidências de correção de erro e remediação			

Atividades			
01 Identificar, relatar e registrar as exceções de controle, e atribuir a responsabilidade por resolvê-las e informar sobre o status.			
02 Considerar o risco empresarial ao estabelecer limites para escalada de exceções de controle e avarias.			
03 Comunicar os procedimentos para a escalada de exceções de controle, análise de causa raiz, e relatórios para os donos de processos de TI.			
04 Decida quais exceções de controle devem ser comunicadas à pessoa responsável pela função e quais exceções devem ser escaladas. Informar os proprietários dos processos afetados e partes interessadas.			
05 Acompanhar todas as exceções para garantir que as ações acordadas foram endereçadas.			
06 Identificar, iniciar, monitorar e implementar ações corretivas decorrentes de avaliações e relatórios de controle.			

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.05 Assegure que os prestadores de seguros são independentes e qualificados.</b>  Certifique-se de que as entidades que exercem garantia são independentes da função, grupos ou organizações em âmbito. As entidades que executam garantia devem demonstrar uma atitude adequada e aparência, competência nas habilidades e conhecimentos necessários para executar a garantia, e a adesão a códigos de ética e normas profissionais.			• Resultados de avaliações por provedores de garantia	Interno

Atividades			
01 Estabelecer a adesão a códigos de ética e padrões aplicáveis (por exemplo, Código de Ética Profissional da ISACA) e normas de garantia (específicos da Indústria localidade), por exemplo: Padrões de Garantia e Auditoria de TI da ISACA, International Auditing and Assurance Standards Board's (IAASB's), International Framework for Assurance Engagements (IAASB Assurance Framework).			
02 Estabelecer a independência dos prestadores de garantia.			
03 Estabelecer competência e qualificação dos prestadores de garantia.			

# COBIT® 5 : HABILITANDO PROCESSOS

## MEA02 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.06 Planejar iniciativas de garantia.</b> Planejar iniciativas de garantia com base em objetivos empresariais e prioridades estratégicas, risco inerente, limitações de recursos e de conhecimentos suficientes sobre a empresa.	BAI01.05	• Planos do programa de auditoria	• Avaliações de alto nível	Interno
	DSS01.02	• Planos de garantia independente	• Planos de garantia	EDM01.03 APO Todos BAI Todos DSS Todos MEA Todos
			• Critérios de avaliação	Interno

### Atividades

- 01 Determinar os usuários pretendidos para os resultados da iniciativa de garantia e o objeto da revisão.
- 02 Realizar uma avaliação de risco de alto nível e/ou avaliação da capacidade do processo para diagnosticar o risco e identificar os processos críticos de TI.
- 03 Selecione, personalizar e chegar a um acordo sobre os objetivos de controle para processos críticos que serão a base para a avaliação de controle.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.07 Definir o escopo de iniciativas de garantia.</b> Definir e acordar com a administração sobre o alcance da iniciativa de garantia, com base nos objetivos de garantia.	APO11.05	• Causa raiz de falhas na entrega de qualidade	• Escopo de revisão de garantia	Interno
	APO12.06	• Causa raiz relacionadas com os riscos	• Plano de compromisso	Interno
	DSS06.01	• Análise de causa raiz e recomendações	• Práticas de revisão de garantia	Interno
	MEA03.04	• Relatórios de problemas de conformidade e causa raiz		

### Atividades

- 01 Definir o alcance real, identificando os objetivos da empresa e de TI para o ambiente em análise, o conjunto de processos e recursos, e todas as entidades auditáveis relevantes dentro da empresa e externas à empresa (por exemplo, prestadores de serviços), se aplicável.
- 02 Definir o plano de engajamento e requisitos de recursos.
- 03 Definir práticas para a coleta e avaliação de informações de processo(s) sob revisão para identificar controles a ser validados, e as conclusões atuais (Ambos garantia positiva e quaisquer deficiências) para avaliação de risco.
- 04 Definir práticas para validar projeto de controle e os resultados e determinar se o nível de eficácia suporta risco aceitável (exigido pela avaliação de risco organizacional ou de processo).
- 05 Sempre que a eficácia do controlo não for aceitável, definir práticas para identificar o risco residual (em preparação para relatórios

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA02.08 Executar iniciativas de garantia.</b> Executar a iniciativa de garantia planejada. Relatar as conclusões identificadas. Fornecer opiniões positivas de garantia, se for o caso, e recomendações para a melhoria relativa ao desempenho operacional identificados, conformidade externa e risco residual do sistema de controles internos.	APO11.05	• Causa raiz de falhas na entrega de qualidade	• Escopo refinado	APO Todos BAI Todos DSS Todos MEA Todos
	APO12.04	• Análise de riscos e relatórios de perfil de riscos para as partes interessadas	• Resultados da revisão de garantia	EDM05.01 EDM05.03 APO Todos BAI Todos DSS Todos MEA Todos
	APO12.06	• Causa raiz relacionadas com os riscos		
	DSS05.02	• Resultados de testes de invasão		
	DSS06.01	• Análise de causa raiz e	• Relatório de revisão de	EDM05.03

	DSS00.01	• Análise de causa raiz e recomendações	• Relatório de revisão de garantia	EDM00.05 APO Todos BAI Todos DSS Todos MEA Todos
	MEA03.03	• Gaps de conformidade identificados		

206

Personal Copy of: Sr. Felipe Soares de Oliveira

## CAPÍTULO 5

### CONTEÚDO DO GUIA DE REFERÊNCIAS DE PROCESSOS DO COBIT 5

#### MEA02 Práticas de Processo, Entradas/Saídas e Atividades.

Atividades
01 Refinar a compreensão do assunto garantia de TI.
02 Refinar o escopo dos objetivos-chave de controlo para o assunto garantia de TI.
03 Testar a eficácia do desenho do controle aos objetivos fundamentais do controle.
04 Em alternativa/adicionalmente testar o resultado dos objetivos de controle chave.
05 Documentar o impacto das deficiências de controle.
06 Comunicar à gestão durante a execução da iniciativa para que haja uma compreensão clara do trabalho realizado e acordo sobre e aceitação das conclusões e recomendações preliminares.
07 Supervisionar as atividades de garantia e certificar-se de que o trabalho realizado está completo, atende aos objetivos e é de qualidade aceitável.
08 Fornecer à gestão um relatório (alinhado com os termos de referência, escopo e padrões de relatórios acordados) que suporta os resultados da iniciativa e permite um foco claro sobre as principais questões e ações importantes.

#### MEA02 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
Nenhum	

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## MEA03 Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos

**Área:** Gestão

**Domínio:** Monitorar, Avaliar e Analisar

### Descrição do Processo

Avaliar que os processos de TI e processos de negócio dependentes de TI estão em conformidade com leis, regulações e requerimentos contratuais. Obter garantia de que os requerimentos foram identificados e estão com conformidade com, e estão integrados com as conformidades de TI dentro da conformidade geral da empresa.

### Declaração de Propósito processo

Garantir que a empresa está em conformidade com todos os requerimentos externos aplicáveis.

