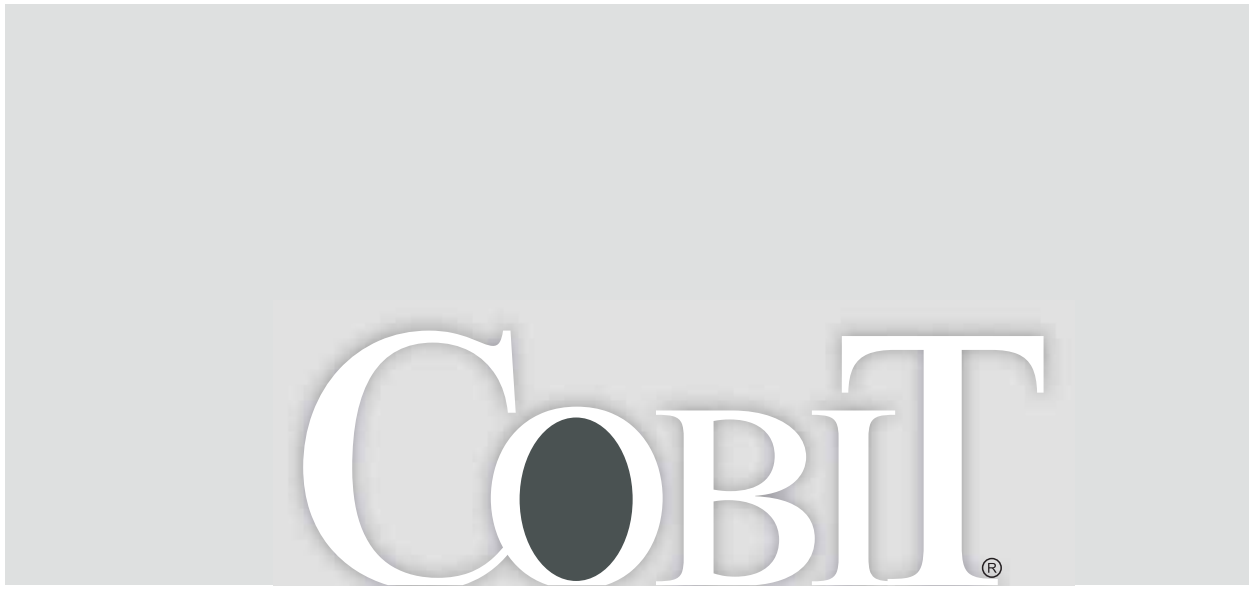


COBIT®

4.1

Modelo

Objetivos de Controle

Diretrizes de Gerenciamento

Modelos de Maturidade

IT Governance Institute™
O IT Governance Institute (ITGI™) (www.itgi.org) foi estabelecido em 1998 para melhoria do pensamento e dos padrões internacionais de direção e controle da tecnologia da informação nas organizações. Uma governança de TI efetiva ajuda a garantir que a TI suporte os objetivos de negócios, otimiza os investimentos em TI e apropriadamente os riscos e as oportunidades relacionados a TI. O ITGI™ oferece pesquisa original, recursos eletrônicos e estudos de caso para auxiliar os líderes de organizações e o conselho de diretores nas suas responsabilidades de governança de TI.

Declaração de responsabilidade pelo uso (disclaimer)
O ITGI™ (o "Proprietário") elaborou e criou esta publicação, intitulada CobiT® 4.1 (o "Trabalho"), primordialmente como um recurso educacional para chief information officers (CIOs), gerência sênior, gerência de TI e profissionais de controle. Os Proprietários não afirmam que qualquer uso do Trabalho irá garantir um resultado de sucesso. O Trabalho não deve ser considerado inclusivo de qualquer informação, procedimentos e teste próprios ou exclusivo de outras informações, procedimentos ou testes que sejam razoavelmente direcionados a obtenção dos mesmos resultados. Ao determinar a propriedade de qualquer informação específica, procedimento ou teste, os CIOs, gerência sênior, gerência de TI e profissionais de controle devem aplicar o seu próprio julgamento profissional às circunstâncias específicas apresentadas por um sistema ou ambiente de TI em particular.

Direitos de Uso

IT Governance Institute™
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

Agradecimentos

O IT Governance Institute gostaria de agradecer a:

Desenvolvedores Especialistas e Revisores

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Ed Chavennes, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche LLP, South Africa
Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA
Philip Le Grand, Capita Education Services, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA

Agradecimentos (Continuação)

Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., South Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Denmark
Jaco Sadie, Sasol, South Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgium
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

Comitê de Direção ITGI
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Trustee

Comitê de Governança de TI
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Rómulo Lomparte, CISA, Banco de Crédito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

Agradecimentos aos profissionais que participaram de forma voluntária do grupo de tradução e revisão do Projeto CobiT-BR
O grupo foi formado por profissionais das áreas de Auditoria, Segurança da Informação e Governança em TI, e é representativo de diversos segmentos, indústria, bancos, seguradoras, serviços, firmas de consultoria e órgãos de Governo.

Participantes

Adriana da Silva Dian Leão, São Paulo
Alberto Bastos, CISSP, Rio de Janeiro
Alberto Fávero, CISSP, CISA, CISM, São Paulo
Alfred John Bacon, CISA CISM, Rio de Janeiro
André Amado, São Paulo
André Pitkowski, CGEIT, OCTAVE, São Paulo
Antonio de Sousa, São Paulo
César Augusto Monteiro, São Paulo
Cristiano Kruel, CISA, CGEIT, Rio Grande do Sul
David De Paulo Pereira, Brasília/DF
Edgar D'Andrea, CISA, CISM, CGEIT, São Paulo
Gianni Ricciardi, São Paulo
Gilmar Souza Santos, CISA, CGEIT, CSQE, São Paulo
Jeferson D'Addario, CBCP, MBCI, São Paulo
João Antônio Ribeiro Ferreira, Coronel PM, São Paulo
Laurence Liu, CGEIT, São Paulo
Luiz Felix Prado, CISA, CIA, CFSA, São Paulo
Luiz Gustavo Ferracini de Oliveira, CISA, CISM, São Paulo
Marcelo Silva, CISA, São Paulo
Marcos Aurélio Rodrigues, Sargento PM, São Paulo
Margarete Furuta, CISA, CISM, São Paulo
Marina Solano, Brasília/DF
Mauro José Souza, CISA, São Paulo
Napoleão Verardi Galegale, CGEIT, São Paulo
Paulo Henrique Passos Ximendes, Brasília/DF
Ricardo Guedes G. da Silveira, CISM, CISA, São Paulo
Ricardo Pires Monteiro Martins, CISA, CIA, São Paulo
Roberval Ferreira França, Tenente Coronel PM, São Paulo
Rodrigo Hiroshi Ruiz Suzuki, CISA, São Paulo
Silvana Laragnoit Ribas, CISA, São Paulo

Coordenação

Marcelo F. Melro, CISA, CISM, CISSP, São Paulo
Carmen O. Fernandes, CISA, CIA, São Paulo
Ricardo Castro, CISA, MCSO, CFE, São Paulo

O projeto CobiT-BR foi resultado de um esforço conjunto dos associados e líderes dos Capítulos ISACA no Brasil, sob a Coordenação da Diretoria do Capítulo São Paulo.

ISACA Capítulo São Paulo/SP

Diretoria Executiva em 2008 – 2009

Marcelo Fernandes Melro, CISA, CISM, CISSP, Presidente
Ricardo Mathias de Castro, CISA, MCSO, CFE, Vice-Presidente
Edméa Pujol Cantón, Diretora Secretária
Carmen Ozores Fernandes, CISA, CIA, Diretora de Educação
Ivo Luiz Cairrão, Diretor de Controladoria e Administração
André Pitkowski, CGEIT, OCTAVE, Diretor de Associados
José Luís Diniz, CGEIT, Diretor de Parcerias
Fernando Nicolau F. Ferreira, CISM, CGEIT, CFE, CITP, Diretor de Comunicação
Valmir Schreiber, CISM, Past President

ISACA Capítulo Rio de Janeiro/RJ

Diretoria Executiva em 2009

Alfred John Bacon, CISA, CISM, CISSP, Presidente
Marcos Sêmola, CISM, Vice-Presidente
Leandro Ribeiro, Diretor Secretário
Ernani Paes de Barros, CISA, CISM, CGEIT,Diretor de Educação
Marcelo Duarte, CISA, CGEIT, Diretor de Controladoria e Administração
Dr Paulo Pagliusi, PhD, Diretor de Comunicação e Relações Institucionais

ISACA Capítulo Brasília/DF

Diretoria Executiva em 2009

Ian Lawrence Webster, Presidente
Dr. João Souza Neto, Vice-Presidente
Andre Luiz Furtado Pacheco, Diretor Secretário
Paulo Henrique Passos Ximendes, Diretor de Associados
Leandro Pfeifer Macedo, Diretor de Comunicação e Marketing
Carlos Renato Araujo Braga, Diretor de Educação
José Geraldo Loureiro Rodrigues, Diretor Tesoureiro
Dr. Rildo Ribeiro dos Santos, Diretor Institucional
Roberta Ribeiro De Queiroz Martins, Presidente do Conselho Fiscal
Cláudio Silva da Cruz, Membro do Conselho Fiscal
Daniel Moreira Guilhon, Membro do Conselho Fiscal

Tabela de Conteúdo

Seu feedback sobre o CobiT 4.1 é bem-vindo. Por favor, acesse o site *www.isaca.org/cobitfeedback* para enviar seus comentários.