#### O processo suporta a realização de um conjunto primário de objetivos de TI:

Objetivos de TI	Métricas Relacionadas
02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos	<ul style="list-style-type: none"> <li>Custos de não-conformidade de TI, incluindo acordos e multas, e o impacto causado por perda reputacional</li> <li>Número de deficiências de não-conformidades de TI reportadas ao conselho ou que causaram comentários ou constrangimentos públicos</li> <li>Número de deficiências de não-conformidades relacionadas à acordos contratuais com provedores de serviço de TI</li> <li>Cobertura da análise de conformidade</li> </ul>
04 Gestão de risco organizacional de TI	<ul style="list-style-type: none"> <li>Porcentagem de processos críticos do negócio, serviços de TI e programas de negócio suportados por TI cobertos pela avaliação de riscos</li> <li>Número de Incidentes Significativos de TI que não foram identificados na avaliação de riscos</li> <li>Porcentagem avaliação de riscos da empresa incluindo riscos de TI</li> <li>Frequência de atualização do perfil de riscos</li> </ul>

#### Objetivos e Métricas do Processo

Objetivo do Processo	Métricas relacionadas
01 Todos os requerimentos externos de conformidade foram identificados.	<ul style="list-style-type: none"> <li>Média de tempo entre a identificação de deficiências de conformidade externas e sua resolução</li> <li>Frequência de revisões de conformidade</li> </ul>
02 Requerimentos de Conformidade Externas estão adequadamente endereçadas.	<ul style="list-style-type: none"> <li>Número de deficiências críticas de não conformidade identificadas por ano</li> <li>Porcentagem de aprovações dos donos dos processos confirmando conformidade</li> </ul>

CAPÍTULO 5

MEA03 Tabela RACI

**Nota:** Algumas práticas de governança e gestão produzem saídas que servem como entradas para outras práticas. Estas saídas são detalhadas na figura 11. Por favor, verifique a figura 11 para garantir a cobertura necessária quando estiver trabalhando com as práticas que as seguem.

MEAD3 Práticas de Processo, Entradas/Saídas e Atividades.

Prática de Gestão	Entradas		Saídas			
	De	Descrição	Descrição	Para		
<b>MEA03.01 Identificar requerimentos externos de conformidade.</b>  Com base continua, identificar e monitorar alterações em leis e regulações locais e internacionais, assim como outros requerimentos externos de TI que precisam ser atendidos.	Referência externa ao COBIT	<ul style="list-style-type: none"> <li>• Requerimentos de conformidade legais e regulatórios</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de requerimentos de Conformidade</li> </ul>	Interno		
			<ul style="list-style-type: none"> <li>• Registro de ações de conformidade requeridas</li> </ul>	Interno		
<b>Atividades</b>						
01 Atribuir responsabilidades por identificação e monitoramento de quaisquer alterações legais, regulatórias e outros requerimentos contratuais externos relevantes para o uso de recursos de TI e para o processamento de informações de negócios e operações de TI da empresa						
02 Identificar e avaliar todos os potenciais requerimentos de conformidade e impactos em atividade de TI em áreas como fluxo de dados, privacidade, controles internos, reportes financeiros, regulações industriais específicas, propriedade intelectuais, saúde e segurança						
03 Avaliar o impacto à TI relacionado a requerimentos legais e regulatórios em contratos com fornecedores de operações de TI, provedores de serviço e parceiros de negócio.						
04 Obter aconselhamento independente, onde for apropriado, quanto a alterações aplicáveis a leis, regulações e standards						
05 Manter um registro atualizado de todos os requerimentos relevantes legais, regulatórios e contratuais, assim como impactos e ações requeridas.						
06 Manter um registro harmonizado e geral de requerimentos de conformidade externos para a empresa.						
Prática de Gestão	Entradas		Saídas			
<b>MEA03.02 Otimizar respostas a requerimentos externos.</b>	De	Descrição	Descrição	Para		
			Políticas, princípios,	APO01.07		

Personal Copy of: Sr. Felipe Soares de Oliveira

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

## MEA03 Práticas de Processo, Entradas/Saídas e Atividades.

### Atividades

- 01 Revisar e ajustar regularmente políticas, princípios, standards, procedimentos e metodologias para sua eficácia na garantia necessária de conformidade e endereçamento de riscos da empresa utilizando especialistas internos e externos, caso necessários.
- 02 Comunicar requerimentos novos e alterados a todo pessoal relevante.

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA03.03 Confirmar conformidade externa.</b> Confirmar conformidade com políticas, princípios, standards, procedimentos e metodologias com requerimentos legais regulatórios e contratuais.	BAI05.06	• Resultados da auditoria de Conformidade	• Gaps de Conformidade identificados	MEA02.08
	BAI09.05	• Resultado de auditorias de licenças instaladas	• Confirmações de Conformidade	EDM01.03
	BAI10.05	• Desvios de Licenças		
	DSS01.04	• Relatório de Apólices de seguro		

### Atividades

- 01 Avaliar regularmente políticas organizacionais, standards, procedimentos e metodologias em todas as funções da empresa para garantir conformidade com requerimentos legais e regulatórios relevantes com relação ao processamento de informações.
- 02 Endereçar gaps de políticas, standards e procedimentos de forma tempestiva.
- 03 Avaliar periodicamente processos e atividades de negócios e de TI para garantir aderência à requerimentos aplicáveis legais, regulatórios e contratuais.
- 04 Revisar regularmente para padrões recorrentes de falhas de conformidade. Onde for necessário, aprimore políticas, standards, procedimentos, metodologias e atividades e processos associados

Prática de Gestão	Entradas		Saídas	
	De	Descrição	Descrição	Para
<b>MEA03.04 Obter garantia de conformidade externa.</b> Obter e reportar garantia de conformidade e aderência com políticas, princípios, standards, procedimentos e metodologias. Confirmar que ações corretivas para endereçar gaps de conformidade são finalizadas tempestivamente.	EDM05.02	• Regras para validação e aprovação de relatórios mandatórios	• Relatórios de garantia de conformidade	EDM01.03
	EDM05.03	• Avaliação da eficácia de reporte	• Relatórios de deficiências de não conformidade e causas raízes	

### Atividades

- 01 Obter confirmações regulares de conformidade com políticas internas de donos de processos de TI e de Negócios, assim como de chefes de unidades.
- 02 Realizar revisões regulares (e onde apropriado, independente) internas e externas para avaliar o nível de conformidade.
- 03 Se requerido, obter declarações de terceiros provedores de serviços de TI quanto aos seus níveis de conformidade com leis e regulações aplicáveis.
- 04 Se requerido, obter declaração de parceiros de negócios quanto aos seus níveis de conformidade com leis e regulações aplicáveis a transações eletrônicas entre empresas.
- 05 Monitorar e reportar deficiências de não conformidade e, quando necessário, investigar a causa raiz.
- 06 Integrar relatórios sobre requisitos legais, regulatórios e contratuais a um nível completo de empresa, envolvendo todas as unidades de negócio.

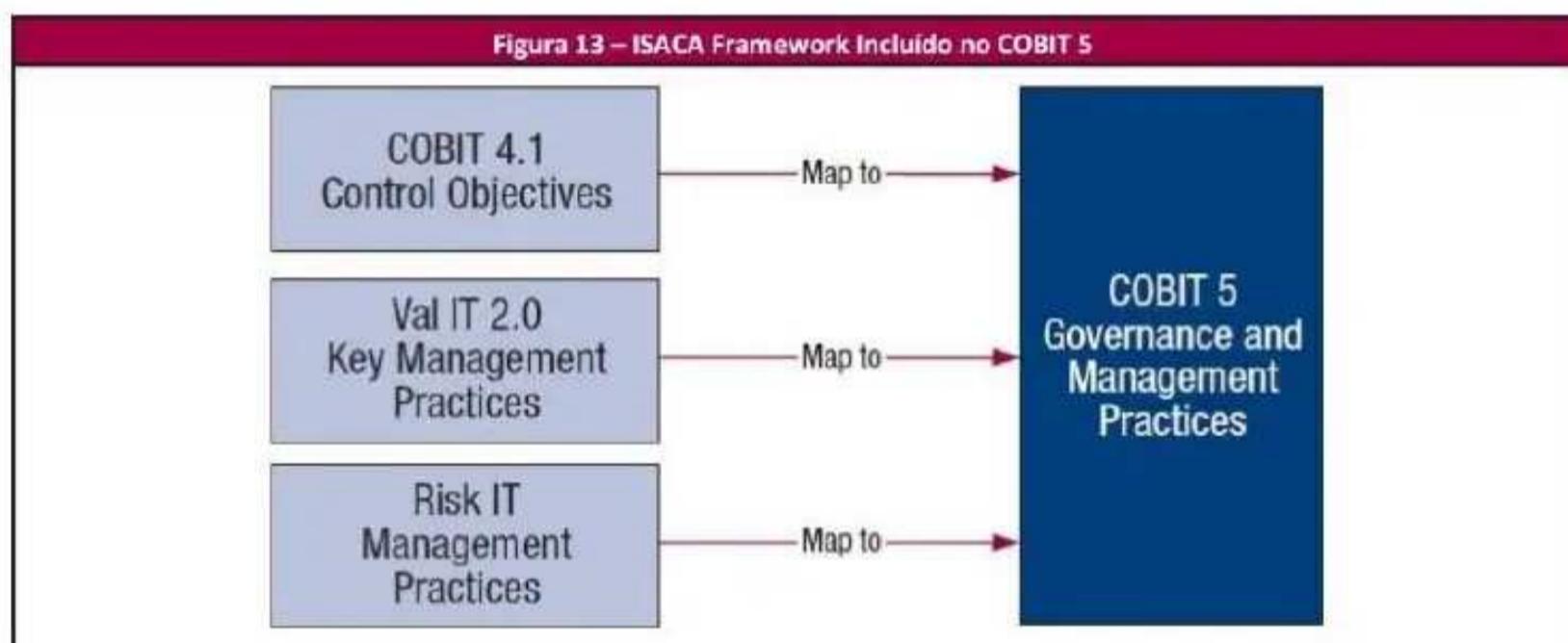
## MEA03 Orientação Relacionada

Padrão Relacionado	Referência Detalhada
Nenhum	

## APÊNDICE A MAPEAMENTO DO COBIT5 E MODELOS LEGADOS DA ISACA

### APÊNDICE A MAPEAMENTO DO COBIT5 E MODELOS LEGADOS DA ISACA

Figura 13 apresenta os modelos da ISACA incluídos no COBIT 5.



O mapeamento do COBIT 4.1, Val IT e componentes de Risco de TI para o COBIT 5 está representado nas figuras 14, 15 e 16.

**Figura 14 – Objetivos de Controle do COBIT 4.1 Mapeados para COBIT 5**

Objetivo de Controle COBIT 4.1		Coberto no COBIT 5 por:
AC1	Preparação e Autorização de Dados Originais	DSS06.02; DSS06.03; BAI03.02; BAI03.03; BAI03.05; BAI03.07
AC2	Entrada e Coleta de Dados Fontes	DSS06.02
AC3	Testes de Veracidade, Totalidade e Autenticidade	DSS06.02
AC4	Processamento Íntegro e Válido	DSS06.02
AC5	Revisão das Saídas, Reconciliação e Manuseio de Erros	DSS06.02
AC6	Autenticação e Integridade das Transações	DSS06.02
PO1.1	Gerenciamento de Valor da TI	EDM02
PO1.2	Alinhamento entre TI e Negócio	APO02.01
PO1.3	Avaliação da Capacidade e Desempenho Correntes	APO02.02
PO1.4	Plano Estratégico de TI	APO02.03-05
PO1.5	Planos Táticos de TI	APO02.05
PO1.6	Gerenciamento do Portfólio de TI	APO05.05
PO2.1	Modelo de Arquitetura da Informação da Organização	APO03.02
PO2.2	Dicionário de Dados Corporativos e Regras de Sintaxe de Dados	APO03.02
PO2.3	Esquema de Classificação de Dados	APO03.02
PO2.4	Gerenciamento de Integridade	APO01.06
PO3.1	Planejamento da Diretriz Tecnológica	APO02.03; APO04.03
PO3.2	Plano de Infraestrutura Tecnológica	APO02.03-05; APO04.03-05
PO3.3	Monitoramento de Regulamentos e Tendências Futuras	EDM01.01; APO04.03

PO3.3	Avaliação e Revisão de Regulamentos e Procedimentos	EDM03.02; APO01.02
PO3.4	Padrões Tecnológicos	APO03.05
PO3.5	Conselho de Arquitetura de TI	APO01.01
PO4.1	Estrutura de Processos de TI	APO01.03; APO01.07
PO4.2	Comitê Estratégico de TI	APO01.01
PO4.3	Comitê Executivo de TI	APO01.01