Sumário Executivo

Sumário Executivo

Para muitas organizações a informação e a tecnologia que a suporta representam o seu bem mais valioso, mas muitas vezes é o menos compreendido. Organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação e a utiliza para direcionar os valores das partes interessadas no negócio. Essas organizações também entendem e gerenciam os riscos associados, tais como as crescentes demandas regulatórias e a dependência crítica de muitos processos de negócios da TI.

A necessidade da avaliação do valor de TI, o gerenciamento dos riscos relacionados à TI e as crescentes necessidades de controle sobre as informações são agora entendidos como elementos-chave da governança corporativa. Valor, risco e controle constituem a essência da governança de TI.

A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização.

Além disso, a governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócios. A governança de TI habilita a organização a obter todas as vantagens de sua informação, maximizando os benefícios, capitalizando as oportunidades e ganhando em poder competitivo. Esses resultados requerem um modelo para controle de TI que se adeque e dê suporte ao COSO *("Committe of Sponsoring Organisations of the Treadway Commission's Internal Control – Integrated Framework")*, um modelo para controles internos amplamente aceito para governança e gerenciamento de riscos empresariais, e outros modelos similares.

As organizações devem satisfazer os requisitos de qualidade, guarda e segurança de suas informações, bem como de todos seus bens. Os executivos devem também otimizar o uso dos recursos de TI disponíveis, incluindo os aplicativos, informações, infra-estrutura e pessoas. Para cumprir essas responsabilidades bem como atingir seus objetivos, os executivos devem entender o estágio atual de sua arquitetura de TI e decidir que governança e controles ela deve prover.

O *Control Objectives for Information and related Technology* (CobiT®) fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas práticas do CobiT representam o consenso de especialistas. Elas são fortemente focadas mais nos controles e menos na execução. Essas práticas irão ajudar a otimizar os investimentos em TI, assegurar a entrega dos serviços e prover métricas para julgar quando as coisas saem erradas.

Para a área de TI ter sucesso em entregar os serviços requeridos pelo negócio, os executivos devem implementar um sistema interno de controles ou uma metodologia. O modelo de controle do CobiT contribui para essas necessidades ao:
- Fazer uma ligação com os requisitos de negócios.
- Organizar as atividades de TI em um modelo de processos geralmente aceito.
- Identificar os mais importantes recursos de TI a serem utilizados.
- Definir os objetivos de controle gerenciais a serem considerados.

A orientação aos negócios do CobiT consiste em objetivos de negócios ligados a objetivos de TI, provendo métricas e modelos de maturidade para medir a sua eficácia e identificando as responsabilidades relacionadas dos donos dos processos de negócios e de TI.

O foco em processos do CobiT é ilustrado por um modelo de processos de TI subdivididos em quatro domínios e 34 processos em linha com as áreas responsáveis por planejar, construir, executar e monitorar, provendo assim uma visão total da área de TI. Conceitos de arquitetura corporativa ajudam a identificar os recursos essenciais para o sucesso dos processos, ou seja, aplicativos, informações, infraestrutura e pessoas.

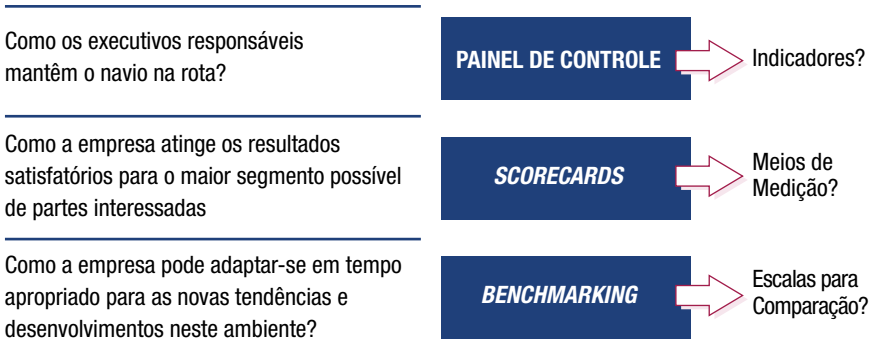
Em resumo, para prover as informações de que a empresa necessita para atingir seus objetivos, os recursos de TI precisam ser gerenciados por uma série de processos naturalmente agrupados.

Mas como a empresa consegue implementar controles na área de TI de forma que ela entregue as informações que a empresa precisa? Como ela gerencia os riscos e garante a segurança dos recursos de TI dos quais é tão dependente? Como a empresa assegura que a área de TI atinge os seus objetivos e atende aos negócios?

Primeiramente os executivos precisam de objetivos de controles que definam a meta básica de implementar políticas, planos e procedimentos, bem como a estrutura organizacional designada para prover razoável garantia de que:
- Os objetivos de negócio serão atingidos
- Eventos indesejáveis serão prevenidos ou detectados e corrigidos

Em segundo lugar, no complexo ambiente atual, os executivos estão continuamente procurando informações condensadas e disponíveis que os auxiliem a tomar decisões difíceis relacionadas a valor, risco e controles, de forma rápida e correta. O que deve ser avaliado e como? As organizações precisam de medidas objetivas que mostrem onde elas estão e onde são necessárias melhorias e também precisam implementar instrumentos que monitorem essas melhorias. A **Figura 1** exibe algumas questões comuns e as ferramentas de gerenciamento de informações usadas para encontrar as respostas, mas os painéis de controles *(dashboards)* precisam de indicadores, os *"scorecards"* precisam de meios de medição e o *"benchmarking"*, de uma escala para comparações.

Figura 1 - Gerenciamento de Informações



Uma resposta para esses requisitos de definição e monitoramento dos controles e nível de performance de TI é a definição do CobiT de:
- **Benchmarking** da performance e capacidade dos processos de TI, expressos em modelos de maturidade, derivados do *"Capability Maturity Model (CMM)* do *Software Engineering Institute"*.
- **Objetivos e métricas** dos processos de TI para definir e avaliar os seus resultados e performance baseados nos princípios do balanced business scorecard publicado por Robert Kaplan e David Norton.
- **Objetivos das atividades** para controlar esses processos com base nos objetivos de controle do CobiT.

A avaliação do processo de capacidade baseado nos modelos de maturidade do CobiT é uma parte fundamental da implementação da governança de TI. Depois de identificar os processos e controles críticos de TI, o modelo de maturidade permite a identificação das deficiências em capacidade e a sua demonstração para os executivos. Planos de ação podem ser desenvolvidos para elevar esses processos ao desejado nível de capacidade.

Assim o CobiT suporta a governança de TI **(Figura 2)** provendo uma metodologia para assegurar que:
- A área de TI esteja alinhada com os negócios
- A área de TI habilite o negócio e maximiza os benefícios
- Os recursos de TI sejam usados responsavelmente
- Os riscos de TI sejam gerenciados apropriadamente

A mensuração da performance é essencial para a governança de TI. Isto é suportado pelo CobiT, incluindo a definição e o monitoramento dos objetivos de mensuração sobre os quais os processos de TI precisam entregar (processo de saída) e como entregam (processo de capacidade e performance). Muitas pesquisas identificaram a falta de transparência dos custos, do valor e dos riscos de TI como uma das mais importantes metas para a governança de TI. Embora outras áreas de foco contribuam, a transparência é primariamente atingida através da medição da performance.

Figura 2 - Áreas de Foco na Governança de TI

- Alinhamento estratégico: foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização.
- Entrega de valor: é a execução da proposta de valor de IT através do ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização, concentrado-se em otimizar custos e provendo o valor intrínseco de TI.
- Gestão de recursos: refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem-se à otimização do conhecimento e infraestrutura.
- Gestão de risco: requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia.
- Mensuração de desempenho: acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de performance e entrega dos serviços, usando, por exemplo, *"balanced scorecards"* que traduzem as estratégia em ações para atingir os objetivos, medidos através de processos contábeis convencionais.

Essas áreas de foco em governança de TI descrevem os tópicos que os executivos precisam atentar para direcionar a área de TI dentro de suas organizações. Gerentes operacionais usam os processos para organizar e gerenciar as atividades contínuas de TI. O CobiT provê um modelo de processo genérico que representa todos os processos normalmente encontrados nas funções de TI, fornecendo assim um modelo de referência comum compreendido por gerentes operacionais de TI e gerentes de negócios. O modelo de processos do CobiT foi mapeado com as áreas de governança de TI (veja o apêndice II, Mapeando os Processos de TI com as Áreas Foco de Governança de TI, COSO, Recursos de TI CobiT e Critérios de Informação CobiT), criando uma ponte entre o que os gerentes operacionais precisam executar e o que os executivos desejam controlar.