# COBIT® 5 : HABILITANDO PROCESSOS

Figura 14 – Objetivos de Controle do COBIT 4.1 Mapeados para COBIT 5

Objetivo de Controle COBIT 4.1	Coberto no COBIT 5 por:
PO4.4 Posicionamento Organizacional da área de TI	APO01.05
PO4.5 Estrutura Organizacional de TI	APO01.01
PO4.6 Definição de Papéis e Responsabilidades	APO01.02
PO4.7 Responsabilidade pela Garantia de Qualidade	APO11.01
PO4.8 Responsabilidade por Riscos, Segurança e Conformidade	Removido — Esses papéis específicos não são mais explicitamente especificados como prática.
PO4.9 Proprietários de Dados e Sistemas	APO01.06
PO4.10 Supervisão	APO01.02
PO4.11 Segregação de Funções	APO01.02
PO4.12 Recrutamento de pessoal de TI	APO07.01
PO4.13 Pessoal Chave de TI	APO07.02
PO4.14 Políticas e Procedimentos para Pessoal Contratado	APO07.06
PO4.15 Relacionamentos	APO01.01
PO5.1 Estrutura da Administração Financeira	APO06.01
PO5.2 Priorização dentro do Orçamento de TI	APO06.02
PO5.3 Processo de Orçamento de TI	APO06.03
PO5.4 Gerenciamento de Custo	APO06.04-05
PO5.5 Gerenciamento de Benefícios	APO05.06
PO6.1 Política de TI e Ambiente de Controle	APO01.03
PO6.2 Risco de TI Corporativo e Estrutura Interna de Controle	EDM03.02; APO01.03
PO6.3 Gerenciamento de Políticas de TI	APO01.03; APO01.08
PO6.4 Distribuição da Política	APO01.03; APO01.08
PO6.5 Comunicação dos Objetivos e Diretrizes de TI	APO01.04
PO7.1 Recrutamento e Retenção de Pessoal	APO07.01; APO07.05
PO7.2 Competências Pessoais	APO07.03
PO7.3 Preenchimento de Vagas	APO01.02; APO07.01
PO7.4 Treinamento do Pessoal	APO07.03
PO7.5 Dependência de Indivíduos	APO07.02
PO7.6 Procedimentos de Liberação de Pessoal	APO07.01; APO07.06
PO7.7 Avaliação de Desempenho Profissional	APO07.04
PO7.8 Mudança e Desligamento de Cargo	APO07.01
PO8.1 Sistema de Gerenciamento de Qualidade (SGQ)	APO11.01
PO8.2 Padrões e Práticas de Qualidade de TI	APO11.02
PO8.3 Padrões de Desenvolvimento e Aquisição	APO11.02; APO11.05
PO8.4 Foco no Cliente	APO11.03
PO8.5 Melhoria Contínua	APO11.06
PO8.6 Medição, Monitoramento e Revisão da Qualidade	APO11.04
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios	EDM03.02; APO01.03
PO9.2 Estabelecimento do Contexto de Risco	APO12.03
PO9.3 Identificação de Eventos	APO12.01; APO12.03
PO9.4 Avaliação de Risco	APO12.02; APO12.04
PO9.5 Resposta ao Risco	APO12.06
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	APO12.04-05
PO10.1 Estrutura de Gestão de Programas	BAI01.01
PO10.2 Estrutura de Gestão de Projetos	BAI01.01

PO10.3	Abordagem da Gestão de Projetos	BAI01.01
PO10.4	Comprometimento das Partes Interessadas	BAI01.03
PO10.5	Declaração do Escopo do Projeto	BAI01.07
PO10.6	Fase de Início do Projeto	BAI01.07
PO10.7	Plano Integrado de Projeto	BAI01.08

**APÊNDICE A**  
**MAPEAMENTO DO COBIT5 E MODELOS LEGADOS DA ISACA**

**Figura 14 – Objetivos de Controle do COBIT 4.1 Mapeados para COBIT 5**

Objetivo de Controle COBIT 4.1	Coberto no COBIT 5 por:
PO10.8 Recursos do Projeto	BAI01.08
PO10.9 Gestão de Risco do Projeto	BAI01.10
PO10.10 Plano de Qualidade de Projeto	BAI01.09
PO10.11 Controle de Mudança de Projeto	BAI01.11
PO10.12 Planejamento de métodos de validação	BAI01.08
PO10.13 Medição de Desempenho, Monitoramento e Reporte do Projeto	BAI01.06; BAI01.11
PO10.14 Conclusão do Projeto	BAI01.13
AI1.1 Definição e Manutenção de Requisitos Técnicos e Funcionais de Negócio	BAI02.01
AI1.2 Relatório de Análise de Risco	BAI02.03
AI1.3 Estudo de Viabilidade e Formulação de Ações Alternativas	BAI02.02
AI1.4 Decisão e Aprovação de Requisitos e Estudo de Viabilidade	BAI02.04
AI2.1 Projeto em Nível Macro	BAI03.01
AI2.2 Projeto Detalhado	BAI03.02
AI2.3 Controle e Auditabilidade do Aplicativo	BAI03.05
AI2.4 Segurança e Disponibilidade do Aplicativo	BAI03.01-03; BAI03.05
AI2.5 Configuração e Implementação de Software Aplicativo Adquirido	BAI03.03; BAI03.05
AI2.6 Principais Atualizações dos Sistemas Existentes	BAI03.10
AI2.7 Desenvolvimento de Software Aplicativo	BAI03.03-04
AI2.8 Garantia de Qualidade de Software	BAI03.06
AI2.9 Gestão dos Requisitos das Aplicações	BAI03.09
AI2.10 Manutenção de Software Aplicativo	BAI03.10
AI3.1 Plano de Aquisição de Infraestrutura Tecnológica	BAI03.04
AI3.2 Infraestrutura de Recursos, Proteção e Disponibilidade	BAI03.03; DSS02.03
AI3.3 Manutenção da Infraestrutura	BAI03.10
AI3.4 Viabilidade do Ambiente de Teste	BAI03.07-08
AI4.1 Planejamento para Soluções Operacionais	BAI05.05
AI4.2 Transferência de Conhecimento ao Gerenciamento do Negócio	BAI08.01-04
AI4.3 Transferência de Conhecimento aos Usuários Finais	BAI08.01-04
AI4.4 Transferência de Conhecimento às Equipes de Operações e Suporte	BAI08.01-04
AI5.1 Controle de Aquisição	BAI03.04
AI5.2 Gerenciamento de Contratos de Fornecedores	APO10.01; APO10.03
AI5.3 Seleção de Fornecedores	APO10.02
AI5.4 Aquisição de Recursos de TI	APO10.03
AI6.1 Padrões e Procedimentos de Mudança	BAI06.01-04
AI6.2 Avaliação de Impacto, Priorização e Autorização	BAI06.01
AI6.3 Mudanças de Emergência	BAI06.02
AI6.4 Acompanhamento de Status e Relatórios de Mudanças	BAI06.03
AI6.5 Finalização da Mudança e Documentação	BAI06.04
AI7.1 Treinamento	BAI05.05
AI7.2 Plano de Teste	BAI07.01; BAI07.03
AI7.3 Plano de Implementação	BAI07.01
AI7.4 Ambiente de Testes	BAI07.04
AI7.5 Conversão de Dados e Sistemas	BAI07.02
AI7.6 Teste de Mudanças	BAI07.05
AI7.7 Teste de Aceitação Final	BAI07.05
AI7.8 Preparação para a Produção	BAI07.05

AI7.8	Promoção para a Produção	BAI07.06
AI7.9	Revisão pós-implementação	BAI07.08
DS1.1	Estrutura de Gestão de Níveis de Serviço	APO09.01-05
DS1.2	Definição de Serviços	APO09.01-02
DS1.3	Acordos de Nível de Serviço	APO09.03
DS1.4	Acordos de Nível Operacional	APO09.03

# COBIT® 5 : HABILITANDO PROCESSOS

Figura 14 – Objetivos de Controle do COBIT 4.1 Mapeados para COBIT 5

Objetivo de Controle COBIT 4.1	Coberto no COBIT 5 por:
DS1.5 Monitoramento e Relatório de Realizações de Nível de Serviço	APO09.04
DS1.6 Revisão dos Acordos de Nível de Serviço e dos Contratos	APO09.05
DS2.1 Identificação do Relacionamento com Todos os Fornecedores	APO10.01
DS2.2 Gestão do Relacionamento com Fornecedores	APO10.03
DS2.3 Gerenciamento de Riscos do Fornecedor	APO10.04
DS2.4 Monitoramento de Desempenho do Fornecedor	APO10.05
DS3.1 Desempenho e Planejamento de Capacidade	BAI04.03
DS3.2 Capacidade e Desempenho Atuais	BAI04.01-02
DS3.3 Capacidade e Desempenho Futuros	BAI04.01
DS3.4 Disponibilidade de Recursos de TI	BAI04.05
DS3.5 Monitoramento e Relatórios	BAI04.04
DS4.1 Estrutura de Continuidade	DSS04.01-02
DS4.2 Planos de Continuidade de TI	DSS04.03
DS4.3 Recursos Críticos de TI	DSS04.04
DS4.4 Manutenção do Plano de Continuidade de TI	DSS04.02; DSS04.05
DS4.5 Teste do Plano de Continuidade de TI	DSS04.04
DS4.6 Treinamento do Plano de Continuidade de TI	DSS04.06
DS4.7 Distribuição do Plano de Continuidade	DSS04.03
DS4.8 Recuperação e Retomada dos Serviços de TI	DSS04.03
DS4.9 Armazenamento de Cópias de Segurança em Locais Remotos	DSS04.07
DS4.10 Revisão Pós-Retomada dos Serviços	DSS04.08
DS5.1 Gestão da Segurança de TI	APO13.01; APO13.03
DS5.2 Plano de Segurança de TI	APO13.02
DS5.3 Gestão de Identidade	DSS05.04
DS5.4 Gestão de Contas de Usuário	DSS05.04
DS5.5 Teste de Segurança, Vigilância e Monitoramento	DSS05.07
DS5.6 Definição de Incidente de Segurança	DSS02.01
DS5.7 Proteção da Tecnologia de Segurança	DSS05.05
DS5.8 Gestão de Chave Criptográfica	DSS05.03
DS5.9 Prevenção, Detecção e Correção de Software Malicioso	DSS05.01
DS5.10 Segurança de Rede	DSS05.02
DS5.11 Comunicação de Dados Confidenciais	DSS05.02
DS6.1 Definição de Serviços	APO06.04
DS6.2 Contabilidade de TI	APO06.01
DS6.3 Modelagem de Custo e Cobrança	APO06.04
DS6.4 Manutenção do Modelo de Custo	APO06.04
DS7.1 Identificação das Necessidades de Ensino e Treinamento	APO07.03
DS7.2 Entrega de Treinamento e Ensino	APO07.03
DS7.3 Avaliação do Treinamento Recebido	APO07.03
DS8.1 Central de Serviço	Removido — O ITIL 3 não trata central de serviço como processo.
DS8.2 Registro dos Chamados dos Clientes	DSS02.01-03
DS8.3 Escalonamento de Incidentes	DSS02.04
DS8.4 Encerramento de Incidente	DSS02.05-06
DS8.5 Relatórios e Análises de Tendências	DSS02.07
DS9.1 Repositório de Configuração e Perfil Básicos	BAI10.01-02; BAI10.04; DSS02.01

DS9.1	Repositório de Configuração e Requisitos Básicos	BAI10.01-02; BAI10.04; DSS02.02
DS9.2	Identificação e Manutenção dos Itens de Configuração	BAI10.03
DS9.3	Revisão da Integridade de Configuração	BAI10.04-05; DSS02.05
DS10.1	Identificar e Classificar os Problemas	DSS03.01
DS10.2	Rastreamento e Resolução de Problemas	DSS03.02
DS10.3	Encerramento do Problema	DSS03.03-04

**APÊNDICE A**  
**MAPEAMENTO DO COBIT5 E MODELOS LEGADOS DA ISACA**

**Figura 14 – Objetivos de Controle do COBIT 4.1 Mapeados para COBIT 5**

Objetivo de Controle COBIT 4.1	Coberto no COBIT 5 por:
DS10.4 Integração de Gerenciamento de Mudanças, Configuração e Problemas	DSS03.05
DS11.1 Requisitos de Negócio para o Gerenciamento de Dados	DSS01.01
DS11.2 Arranjos de Armazenamento e Retenção	DSS04.08; DSS06.04
DS11.3 Sistema de Gerenciamento de Biblioteca de Mídia	DSS04.08
DS11.4 Descarte de Dados e Equipamentos	DSS05.06; DSS06.05-06
DS11.5 Backup e Restauração	DSS04.08
DS11.6 Requisitos de Segurança para o Gerenciamento de Dados	DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
DS12.1 Seleção do Local e Layout	DSS01.04-05; DSS05.05
DS12.2 Medidas de Segurança Física	DSS05.05
DS12.3 Acesso Físico	DSS05.05
DS12.4 Proteção contra Fatores Ambientais	DSS01.04
DS12.5 Gerenciamento de Instalações Físicas	DSS01.05
DS13.1 Procedimentos e Instruções de Operações	DSS01.01
DS13.2 Agendamento de Jobs	DSS01.01
DS13.3 Monitoramento da Infraestrutura de TI	DSS01.03
DS13.4 Documentos Confidenciais e Dispositivos de Saída	DSS05.06
DS13.5 Manutenção Preventiva de Hardware	BAI09.02
ME1.1 Abordagem de Monitoramento	MEA01.01
ME1.2 Definição e Coleta dos Dados de Monitoramento	MEA01.02-03
ME1.3 Método de Monitoramento	MEA01.03
ME1.4 Avaliação de Desempenho	MEA01.04
ME1.5 Relatórios para a Alta Direção	MEA01.04
ME1.6 Ações Corretivas	MEA01.05
ME2.1 Monitoramento da Estrutura de Controles Internos	MEA02.01-02
ME2.2 Revisão Gerencial	MEA02.01
ME2.3 Exceções aos Controles	MEA02.04
ME2.4 Autoavaliação dos Controles	MEA02.03
ME2.5 Garantia dos Controles Internos	MEA02.06-08
ME2.6 Controles Internos Aplicados a Terceiros	MEA02.01
ME2.7 Ações Corretivas	MEA02.04
ME3.1 Identificação dos Requisitos de Conformidade com Leis, Regularizações e Contratos Externos	MEA03.01
ME3.2 Otimização da Resposta aos Requisitos Externos	MEA03.02
ME3.3 Avaliação da Conformidade com Requisitos Externos	MEA03.03
ME3.4 Assegurar a Conformidade	MEA03.04
ME3.5 Informes Integrados	MEA03.04
ME4.1 Estabelecimento de uma Estrutura de Governança de TI	EDM01
ME4.2 Alinhamento Estratégico	Removido—No COBIT 5, alinhamento é considerado resultado de todas as atividades de governança e gestão
ME4.3 Entrega de Valor	EDM02
ME4.4 Gerenciamento de Recursos	EDM04
ME4.5 Gestão de Riscos	EDM03
ME4.6 Medição de Desempenho	EDM01.03; EDM02.03; EDM03.03; EDM04.03
ME4.7 Avaliação Independente	MEA02.05-07; MEA02-08