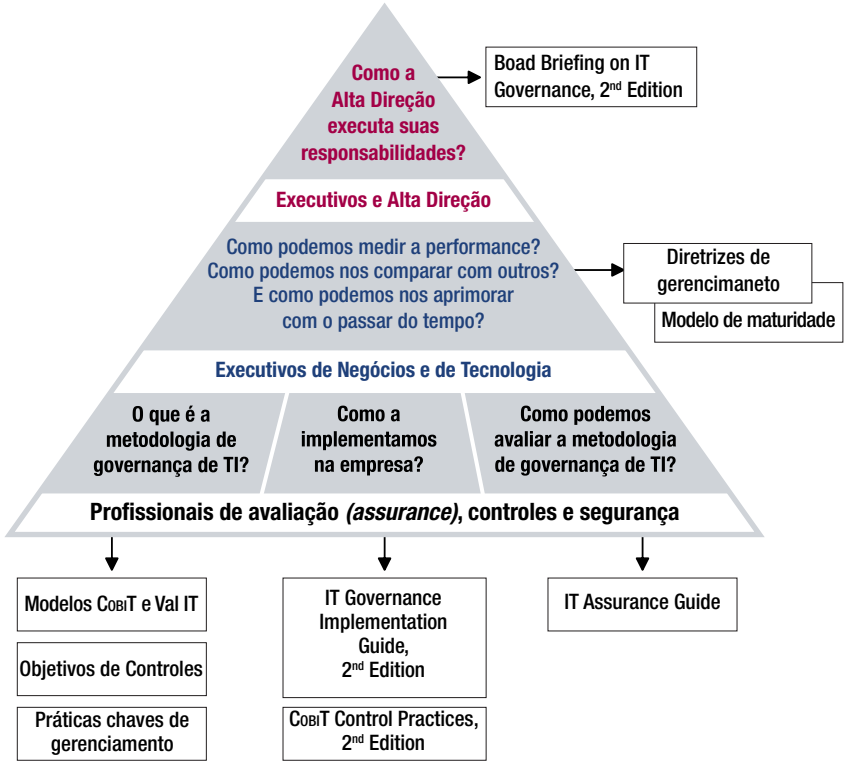
Para atingir um governança efetiva, os executivos requerem que os controles sejam implementados pelos gerentes operacionais com uma metodologia de controles definida para todos os processos de TI. Os objetivos de controle de TI do CobiT são organizados em processos de TI; portanto o modelo proporciona uma clara ligação entre os requerimentos de governança de TI, processos de TI e controles de TI.

O CobiT é focado no que é necessário para atingir um adequado controle e gerenciamento de TI e está posicionado em elevado nível. O CobiT foi alinhado e harmonizado com outros padrões e boas práticas de TI (veja o apêndice IV, CobiT 4.1 Material de Referência Principal) mais detalhados. O CobiT atua como um integrador desses diferentes materiais de orientação, resumindo os principais objetivos sob uma metodologia que também está relacionada aos requisitos de governança e de negócios.

O COSO (e outras metodologias similares) é geralmente aceito como uma metodologia de controle interno para corporações. O CobiT é um modelo de controles internos geralmente aceitos para a área de TI.

Os produtos do CobiT foram organizados em 3 níveis (Figura 3) criados para dar suporte a:
- Executivos e Alta Direção
- Gerentes de TI e de negócios
- Profissionais de avaliação (assurance), controles e segurança

Figura 3 - Diagrama com o Conteúdo do CobiT



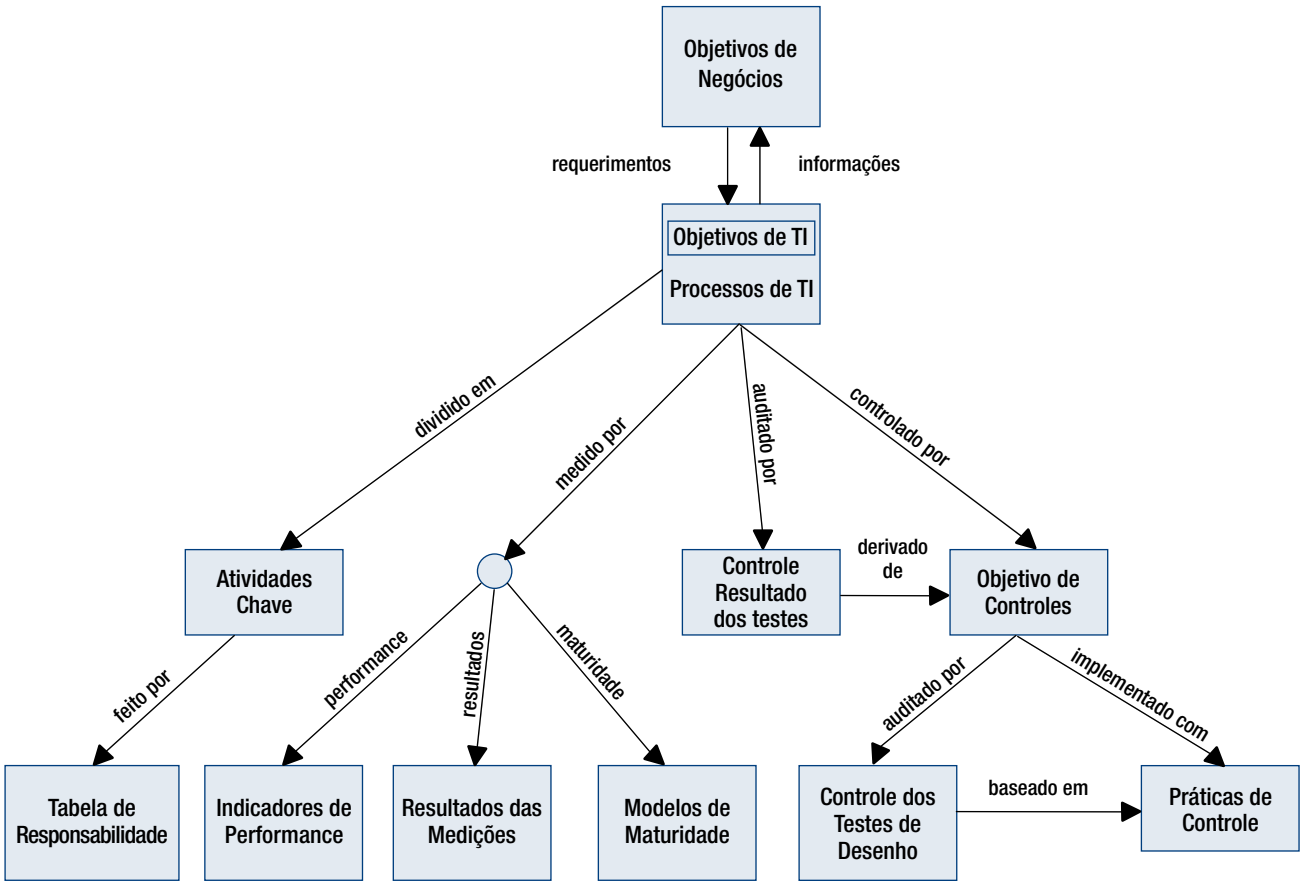
Este diagrama de produtos baseado no CobiT apresenta os produtos geralmente aplicáveis e suas respectivas audiências. Também existem produtos derivados para propósitos específicos *(IT Control Objectives for Sarbanes-Oxley, 2nd Edition)*, para domínios tais como segurança *(CobiT Security Baseline and Information Security Governance: Guidance for Boards of Directors and Executive Management)*, ou para empresas específicas *(CobiT Quickstart* para pequenas e médias empresas ou para grandes empresas desejando atingir a implementação de uma mais extensiva governança de TI).

De forma resumida, os produtos CobiT incluem:
- *Board Briefing on IT Governance, 2nd Edition* – Publicação que auxilia os executivos a entender por que a governança de TI é importante, quais são suas principais questões e o papel deles em gerenciá-la.
- Diretrizes de gerenciamento / modelos de maturidade – auxiliam na designação de responsabilidades, avaliação de desempenho e *benchmark*, e trata da solução de deficiências de capacidade.
- Diretrizes de gerenciamento / modelos de maturidade – auxiliam na designação de responsabilidades, avaliação de desempenho e *benchmark* e trata da solução de deficiências de capacidade
- Métodos: organiza os objetivos da governança de TI por domínios e processos de TI e os relaciona com os requisitos de negócios.
- Objetivos de controle – proporcionam um completo conjunto de requisitos de alto nível a serem considerados pelos executivos para o controle efetivo de cada processo de TI
- *IT Governance Implementation Guide: Using CobiT® and Val IT TM, 2nd Edition* – provê um mapa geral para implementar a governança de TI usando os recursos do obiT e o Val IT
- *CobiT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* – explica porque os controles merecem ser implementados e como implementá-los
- *IT Assurance Guide: Using CobiT®* – traz orientações sobre como o CobiT pode ser usado para suportar as variadas atividades de avaliação junto com sugestões de passos de testes para todos os processos e objetivos de controle de TI.

O diagrama de conteúdo do CobiT descrito na **Figura 3** apresenta o principal público-alvo, suas dúvidas sobre governança de TI e os produtos aplicáveis que podem lhes dar as respostas. Também existem produtos derivados para finalidades específicas, domínios (como segurança) ou organizações específicas.

Todos os componentes do CobiT são inter-relacionados, proporcionando o suporte para as necessidades de governança, gerenciamento, controle e avaliação de diferentes audiências, conforme demonstrado na **figura 4.**

Figura 4 - Inter-relacionamento dos componentes CobiT



O CobiT é um modelo e uma ferramenta de suporte que permite aos gerentes suprir as deficiências com respeito aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas. O CobiT habilita o desenvolvimento de políticas claras e boas práticas para controles de TI em toda a empresa. O CobiT é atualizado continuamente e harmonizado com outros padrões e guias. Assim, o CobiT tornou-se o integrador de boas práticas de TI e a metodologia de governança de TI que ajuda no entendimento e gerenciamento dos riscos e benefícios associados com TI.
A estrutura de processos do CobiT e o seu enfoque de alto nível orientado aos negócios fornece uma visão geral de TI e das decisões a serem tomadas sobre o assunto.