Figura 15 – Práticas Chave do Val IT 2.0 Cobertas pelo COBIT 5

Práticas Chave do Val IT 2.0		Cobertas no COBIT 5 por:
VG1.1	Desenvolva um entendimento do significado de TI e o papel de governança.	EDM01.01
VG1.2	Estabeleça linhas de reporte eficazes.	EDM01.01

# COBIT® 5 : HABILITANDO PROCESSOS

Figura 15 – Práticas Chave do Val IT 2.0 Cobertas pelo COBIT 5

Práticas Chave do Val IT 2.0		Cobertas no COBIT 5 por:
VG1.3	Estabeleça um fórum de liderança.	EDM01.02; APO01.01
VG1.4	Defina valor para a empresa.	EDM02.02
VG1.5	Garanta alinhamento e integração das estratégias de TI e Negócio com os objetivos chave de negócios.	APO02.01
VG2.1	Defina o valor da estrutura de governança.	EDM01.02
VG2.2	Avalie a qualidade e cobertura dos processos atuais.	APO01.07
VG2.3	Identifique e priorize os requerimentos dos processos.	APO01.07
VG2.4	Defina e documente os processos.	APO01.07
VG2.5	Estabeleça, implemente e comunique papéis, responsabilidades e responsabilizações.	APO01.02
VG2.6	Estabeleça estruturas organizacionais.	EDM01.02; APO01.02
VG3.1	Defina tipos de portfólios.	EDM02.02
VG3.2	Defina categorias (dentro dos portfólios).	EDM02.02
VG3.3	Desenvolva e comunique critérios de avaliação (para cada categoria).	EDM02.02
VG3.4	Atribua pesos aos critérios.	EDM02.02
VG3.5	Defina requerimentos para revisões do tipo Stage-gates e outras (para cada categoria).	EDM02.02
VG4.1	Revise as práticas orçamentárias da empresa.	APO06.03
VG4.2	Determine a gestão de valor nos requerimentos de planejamento financeiro.	APO06.01
VG4.3	Identifique alterações necessárias.	APO06.01
VG4.4	Implemente práticas otimizadas de planejamento orçamentário para gestão de valor.	APO06.01
VG5.1	Identifique métricas chave.	EDM02.03
VG5.2	Defina processos e abordagens para captura de informações.	EDM02.03
VG5.3	Defina métodos e técnicas de reporte.	EDM02.03
VG5.4	Identifique e monitore performance nas ações de melhoria.	EDM02.03
VG6.1	Implemente lições aprendidas.	EDM02.03
PM1.1	Revise e garanta clareza das estratégias e objetivos de negócio.	APO05.01
PM1.2	Identifique oportunidades para TI influenciar e suportar a estratégia de negócio.	APO05.01
PM1.3	Defina um mix apropriado de investimento.	APO05.01
PM1.4	Traduza a estratégia e objetivos de negócio na estratégia e objetivos de TI.	APO05.01
PM2.1	Determine os fundos globais de investimento	APO05.02
PM3.1	Crie e mantenha um inventário de recursos humanos de negócio.	APO07.01
PM3.2	Compreenda as demandas atuais e futuras (para recursos humanos de negócio).	APO07.01
PM3.2	Identifique déficits (entre as demandas atuais e futuras de recursos humanos de negócio).	APO07.01
PM3.4	Crie e mantenha planos táticos (para recursos humanos de negócio).	APO07.01
PM3.5	Monitore, revise e ajuste (atribuição de função de negócio e pessoal).	APO07.05
PM3.6	Crie e mantenha um inventário de recursos humanos de TI.	APO07.05
PM3.7	Entenda a demanda atual e futura (para recursos humanos de TI).	APO07.05

PM3.8	Identifique déficits (entre a demanda atual e a futura para recursos humanos de TI).	APO07.05
PM3.9	Crie e mantenha planos táticos (para recursos humanos de TI).	APO07.05
PM3.10	Monitore, revise e ajuste (Atribuição de funções de TI e pessoal).	APO07.05
PM4.1	Avalie e atribua pontuações relativas para programar casos de negócio.	APO05.03

APÊNDICE A  
MAPEAMENTO DO COBIT5 E MODELOS LEGADOS DA ISACA

**Figura 15 – Práticas Chave do Val IT 2.0 Cobertas pelo COBIT 5**

Práticas Chave do Val IT 2.0		Cobertas no COBIT 5 por:
PM4.2	Crie uma visão global do portfólio de investimentos.	APO05.03
PM4.3	Faça e comunique decisões de investimentos.	APO05.03
PM4.4	Especifique revisões do tipo stage-gates e alocar fundos para programas selecionados.	APO05.03
PM4.5	Ajuste objetivos, previsões e orçamentos de negócios.	APO05.03
PM5.1	Monitore e reporte performance do portfólio de investimentos.	APO05.04
PM6.1	Otimize a performance do portfólio de investimento.	APO05.04
PM6.2	Redefina as prioridades do portfólio de investimento.	APO05.04
IM1.1	Reconheça oportunidades de investimento.	APO05.03
IM1.2	Desenvolva o conceito inicial do programa para o caso de negócio.	BAI01.02
IM1.3	Avalie o conceito inicial do programa para o caso de negócio.	APO05.03
IM2.1	Desenvolva um entendimento completo e claro do programa candidato.	BAI01.02
IM2.2	Realize análise de alternativas.	BAI01.02
IM3.1	Desenvolva o plano do programa.	BAI01.04
IM4.1	Faça uma identificação completa do ciclo de vida de custos e benefícios.	BAI01.04
IM4.2	Desenvolva um plano de realização de benefícios.	BAI01.04
IM4.3	Realize uma revisão apropriada e obtenha aprovações	BAI01.03-04
IM5.1	Desenvolva um programa detalhado de caso de negócio.	BAI01.02
IM5.2	Atribua responsabilização e propriedade claras.	BAI01.02
IM5.3	Realize revisões apropriadas e obtenha aprovações.	BAI01.02-03
IM6.1	Planeje projetos e recursos e inicie o programa.	BAI01.05
IM6.2	Gerencie o programa.	BAI01.05
IM6.3	Monitore e gerencie benefícios.	BAI01.05
IM7.1	Atualize os portfólios operacionais de TI.	APO05.05
IM8.1	Atualize o caso de negócio.	BAI01.04
IM9.1	Monitore e reporte a performance do programa (fornecimento de soluções).	BAI01.06
IM9.2	Monitore e reporte a performance para negócios (benefício(resultado)).	BAI01.06
IM9.3	Monitore e reporte a performance operacional (entrega de serviços).	BAI01.06
IM10.1	Aposente o programa.	BAI10.14