Os benefícios de implementar o CobiT como um modelo de governança de TI incluem:
· Um melhor alinhamento baseado no foco do negócio
· Uma visão clara para os executivos sobre o que TI faz
· Uma clara divisão das responsabilidades baseada na orientação para processos
· Aceitação geral por terceiros e órgãos reguladores
· Entendimento compreendido entre todas as partes interessadas, baseado em uma linguagem comum
· Cumprimento dos requisitos do COSO para controle do ambiente de TI.

O restante deste documento apresenta uma descrição do modelo CobiT e de todos os principais componentes do CobiT, organizados pelos quatro domínios e 34 processos de TI do CobiT. Isto resulta em um prático guia de referência sobre todas as principais orientações do CobiT. Muitos apêndices são também fornecidos como referências úteis.

Informações mais completas e atualizadas sobre o CobiT e os produtos relacionados, incluindo ferramentas *on-line*, guias de implementação, estudos de caso, notícias e material educacional, estão disponíveis no site *www.isaca.org/cobit.*

MODELO COBIT

MODELO COBIT

MISSÃO DO COBIT:
Pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação.

A NECESSIDADE DE UM MODELO DE CONTROLE PARA A GOVERNANÇA DE TI

Um modelo de controle da governança de TI define as razões pelas quais a governança de TI é necessária, quais são as partes interessadas e o que esse modelo precisa atingir.

Por quê

Cada vez mais a Alta Direção está percebendo o significativo impacto que a informação tem no sucesso da organização. Os executivos esperam um alto entendimento sobre a forma como TI funciona e o quanto ela está sendo bem administrada para atingir vantagens competitivas. Em particular, os executivos precisam saber se as informações estão sendo gerenciadas pela empresa de modo a:
- Possivelmente atingir os objetivos
- Ter resiliência suficiente para aprender e se adaptar
- Gerenciar adequadamente os riscos encontrados
- Apropriadamente reconhecer as oportunidades e agir sobre elas

As organizações não podem atingir seus requisitos de negócios e governança sem adotar e implementar um modelo para governança e controle de TI para:
- Fazer uma ligação com os requisitos de negócios
- Tornar transparente a performance obtida comparada a esses requisitos
- Organizar as atividades de acordo com um modelo de processos geralmente aceito
- Identificar os recursos mais importantes a serem aprimorados
- Definir os objetivos de controles gerenciais a serem considerados

Adicionalmente, as metodologias de governança e controle estão tornando-se parte das boas práticas de gerenciamento de TI e são facilitadoras para o estabelecimento de governança de TI e aderência aos cada vez mais crescentes requisitos regulatórios.

As boas práticas de TI tornaram-se significantes devido a inúmeros fatores:
- Executivos de negócio e a Alta Direção demandando um melhor retorno dos investimentos em TI, isto é, que a área de TI entregue as necessidades da área de negócios para aumentar o valor para partes interessadas
- Preocupação com o aumento observado dos gastos com TI
- A necessidade de atender às exigências regulatórias de controles de TI em áreas como privacidade de informações e relatórios financeiros (por exemplo, Lei Sarbanes-Oxley e Basiléia II) e regulamentações para setores específicos como as áreas de finanças, farmacêutica e saúde
- Seleção de provedores de serviços e o gerenciamento e aquisição de serviços terceirizados
- Os riscos relacionados a TI cada vez mais complexos, como a segurança de redes
- Iniciativas de governança de TI que incluem a adoção de metodologias de controles e boas práticas que ajudem a monitorar e aprimorar as atividades críticas de TI para ampliar o valor do negócio e reduzir os riscos.
- A necessidade de otimizar os custos seguindo, sempre que possível, um enfoque padronizado em vez de abordagens especialmente desenvolvidas.
- A crescente maturidade e consequente aceitação de metodologias bem-sucedidas, tais como o COBIT, IT Infrastructure Library (ITIL), séries ISO 27000 sobre padrões relacionados à segurança da informação, ISO 9001:2000 – Requerimentos – Sistemas de Gerenciamento de Qualidade, Capability Maturity Model Integration (CMNI), Projects in Controlled Environments 2 (PRINCE2) e o Guide to the Project Management Body of Knowledge (PMBOK).
- A necessidade de as empresas avaliarem como estão em relação aos padrões geralmente aceitos e em comparação seus parceiros e organizações similares *(benchmarking)*

Quem

Uma metodologia de governança e controles precisa servir a uma variedade de partes interessadas tanto internas como externas, cada uma com necessidades especificas:

- Partes interessadas dentro da empresa *(stakeholders)* que procuram gerar valor a partir dos investimentos em TI:
  - Aqueles que tomam decisões sobre investimentos
  - Aqueles que decidem sobre requisitos
  - Aqueles que usam os serviços de TI
- Partes interessadas dentro e fora da empresa que fornecem serviços de TI:
  - Aqueles que gerenciam a organização e os processos de TI
  - Aqueles que desenvolvem as capacidades
  - Aqueles que operam os serviços
- Partes interessadas dentro e fora da empresa que têm responsabilidades sobre controles/riscos:
  - Aqueles com responsabilidades sobre segurança, confidencialidade e/ou riscos
  - Aqueles que executam funções de conformidade
  - Aqueles que requerem ou fornecem serviços de avaliação

O quê

Para atender aos requisitos listados na seção anterior, uma metodologia de governança e controle de TI deve:

- Fornecer um foco de negócios para permitir o alinhamento entre os objetivos de negócios e de TI
- Estabelecer um processo de orientação para definir os escopos e a extensão da cobertura, com uma estrutura definida permitindo uma fácil navegação em seu conteúdo
- Ser geralmente aceita por ser consistente com as boas práticas e padrões de TI e independente de tecnologias específicas
- Prover uma linguagem comum com um conjunto de termos e definições geralmente entendidos por todas as partes interessadas
- Ajudar a atender aos requisitos regulatórios por ser consistente com padrões de governança geralmente aceitos (como o COSO) e controles de TI esperados por reguladores e auditores externos

COMO O CobiT ATENDE A NECESSIDADE

Em respostas às necessidades descritas na seção anterior, o modelo CobiT foi criado com as principais características de ser focado em negócios, orientado a processos, baseado em controles e orientado por medições.

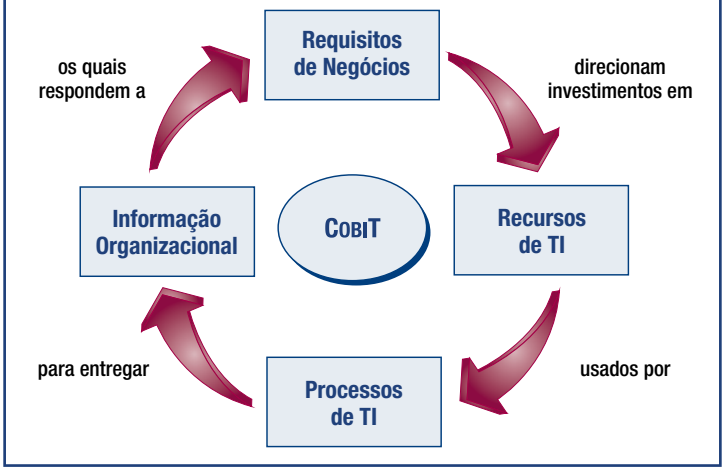
Focado em negócios

A orientação para negócios é o principal tema do CobiT, o qual foi desenvolvido não somente para ser utilizado por provedores de serviços, usuários e auditores, mas também, e mais importante, para fornecer um guia abrangente para os executivos e donos de processos de negócios.

O modelo CobiT é baseado nos seguintes princípios (figura 5): Prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir, gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.

O gerenciamento e o controle da informação estão presentes em toda a metodologia CobiT e ajudam a assegurar o alinhamento com os requisitos de negócios.

Figura 5 - Princípios Básicos do CobiT



CRITÉRIOS DE INFORMAÇAO DO CobiT

Para atender aos objetivos de negócios, as informações precisam se adequar a certos critérios de controles, aos quais o CobiT denomina necessidades de informação da empresa. Baseado em abrangentes requisitos de qualidade, guarda e segurança, sete critérios de informação distintos e sobrepostos são definidos, como segue:

- **Efetividade** lida com a informação relevante e pertinente para o processo de negócio bem como a mesma sendo entregue em tempo, de maneira correta, consistente e utilizável.
- **Eficiência** relaciona-se com a entrega da informação através do melhor (mais produtivo e econômico) uso dos recursos.
- **Confidencialidade** está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida.

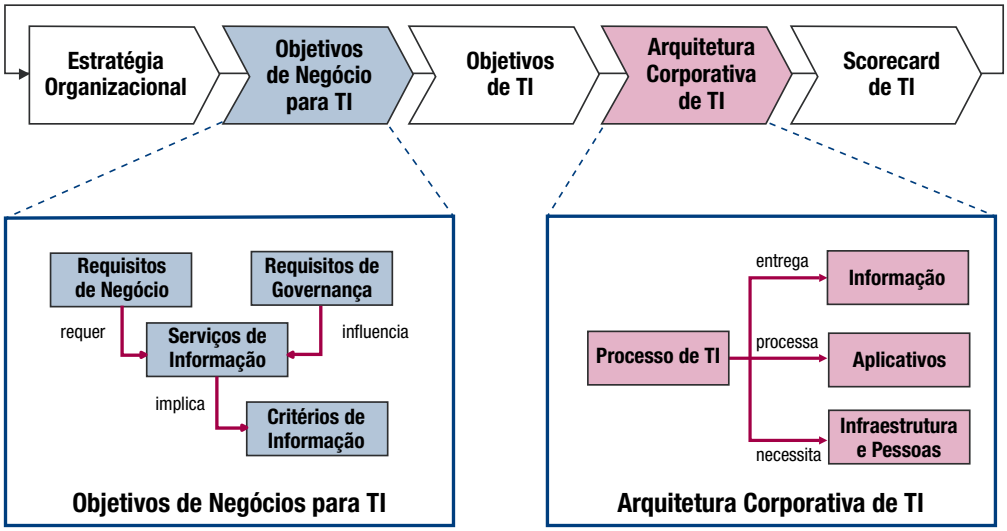
- **Integridade** relaciona-se com a fidedignidade e totalidade da informação bem como sua validade de acordo os valores de negócios e expectativas.
- **Disponibilidade** relaciona-se com a disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro. Também está ligada à salvaguarda dos recursos necessários e capacidades associadas.
- **Conformidade** lida com a aderência a leis, regulamentos e obrigações contratuais aos quais os processos de negócios estão sujeitos, isto é, critérios de negócios impostos externamente e políticas internas.
- **Confiabilidade** relaciona-se com a entrega da informação apropriada para os executivos para administrar a entidade e exercer suas responsabilidades fiduciárias e de governança.

OBJETIVOS DE NEGÓCIOS E OBJETIVOS DE TI

Enquanto os critérios de informação fornecem um método genérico para definir os requisitos de negócios, definir um conjunto genérico de objetivos de negócios e de TI fornece uma base mais refinada para o estabelecimento dos requisitos de negócios e o desenvolvimento de métricas que permitam avaliar se esses objetivos foram atendidos. Toda organização usa TI para fazer funcionar as iniciativas de negócios e essas podem ser representadas como objetivos de negócios para a área de TI. Esses exemplos genéricos podem ser utilizados como um guia para determinar os requisitos de negócios específicos, as metas e as métricas para a organização.

Para a área de TI entregar de maneira bem-sucedida os serviços que suportam as estratégias de negócios, deve existir uma clara definição das responsabilidades e direcionamento dos requisitos pela área de negócios (o cliente) e um claro entendimento acerca do que e como precisa ser entregue pela TI (o fornecedor). A **Figura 6** ilustra como a estratégia da empresa deveria ser traduzida pela área de negócios em objetivos relacionados às iniciativas de TI (objetivos de negócios para TI). Esses objetivos devem levar a uma clara definição dos objetivos próprios da área de TI (os objetivos de TI), o que por sua vez irá definir os recursos e capacidades de TI (a arquitetura de TI para a organização) necessários para executar de maneira bem-sucedida a parte que cabe à TI na estratégia da empresa. [1]

Figura 6 - Definindo os objetivos de TI e a Arquitetura da Empresa para TI



Uma vez que os objetivos alinhados estiverem definidos, eles precisam ser monitorados para assegurar que as entregas atendam às expectativas. Isto é alcançado por métricas derivadas dos objetivos e capturadas pelo *scorecard* de TI.

Para que o cliente entenda os objetivos de TI e o *scorecard* de TI, todos esses objetivos e métricas associadas devem ser expressos em termos de negócios significativos para o cliente. Combinado com um efetivo alinhamento da hierarquia dos objetivos, isto irá assegurar que os negócios confirmem que TI irá provavelmente colaborar para que a empresa atinja seus objetivos.

O Apêndice I 015 – Tabelas Relacionando os Objetivos e Processos – apresenta uma visão global de como os objetivos genéricos de negócios relacionam-se com os objetivos, processos e critérios de informação de TI. As tabelas ajudam a demonstrar o escopo do COBIT e o relacionamento geral dos negócios entre o COBIT e o direcionamento a empresa. Como ilustrado na **figura 6**, esses direcionamentos derivam dos negócios e dos níveis de governança da empresa, o primeiro focando mais na funcionalidade e velocidade da entrega, enquanto que o último foca mais em eficiência dos custos, retorno do investimento (ROI) e aderência.

[1] É necessário mencionar que a definição e a implementação de uma arquitetura corporativa de TI também criarão objetivos internos de TI que contribuem para os objetivos de negócios, mas não são diretamente derivados desses objetivos.

RECURSOS DE TI

A organização de TI entrega de acordo com esses objetivos por um conjunto claramente definido de processos que usam a experiência das pessoas e a infra-estrutura tecnológica para processar aplicativos de negócios de maneira automatizada, aprimorando as informações de negócios. Esses recursos em conjunto com os processos constituem a arquitetura de TI da organização, como demonstrado na figura 6.

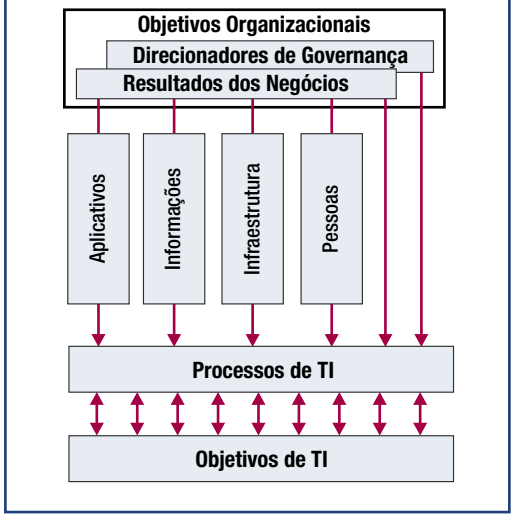
Para atender aos requisitos de negócios para TI, a organização precisa investir nos recursos necessários para criar uma adequada capacidade técnica (ex. um sistema de planejamento de recursos [ERP]) que atenda a uma necessidade de negócios (ex. implementar um canal de suprimentos) resultando no desejado retorno (ex. aumento de vendas e benefícios financeiros).

Os recursos de TI identificados no CobiT podem ser definidos como segue:

- **Aplicativos** são os sistemas automatizados para usuários e os procedimentos manuais que processam as informações.
- **Informações** são os dados em todas as suas formas, a entrada, o processamento e a saída fornecida pelo sistema de informação em qualquer formato a ser utilizado pelos negócios.
- **Infraestrutura** refere-se à tecnologia e aos recursos (ou seja, hardware, sistemas operacionais, sistemas de gerenciamento de bases de dados, redes, multimídia e os ambientes que abrigam e dão suporte a eles) que possibilitam o processamento dos aplicativos.
- **Pessoas** são os funcionários requeridos para planejar, organizar, adquirir, implementar, entregar, suportar, monitorar e avaliar os sistemas de informação e serviços. Eles podem ser internos, terceirizados ou contratados, conforme necessário.

A **Figura 7** mostra como os objetivos de negócios para TI influenciam o modo como os recursos de TI precisam ser gerenciados pelos processos de TI para entregar os objetivos de TI.

Figura 7 - Gerenciando os Recursos de TI para Entregar os Objetivos de TI



Orientado para processos

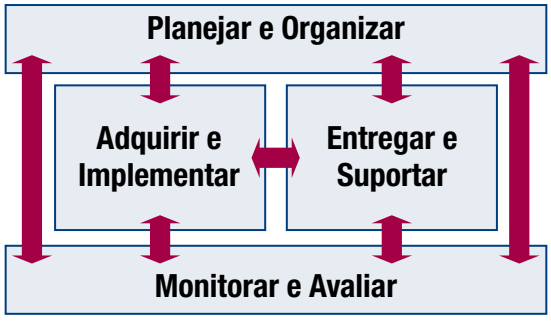
O CobiT define as atividades de TI em um modelo de processos genéricos com quatro domínios. Esses domínios são Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar e Monitorar e Avaliar. Esses domínios mapeiam as tradicionais áreas de responsabilidade de TI de planejamento, construção, processamento e monitoramento.

O modelo CobiT fornece um modelo de processo de referência e uma linguagem comum para que todos na organização possam visualizar e gerenciar as atividades de TI. Incorporar o modelo operacional e a linguagem comum para todas as áreas de negócios envolvidas em TI é um dos mais importantes passos e ações preliminares para uma boa governança. Isto também fornece uma metodologia para medição e monitoramento da performance de TI, comunicação com provedores de serviços e integração das melhores práticas de gerenciamento. Um modelo de processos incentiva a determinação de proprietários dos processos, o que possibilita a definição de responsabilidades.

Para que a governança de TI seja eficiente, é importante avaliar as atividades e riscos da TI que precisam ser gerenciados. Geralmente eles são ordenados por domínios de responsabilidade de planejamento, construção, processamento e monitoramento. No modelo CobiT esses domínios, como demonstrado na Figura 8, são denominados:

- **Planejar e Organizar (PO)** - Provê direção para entrega de soluções (AI) e entrega de serviços (DS)
- **Adquirir e Implementar (AI)** - Provê as soluções e as transfere para tornarem-se serviços
- **Entregar e Suportar (DS)** - Recebe as soluções e as torna passíveis de uso pelos usuários finais
- **Monitorar e Avaliar (ME)** - Monitora todos os processos para garantir que a direção definida seja seguida.