**Figura 16 – Práticas Chave do Risk IT Cobertas pelo COBIT 5**

Prática Chave do Risk IT		Coberto no COBIT 5 por:
RG1.1	Realize uma avaliação de riscos de TI da empresa.	EDM03.01; APO12.02-03
RG1.2	Proponha limites de tolerância para riscos de TI.	EDM03.01
RG1.3	Aprove a tolerância ao risco de TI.	EDM03.01-02
RG1.4	Alinhe a política de risco de TI.	EDM03.01-02
RG1.5	Promova uma cultura de consciência de risco.	EDM03.02
RG1.6	Encoraje uma comunicação eficaz de riscos de TI.	EDM03.03
RG2.1	Estabeleça e mantenha responsabilização pelo gerenciamento de risco de TI.	EDM03.02
RG2.2	Coordene a estratégia de risco de TI e a estratégia de risco de negócio.	EDM03.01-02

# COBIT<sup>®</sup> 5 : HABILITANDO PROCESSOS

Figura 16 – Práticas Chave do Risk IT Cobertas pelo COBIT 5

Prática Chave do Risk IT	Coberto no COBIT 5 por:
análise de riscos de TI.	
RG3.2 Aprove a análise de risco de TI.	EDM03.01
RG3.3 Incorpore as considerações de risco de TI nas tomadas de decisão estratégica de negócio.	EDM03.01
RG3.4 Aceite o risco de TI.	EDM03.01
RG3.5 Priorize as atividades de resposta a risco de TI	EDM03.02
RE1.1 Estabeleça e mantenha um modelo para coleta de dados.	APO12.01
RE1.2 Colete dados do ambiente operacional.	APO12.01
RE1.3 Colete dados dos eventos de risco.	APO12.01
RE1.4 Identifique fatores de risco.	APO12.01
RE2.1 Defina o escopo da análise de riscos de TI.	APO12.02
RE2.2 Calcule o risco de TI.	APO12.02
RE2.3 Identifique opções de resposta ao risco.	APO12.02
RE2.4 Realize uma revisão por pares da análise de riscos de TI.	APO12.02
RE3.1 Mapeie recursos de TI a processos de negócios.	APO12.02
RE3.2 Determine a criticidade para negócios dos recursos de TI.	APO12.03
RE3.3 Entenda as capacidades de TI.	APO12.03
RE3.4 Atualize os componentes do cenário de risco de TI.	APO12.03
RE3.5 Mantenha o registro e o mapa de risco de TI.	APO12.03
RE3.6 Desenvolva indicadores para risco de TI.	APO12.03
RR1.1 Comunique os resultados da análise de risco de TI.	APO12.04
RR1.2 Reporte as atividades de gerenciamento de risco de TI e o estado da conformidade.	APO12.04
RR1.3 Interprete os resultados da avaliação independente de TI.	APO12.04
RR1.4 Identifique oportunidades de TI.	APO12.04
RR2.1 Faça o inventário controles.	APO12.05
RR2.2 Monitore o alinhamento operacional com os limites de tolerância ao risco.	APO12.05
RR2.3 Responda a descoberta de exposição a risco e oportunidades.	APO12.05
RR2.4 Implemente controles.	APO12.05
RR2.5 Reporte o progresso do plano de ação para risco de TI.	APO12.05
RR3.1 Mantenha planos de resposta a incidentes.	APO12.06
RR3.2 Monitore riscos de TI.	APO12.06
RR3.3 Inicie resposta a incidente.	APO12.06
RR3.4 Comunique lições aprendidas de eventos de risco.	APO12.06

## APÊNDICE B

### MAPEAMENTO DETALHADO DOS OBJETIVOS CORPORATIVOS – OBJETIVOS DE TI

#### APÊNDICE B

#### MAPEAMENTO DETALHADO DOS OBJETIVOS CORPORATIVOS – OBJETIVOS DE TI

The COBIT 5 goals cascade is explained in chapter 02 Figure 17 contains:

A cascata de objetivos do COBIT 5 é explicada no capítulo 02 A figura 17 contém:

Nas colunas, todos os 17 objetivos corporativos genéricos definidos no COBIT 5, agrupados pela dimensão BSC

Nas linhas, todos os 17 objetivos de TI, também agrupados pela dimensão BSC de TI

Um mapeamento de como cada objetivo corporativo é apoiado pelos objetivos de TI. Esse mapeamento é expresso utilizando a seguinte escala:

- ‘P’ significa primário, quanto há um relacionamento importante, quando o objetivo de TI representar um apoio fundamental para o objetivo corporativo.
- ‘S’ significa secundário, quando houver uma relação importante, mas menos importante, ou seja, quando o objetivo de TI representar um apoio secundário para o objetivo corporativo.

A tabela foi criada com base nos seguintes itens:

Pesquisas da University of Antwerp Management School IT Alignment e do Governance Research Institute

Revisões adicionais e opiniões de especialistas obtidas durante o desenvolvimento e revisão do COBIT 5

Ao utilizar a tabela da figura 17, por favor, considere as observações feitas no capítulo 2 sobre como utilizar a cascata de objetivos do COBIT 5.

**Figura 17 – Mapeamento dos Objetivos Corporativos do COBIT 5 com os Objetivos de TI**

		Objetivos Corporativos do COBIT 5															
		Objetivos Corporativos do COBIT 5															
Financeira	Objetivos de TI	Financeira				Cliente				Interna				T & c			
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
	01 Alinhamento da estratégia de negócios e de TI	P	P	S			P	S	P	P	S	P	S	P		S	S
	02 Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos			S	P										P		
	03 Compromisso da gerência executiva com a tomada de decisões de TI	P	S	S						S	S	S		P		S	S

					P	S		P	S	P		S	S	S
	04	Gestão de risco organizacional de TI												
	05	Benefícios obtidos pelo investimento de TI e portfólio de serviços	P	P			S	S	S	S	P	S		S
	06	Transparência dos custos, benefícios e riscos de TI	S	S	P			S	P	P				
	07	Prestação de serviços de TI em consonância com os requisitos de negócio	P	P	S	S	P	S	P	S	P	S	S	S
Fin														
Client														

# COBIT® 5 : HABILITANDO PROCESSOS

Figura 17 – Mapeamento dos Objetivos Corporativos do COBIT 5 com os Objetivos de TI

		Objetivos Corporativos do COBIT 5																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		Objetivos de TI		Financeira				Cliente				Interna				T & c		
	08	Uso adequado de aplicativos, informações e soluções tecnológicas	S	S	S			S	S	S	P	S	P		S	S		
	09	Agilidade de TI	S	P	S			S	P		P	S	S	S	S	P		
	10	Segurança da informação, infraestrutura de processamento e aplicativos			P	P		P							P			
	11	Otimização de ativos, recursos e capacidades de TI	P	S				S		P	S	P	S	S		S		
	12	Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia	S	P	S			S	S	S	P	S	S	S		S		
	13	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos	P	S	S			S		S	S	S	P					
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão	S	S	S	S		P	P	S								
	15	Conformidade de TI com as políticas internas			S	S									P			
Interna	16	Equipes de TI e de negócios motivadas e qualificadas	S	S	P			S	S				P	P	S			
T & C	17	Conhecimento, expertise e iniciativas para inovação dos negócios	S	P				S	P	S	S	S	S		S	P		

T &amp; C=Treinamento e Conhecimento

## APÊNDICE C MAPEAMENTO DETALHADO DOS OBJETIVOS DE TI – PROCESSOS DE TI

### APÊNDICE C MAPEAMENTO DETALHADO DOS OBJETIVOS DE TI – PROCESSOS DE TI

A figura 18 contém:

Nas colunas, todos os 17 objetivos de TI genéricos definidos no capítulo 2, agrupados nas dimensões do BSC de TI

Nas linhas, todos os 37 processos do COBIT 5, agrupados por domínio

Um mapeamento de como cada objetivo de TI é apoiado por um processo de TI do COBIT 05. Este mapeamento é expresso usando a seguinte escala:

- ‘P’ significa primário, quando houver uma relação direta importante, ou seja, quando o processo do COBIT 5 for um apoio fundamental para a consecução de um objetivo de TI.
- ‘S’ significa secundário, quando houver uma relação ainda forte, mas menos importante, ou seja, quando o processo do COBIT 5 for um apoio secundário para o objetivo de TI.