Figura 8 - Os Quatro Domínios Inter-relacionados do CobiT



PLANEJAR E ORGANIZAR (PO)

Este domínio cobre a estratégia e as táticas, preocupando-se com a identificação da maneira em que TI pode melhor contribuir para atingir os objetivos de negócios. O sucesso da visão estratégica precisa ser planejado, comunicado e gerenciado por diferentes perspectivas. Uma apropriada organização bem como uma adequada infraestrutura tecnológica devem ser colocadas em funcionamento. Este domínio tipicamente ajuda a responder as seguintes questões gerenciais:

- As estratégias de TI e de negócios estão alinhadas?
- A empresa está obtendo um ótimo uso dos seus recursos?
- Todos na organização entendem os objetivos de TI?
- Os riscos de TI são entendidos e estão sendo gerenciados?
- A qualidade dos sistemas de TI é adequada às necessidades de negócios?

ADQUIRIR E IMPLEMENTAR (AI)
Para executar a estratégia de TI, as soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, implementas e integradas ao processo de negócios. Além disso, alterações e manutenções nos sistemas existentes são cobertas por esse domínio para assegurar que as soluções continuem a atender aos objetivos de negócios. Este domínio tipicamente trata das seguintes questões de gerenciamento:
- Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
- Os novos projetos serão entregues no tempo e orçamento previstos?
- Os novos sistemas ocorreram apropriadamente quando implementado?
- As alterações ocorrerão sem afetar as operações de negócios atuais?

ENTREGAR E SUPORTAR (DS)
Este domínio trata da entrega dos serviços solicitados, o que inclui entrega de serviço, gerenciamento da segurança e continuidade, serviços de suporte para os usuários e o gerenciamento de dados e recursos operacionais. Trata geralmente das seguintes questões de gerenciamento:
- Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios?
- Os custos de TI estão otimizados?
- A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura?
- Os aspectos de confidencialidade, integridade e disponibilidade estão sendo contemplados para garantir a segurança da informação?

MONITORAR E AVALIAR (ME)
Todos os processos de TI precisam ser regularmente avaliados com o passar do tempo para assegurar a qualidade e a aderência aos requisitos de controle. Este domínio aborda o gerenciamento de performance, o monitoramento do controle interno, a aderência regulatória e a governança. Trata geralmente das seguintes questões de gerenciamento:
- A performance de TI é mensurada para detectar problemas antes que seja muito tarde?
- O gerenciamento assegura que os controles internos sejam efetivos e eficientes?
- O desempenho da TI pode ser associado aos objetivos de negócio?
- Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?

Dentro desses quatro domínios o COBIT identificou 34 processos de TI geralmente utilizados (veja a **Figura 23** para uma lista completa). Embora a maioria das organizações tenha definido as responsabilidades de TI de planejar, construir, processar e monitorar, e muitas delas tenham os mesmos processos-chave, poucas terão a mesma estrutura de processos ou aplicarão todos os 34 processos do COBIT. O COBIT fornece uma completa lista de processos que podem ser utilizados para verificar a totalidade das atividade e responsabilidades. No entanto, nem todos precisam ser aplicados e podem ser combinados conforme as necessidades de cada empresa.

Para cada um desses 34 processos, uma ligação foi feita com os objetivos de negócios e de TI suportados. Também são fornecidas informações sobre como os objetivos podem ser medidos, quais são as atividades-chave, as principais entregas e quem é responsável por elas.

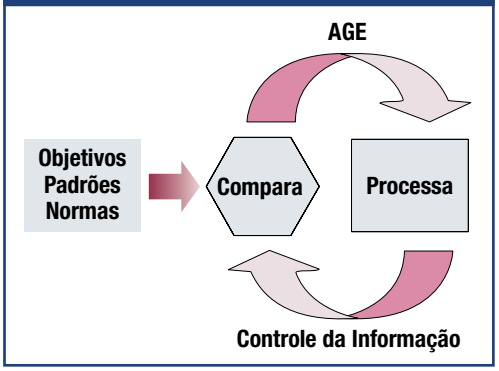
Baseado em Controles
O COBIT define objetivos de controles para todos os 34 processos e engloba todos os processos e controles de aplicativos.

PROCESSOS PRECISAM DE CONTROLES
Controle é definido como políticas, procedimentos, práticas e estruturas organizacionais criadas para prover uma razoável garantia de que os objetivos de negócios serão atingidos e que eventos indesejáveis serão evitados ou detectados e corrigidos.

Os objetivos de controle de TI fornecem um conjunto completo de requisitos de alto nível a serem considerados pelos executivos para um controle efetivo de cada processo de TI. Eles:
- São definições de ações gerenciais para aumentar o valor ou reduzir o risco
- Consistem em políticas, procedimentos, práticas e estruturas organizacionais
- São desenvolvidos para prover uma razoável garantia de que os objetivos de controle serão atingidos e que eventos indesejáveis serão evitados ou detectados e corrigidos

A empresa precisa fazer escolhas relacionadas a esses processos ao:
- Selecionar aqueles que são aplicáveis
- Decidir quais deles serão implementados
- Escolher como implementá-los (frequência, abrangência, automação, etc.)
- Aceitar o risco de não implementar aqueles que podem ser aplicáveis

Figura 9 - Modelo de Controle



Uma diretriz pode ser obtida no modelo padrão de controle apresentado na **Figura 9**. Ele segue o principio evidente na seguinte analogia: Quando a temperatura da sala (padrão) do sistema de aquecimento (processo) está definida, o sistema irá constantemente averiguar (comparar) a temperatura ambiente da sala (controle de informação) e irá sinalizar (agir) para o sistema de aquecimento para prover mais ou menos calor.

Os gerentes operacionais usam os processos para organizar e gerenciar as atividades de TI em andamento. O CobiT provê um modelo de processo genérico que representa todos os processos normalmente encontrados nas funções de TI, fornecendo um modelo referência comum compreensível para os gerentes das operações de TI e de negócios. Para atingir uma governança efetiva, os controles precisam ser implementados pelos gerentes operacionais de acordo com um método definido de controles para todos os processos de TI. Uma vez que os controles de TI do CobiT são organizados por processos de TI, o método fornece uma ligação clara em relação aos requisitos de governança, processos e controles de TI.

Cada um dos processos de TI do CobiT possui uma descrição do processo e um número do objetivo de controle. No todo, eles formam as características de um processo bem gerenciado.

Os objetivos de controles são identificados por duas letras para identificar o domínio (PO, AI, DS e ME), um número de processo e um número de objetivo de controle. Além dos objetivos de controle, cada processo do CobiT possui requisitos de controle genéricos identificados por PC(n), que indica o número de controle do processo. Eles devem ser considerados junto com os objetivos de controle dos processos para que se tenha uma visão completa dos requisitos de controle.

PC1 Metas e Objetivos do Processo
Define e comunica as metas e objetivos específicos, mensuráveis, acionáveis, realísticos, orientados a resultados e no tempo apropriado (SMARRT) para a efetiva execução de cada processo de TI. Assegura que eles estão ligados aos objetivos de negócios e que são suportados por métricas apropriadas.

PC2 Propriedade dos Processos
Designa um proprietário para cada processo de TI e claramente define os papéis e responsabilidades de cada proprietário de processo. Inclui por exemplo, a responsabilidade pela elaboração do processo, interação com outros processos, responsabilidade pelos resultados finais, medidas da performance do processo e a identificação de oportunidades de melhorias.

PC3 Repetibilidade dos Processos
Elabora e estabelece cada processo-chave de TI de maneira que possa ser repetido e produzir de maneira consistente os resultados esperados. Fornece uma sequência lógica mas flexível das atividades que levarão ao resultado desejado, sendo ágil o suficiente para lidar com exceções e emergências. Usa processos consistentes, quando possível, e processos personalizados apenas quando inevitável.

PC4 Papéis e Responsabilidades
Define as atividades-chaves e as entregas do processo. Designa e comunica papéis e responsabilidades para uma efetiva e eficiente execução das atividades-chaves e sua documentação bem como a responsabilização pelo processo e suas entregas.

PC5 Políticas Planos e Procedimentos
Define e comunica como todas as políticas, planos e procedimentos que direcionam os processos de TI são documentados, revisados, mantidos, aprovados, armazenados, comunicados e utilizados para treinamento. Designa responsabilidades para cada uma dessas atividades e em momentos apropriados verifica se elas são executadas corretamente. Assegura que as políticas, planos e procedimentos sejam acessíveis, corretos, entendidos e atualizados.

PC6 Melhoria do Processo de Performance
Identifica um conjunto de métricas que fornecem direcionamento para os resultados e performance dos processos. Estabelece metas que refletem nos objetivos dos processos e indicadores de performance que permitem atingir os objetivos dos processos. Definem como os dados são obtidos. Compara as medições reais com as metas e toma medidas quanto aos desvios quando necessário. Alinha métricas, metas e métodos com o enfoque de monitoramento de performance geral de TI.

Controles efetivos reduzem riscos, aumentam a probabilidade da entrega de valor e aprimoram a eficiência, pois existirão poucos erros e o enfoque de gerenciamento será mais consistente.