A tabela foi criada com base nas seguintes informações:

Pesquisas da University of Antwerp Management School IT Management e do Governance Research Institute. Revisões adicionais e opiniões de especialistas obtidos durante o processo de desenvolvimento e revisão do COBIT 5

Ao usar a tabela contida na figura 18, considerar as observações feitas no capítulo 2 sobre como usar a cascata de objetivos do COBIT 5.

**Figura 18 – Mapeamento dos Objetivos de TI do COBIT 5 com os Processos**

		Objetivo de TI																							
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17							
		Processos COBITS							Financeira							Cliente			Interna					T & C	
Dirigir e Monitorar	EDM01	Garantir a Definição e Manutenção do Modelo de Governança	P	S	P	S	S	S	P	S	S	S	S	S	S	S	S	S	S	S	S				
	EDM02	Garantir a Realização de Benefícios		P		S		P	P				S	S	S	S		S	S	P					

Avaliar, Dir.	<b>EDM03</b>	Garantir a Otimização do Risco	S	S	S	P		P	S	S		P		S	S	P	S	S
	<b>EDM04</b>	Garantir a Otimização de Recursos	S		S	S	S	S	S	S	S	P	P	S		P	S	

# COBIT® 5 : HABILITANDO PROCESSOS [MEA]

Figura 18 – Mapeamento dos Objetivos de TI do COBIT 5 com os Processos

		Objetivo de TI																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processos COBIT5		Financeira					Cliente			Interna					T & C			
	<b>EDM05</b>	Garantir a Transparência às Partes Interessadas	S	S	P			P	P					S	S	S		S
Alinhar, Planejar e Organizar	<b>APO01</b>	Gerenciar a estrutura de gestão de TI.	P	P	S	S		S		P	S	P	S	S	S	P	P	P
	<b>APO02</b>	Gerenciar a estratégia	P		S	S	S	P	S	S	S	S	S	S	S	S	S	P
	<b>APO03</b>	Gerenciar arquitetura da organização	P		S	S	S	S	S	S	P	S	P	S	S			S
	<b>APO04</b>	Gerenciar inovação	S		S	P		P	P		P	S		S				P
	<b>APO05</b>	Gerenciar portfolio	P		S	S	P	S	S	S	S	S	P					S
	<b>APO06</b>	Gerenciar orçamento e custos	S		S	S	P	P	S	S	S	S	S	S	S			
	<b>APO07</b>	Gerenciar recursos humanos	P	S	S	S		S		S	S	P		P		S	P	P
	<b>APO08</b>	Gerenciar relacionamentos	P		S	S	S	S	P	S		S	P	S	S	S	S	P
	<b>APO09</b>	Gerenciar contratos de prestação de serviços	S		S	S	S	P	S	S	S	S	S	S	S	P	S	
	<b>APO10</b>	Gerenciar fornecedores		S	P	S	S	P	S	P	S	S	S	S	S	S	S	S
	<b>APO11</b>	Gerenciar qualidade	S	S	S	P		P	S	S	S	S	S	P	S	S	S	S
	<b>APO12</b>	Gerenciar riscos	P		P	P	P	S	S	S	P			P	S	S	S	S

	APO12	Gerenciar riscos	P	P	P	S	S	S	P	P	S	S	S	S
	APO13	Gerenciar segurança	P	P	P	S	S	S	P	P	S	S	S	S
Construi	BAI01	Gerenciar programas e projetos	P	S	P	P	S	S	S		S	P	S	S

APÊNDICE C  
MAPEAMENTO DETALHADO DOS OBJETIVOS DE TI – PROCESSOS DE TI

Figura 18 – Mapeamento dos Objetivos de TI do COBIT 5 com os Processos

		Objetivo de TI																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processos COBITS		Financeira						Cliente			Interna						T & C	
	BAI02	Gerenciar definição de requisitos	P	S	S	S	S		P	S	S	S	P	S	S		S	
	BAI03	Gerenciar identificação e desenvolvimento de soluções	S			S	S		P	S		S	S	S	S		S	
	BAI04	Gerenciar disponibilidade e capacidade				S	S		P	S	S	P		S	P		S	
	BAI05	Gerenciar capacidade da mudança organizacional	S		S		S		S	P	S	S	S	P			P	
	BAI06	Gerenciar mudanças			S	P	S		P	S	S	P	S	S	S	S	S	
	BAI07	Gerenciar aceitação e transição da mudança				S	S		S	P	S		P	S	S	S	S	
	BAI08	Gerenciar conhecimento	S				S		S	S	P	S	S		S	S	P	
	BAI09	Gerenciar ativos	S		S		P	S		S	S	P		S	S			
	BAI10	Gerenciar configuração	P		S		S		S	S	S	P		P	S			
e Suporte	DSS01	Gerenciar Operações		S		P	S		P	S	S	S	P		S	S	S	
	DSS02	Gerenciar Solicitações e Incidentes de Serviços			P			P	S		S			S	S	S	S	
	DSS03	Gerenciar Problemas		S		P	S		P	S	S		P	S	P	S	S	

Entregar, Serviço	DSS04	Gerenciar Continuidade		S	S	P	S	P	S	S	S	S	P	S	S	S
		S	P	P		S	S	P	S	S	S	S	S	S	S	
DSS05	Gerenciar Serviços de Segurança		S	P	P		S	S	P	S	S	S	S	S	S	

# COBIT® 5 : HABILITANDO PROCESSOS [MEA]

Figura 18 – Mapeamento dos Objetivos de TI do COBIT 5 com os Processos

Processos COBIT5		Objetivo de TI																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	DSS06	Gerenciar Controles de Processos de Negócio		S		P		P	S	S	S	S	S	S	S	S	S	S
M Monitorar, Avaliar e Analisar	MEA01	Monitorar, avaliar e analisar o desempenho e conformidade	S	S	S	P	S	S	P	S	S	P	S	S	P	S	S	S
	MEA02	Monitorar, avaliar e analisar o sistema de controle interno	P		P		S	S	S		S			S	P	S		S
	MEA03	Monitorar, avaliar e analisar a conformidade com os requisitos externos	P		P	S		S		S				S	S			S