Além disso, o CobiT traz exemplos de cada processo que são ilustrativos, mas não definidores ou completos, de:
Entradas e saídas em geral
- Atividades e orientações sobre papéis e responsabilidades em uma tabela que indica quem é responsável, responsabilizado, consultado e informado (RACI).
- Principais objetivos da atividade (o que de mais importante deve ser feito).
- Métricas

Além de avaliar quais controles são necessários, os proprietários dos processos devem entender quais entradas eles precisam receber de outros e o que os outros precisam de seu processo. O COBIT fornece exemplos de entradas e saídas básicos que servem para qualquer processo, incluindo requisitos externos de TI. Existem alguns tipos de saída que servem de entrada para todos os outros processos, os quais são marcados como "ALL" nas tabelas de saídas e, portanto, não são mencionados como entradas para todos os processos. Geralmente incluem os padrões de qualidade e requisitos de métricas, a estrutura do processo de TI, os papéis e responsabilidades documentados, a estrutura de controle de TI da organização, as políticas de TI e as funções e responsabilidades dos funcionários.

O entendimento dos papéis e responsabilidades de cada processo é essencial para uma efetiva governança. O COBIT provê a tabela RACI para cada processo. O termo Responsabilizado significa que "a responsabilidade é deste indivíduo" – esta é a pessoa que dá orientações e autoriza uma atividade. A responsabilidade é atribuída à pessoa que faz com que a tarefa seja executada. Os outros dois papéis (consultado e informado) asseguram que todos que precisam serão envolvidos e suportam o processo.

CONTROLES DE NEGÓCIOS E DE TI

Os sistemas de controles internos das organizações afetam a área de TI em três níveis:

- No nível da Alta Direção, os objetivos de negócios e as políticas são definidos e decisões são tomadas em relação a como entregar e gerenciar os recursos da organização para executar a estratégia. O enfoque geral para a governança e o controle é definido pela Alta Direção e comunicado para toda a organização. O ambiente de controle de TI é direcionado por estes objetivos e políticas de alto nível.
- No nível dos processos de negócios, os controles são aplicados às atividades específicas dos negócios. A maioria dos processos de negócios é automatizada e integrada aos sistemas aplicativos de TI. No entanto, alguns controles existentes no processo de negócios permanecem como procedimentos manuais, tais como a autorização para transações, a segregação de funções e as reconciliações manuais. Portanto, os controles no nível dos processos de negócios são uma combinação de controles manuais conduzidos pela área de negócios e controles de negócios e de aplicativos automatizados. Ambos são de responsabilidade da área de negócios no que se refere a definição e gerenciamento, embora os controles dos aplicativos exijam a participação da área de TI no seu projeto e desenvolvimento.
- Para suportar os processos de negócios, a área de TI fornece serviços de TI, usualmente de maneira compartilhada para diversos processos de negócios, uma vez que muitos processos de desenvolvimento e operacionais de TI são supridos para toda a organização e boa parte da infra-estrutura de TI é provida como um serviço comum (por exemplo, redes, bases de dados, sistemas operacionais e armazenamento). Os controles aplicados a todas as atividades de serviços de TI chamados de controles gerais de TI. A operação confiável desses controles é necessária para que se possa confiar nos controles existentes nos aplicativos. Por exemplo, um gerenciamento de mudanças insatisfatório poderia prejudicar (acidental ou deliberadamente) a confiança depositada em testes de integridade automáticos.

CONTROLES GERAIS DE TI E CONTROLES DE APLICATIVOS

Os controles gerais são controles inseridos nos processos de TI e serviços. Como exemplo citamos:

- Desenvolvimento de sistemas
- Gerenciamento de mudanças
- Segurança
- Operação de computadores

Os controles inseridos nos aplicativos de processos de negócios são comumente chamados de controles de aplicativos. Exemplos:

- Totalidade
- Veracidade
- Validade
- Autorização
- Segregação de funções

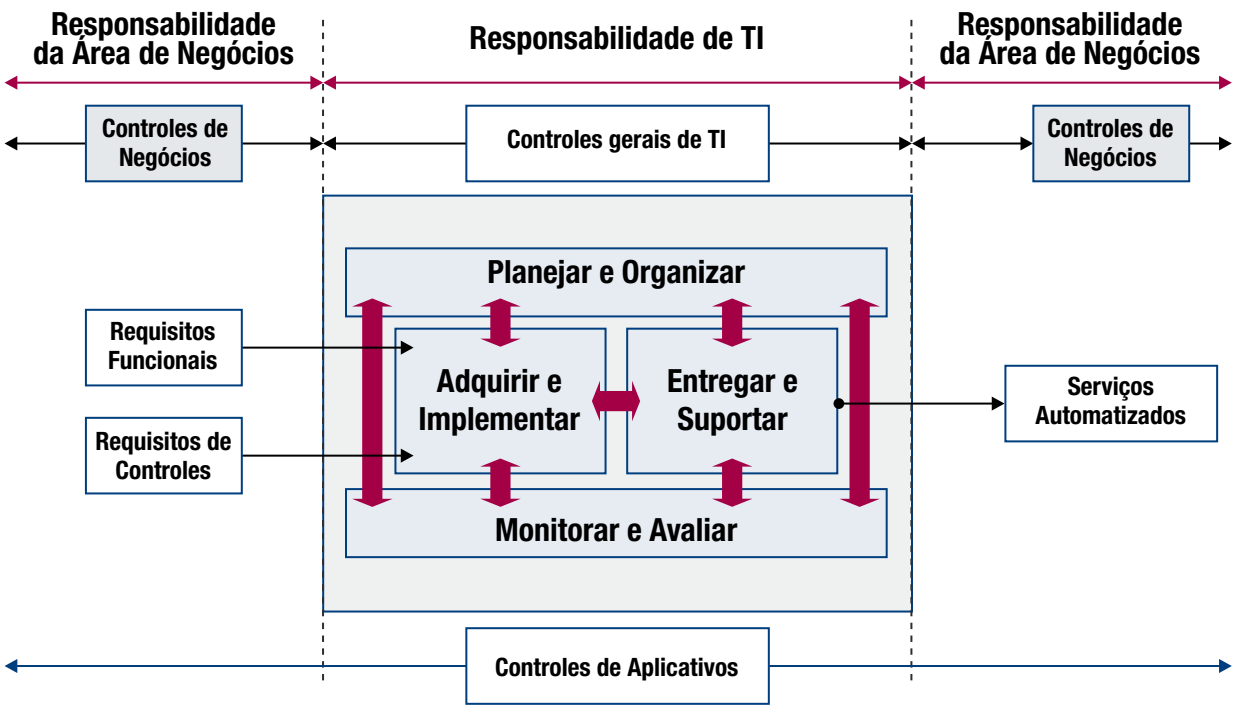
O COBIT assume que o projeto e a implementação dos controles automatizados em aplicativos é de responsabilidade da área de TI, cobertos no domínio Aquisição e Implementação, com base nos requisitos de negócios definidos a partir dos critérios de informação do COBIT, como demonstrado na Figura 10. A responsabilidade pelo controle e o gerenciamento operacional dos controles de aplicativos não é da área de TI, mas do proprietário do processo de negócio.

Assim, a responsabilidade pelos controles de aplicativos é compartilhada entre as áreas de negócios e de TI, mas a natureza das responsabilidades muda, como segue:

- A área de negócios é responsável por:
  - Definir os requisitos funcionais e de controles
  - Utilizar os serviços automatizados
- A área de TI é responsável por:
  - Automatizar e implementar os requisitos funcionais e de controles
  - Estabelecer controles para manter a integridade dos controles de aplicativos

Portanto os processos de TI do COBIT cobrem os controles gerais de TI, mas somente os aspectos do desenvolvimento dos controles de aplicativos; a responsabilidade pela definição e o uso operacional é da área de negócio.

Figura 10 - Fronteiras de Negócios, Controles Gerais e de Aplicativos



A lista a seguir apresenta um conjunto recomendado de objetivos de controles de aplicativos. Eles são identificados como “ACn” , que significa o número do controle de aplicação.

AC1 Preparação e Autorização de Dados Originais
Assegura que os documentos fonte sejam preparados por pessoal autorizado e qualificado seguindo os procedimentos estabelecidos, levando em consideração uma adequada segregação de funções relacionadas com a criação e aprovação desses documentos. Erros e omissões podem ser minimizados através de bom desenho de formulário para entrada da informação, permitindo que erros e irregularidades detectados sejam reportados e corrigidos.

AC2 Entrada e Coleta de Dados Fontes
Estabelece que a entrada de dados seja executada de maneira apropriada por pessoal autorizado e qualificado. A correção e o reenvio de dados que foram erroneamente inseridos devem ser executados sem comprometer o nível de autorização da transação original. Quando apropriado para a reconstrução, os documentos originais devem ser guardados por um período adequado.

AC3 Testes de Veracidade, Totalidade e Autenticidade
Assegura que as transações sejam exatas, completas e válidas. Valida os dados que foram inseridos e editados ou enviados de volta para correção o mais próximo possível do ponto onde foram originados.

AC4 Processamento Íntegro e Válido
Mantém a integridade e validade dos dados no ciclo de processamento. A detecção de transações errôneas não interrompe o processamento de transações válidas.

AC5 Revisão das Saídas, Reconciliação e Manuseio de Erros
Estabelece procedimentos e responsabilidades associadas para assegurar que as saídas sejam manuseadas de uma forma autorizada, entregues para os destinatários corretos e protegidas durante a transmissão. Garante que ocorre a verificação, detecção e correção da exatidão das saídas e que a informação provida pela saída é usada.

AC6 Autenticação e Integridade das Transações
Antes de transportar os dados das transações entre os aplicativos e as funções de negócios/operacionais (internas ou externas à organização), verifica endereçamento adequado, autenticidade da origem e integridade do conteúdo. Mantém a autenticidade e integridade durante a transmissão ou transporte.

Direcionamento Baseado em Medição

Uma necessidade básica para toda organização é entender a situação dos seus próprios sistemas de TI e decidir que nível de gerenciamento e controle a empresa deveria ter. Para decidir dentro de um nível correto, os executivos devem se perguntar: Quão distante devemos ir e será que o custo é justificado pelo benefício?

Obter uma visão objetiva do nível de performance da própria organização não é fácil. O que deve ser avaliado e como? As organizações precisam avaliar onde elas e onde são requeridas melhorias, bem como implementar um conjunto de ferramentas de gerenciamento para atingir esse aprimoramentos. O CobiT lida com essas questões por fornecer:

- Modelos de maturidade que permitem fazer comparações e identificar os necessários aprimoramentos de capacidades,
- Objetivos de performance e métricas para os processos de TI, demonstrando como os processos atingem os objetivos de negócios e de TI e são utilizados para mensurar a performance dos processos internos baseados nos princípios do *balanced scorecard*
- Objetivo de atividades para habilitar o efetivo desempenho do processo

MODELOS DE MATURIDADE

A Alta Direção de corporações e de grandes organizações é cada vez mais solicitada a considerar quão bem a área de TI está sendo gerenciada. Em resposta, planos de negócios requerem o desenvolvimento de melhorias e um apropriado gerenciamento e controle sobre a infra-estrutura de informação. Enquanto alguns argumentariam que isso não é algo importante, é preciso considerar o custo-benefício e as seguintes questões relacionadas:

- O que os nossos concorrentes estão fazendo e como estamos posicionados em relação a eles?
- Quais são as boas práticas aceitáveis para o ambiente de negócio e como estamos colocados em relação a essas práticas?
- Com base nessas comparações, podemos dizer que estamos fazendo o suficiente?
- Como podemos identificar o que precisa ser feito para atingir um nível adequado de gerenciamento e controle sobre os processos de TI?

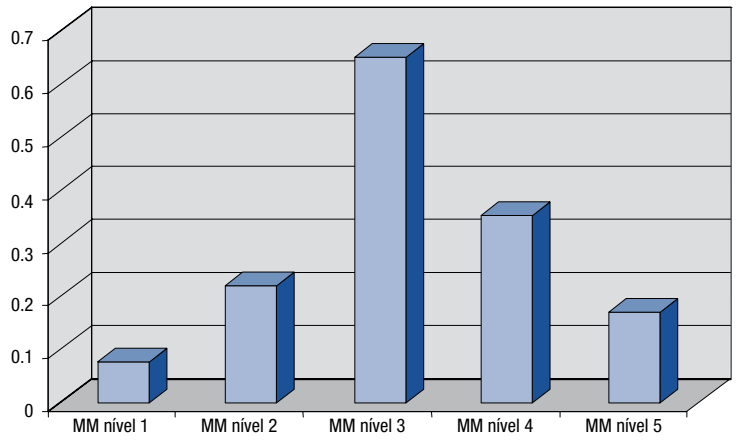
Pode ser difícil fornecer respostas significativas para essas questões. O gerenciamento de TI está constantemente procurando ferramentas de benchmarking e de autoavaliação em resposta à necessidade de saber o que fazer de maneira eficiente. Começando com os processos CobiT, o proprietário do processo poderá gradativamente ampliar as comparações com os objetivos de controle. Isso atende a três necessidades:

1. Uma medida relativa de onde a empresa está
2. Uma maneira de eficientemente decidir para onde ir
3. Uma ferramenta para avaliação do progresso em relação às metas

O modelo de maturidade para o gerenciamento e controle dos processos de TI é baseado num método de avaliar a organização, permitindo que ela seja pontuada de um nível de maturidade não-existente (0) a otimizado (5). Este enfoque é derivado do modelo de maturidade do Software Engineering Institute (SEI) definido para a maturidade da capacidade de desenvolvimento de software. Embora siga os conceitos do SEI, a implementação CobiT difere consideravelmente do original do SEI, o qual era orientado para os princípios de engenharia de produtos de software, organizações buscando excelência nessas áreas e uma avaliação formal dos níveis de maturidade para que os desenvolvedores de software pudessem ser "certificados". No CobiT, uma definição genérica é provida para as escalas de maturidade do CobiT as quais são similares às do CMM mas interpretadas de acordo com a natureza dos processos de gerenciamento de TI do CobiT. Um modelo específico é fornecido derivando dessa escala genérica para cada um dos 34 processos CobiT. Independente do modelo, as escalas não devem ser tão granulares visto que seria difícil de utilizar e sugeriria um precisão não justificável, por que em geral o propósito é identificar onde estão as questões e como definir prioridades para aprimoramentos. O propósito não é avaliar o nível de aderência aos objetivos de controles.

Os níveis de maturidade são designados como perfis de processos de TI que a empresa reconheceria como descrição de possíveis situações atuais e futuras. Eles não são designados como um modelo inicial, onde não se pode avançar para o próximo nível sem antes ter cumprido todas as condições do nível inferior. Com os modelos de maturidade do CobiT, diferentemente do enfoque original SEI CMM, não há intenção de medir os níveis de maneira precisa ou tentar certificar que aquele nível foi exatamente atingido. A avaliação de maturidade do CobiT espera resultar em um perfil em que as condições relevantes para diversos níveis de maturidade serão atingidas, como demonstrado no gráfico de exemplo da **Figura 11**.

Figura 11 - Possível Nível de Maturidade de um Processo de TI



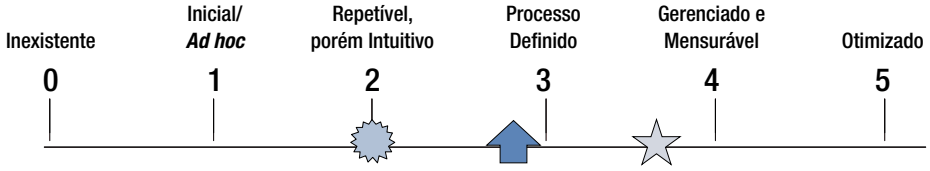
Possível Nível de Maturidade de um Processo de TI: O exemplo ilustra um processo que está amplamente situado no nível 3 mas que ainda tem algumas questões de aderência como os requerimentos de nível mais baixo, embora já esteja investindo na medição de performance (nível 4) e em otimização (nível5)

Isto ocorre porque quando aplicamos a avaliação de maturidade usando o CobiT, às vezes uma implementação estará em andamento em diferentes níveis mesmo que não de maneira completa e suficiente. Esses pontos fortes podem ser trabalhados para aprimorar a maturidade. Por exemplo, algumas partes do processo podem estar bem definidas e mesmo estando incompletas, seria enganoso afirmar que o processo não está definido.

Ao utilizar os modelos de maturidade desenvolvidos para cada um dos 34 processos de TI do CobiT, a gerencia pode identificar:
- O estágio atual de performance da empresa – Onde a empresa está hoje
- O estágio atual do mercado – A comparação
- A meta de aprimoramento da empresa – Onde a empresa quer estar
- O caminho de crescimento entre o "como está" e "como será"

Para tornar os resultados mais facilmente utilizáveis em sumários gerenciais, onde serão mostrados como meio de suporte para planos de negócios *(business cases)*, um método de apresentação é necessário (**Figura 12**).

Figura 12 - Representação Gráfica dos Modelos de Maturidade



LEGENDAS PARA OS SÍMBOLOS UTILIZADOS

Estágio atual da empresa

Média do mercado

Meta da empresa

LEGENDA UTILIZADA PARA MEDIÇÃO

0 - Gerenciamento de processos não aplicado.
1 - Processos são *ad hoc* e desorganizados.
2 - Processos seguem um caminho padrão.
3 - Processos são documentados e comunicados.
4 - Processos são monitorados e medidos.
5 - Boas práticas são seguidas e automatizadas.

O desenvolvimento dessa representação gráfica foi baseado nas descrições genéricas do modelo de maturidade demonstradas na **Figura 13**.

O modelo CobiT para o gerenciamento de processos de TI foi desenvolvido como uma ênfase forte em controles. Essas escalas precisam ser práticas para serem aplicadas e de fácil entendimento. O assunto gerenciamento de processos de TI é inerentemente complexo e subjetivo e portanto, é mais bem tratado através de avaliações facilitadas que provocam a consciência, capturam o consenso geral e motivam o aprimoramento. Essas avaliações podem ser executadas com base nas descrições do nível de maturidade como um todo ou com um maior rigor contra cada uma das afirmações individuais dessas descrições. Seja qual for o caminho escolhido, é preciso ter experiência no processo que está sendo revisado.

A vantagem de uma abordagem de modelo de maturidade é a relativa facilidade de os gerentes colocarem-se a si mesmos em uma escala e avaliar o que está envolvido no aprimoramento da performance, se necessário. As escalas incluem o 0, pois é possível que um processo não exista de fato. A escada de 0 a 5 é baseada em uma escala simples de maturidade, demonstrando como um processo evolui de capacidade inexistente para capacidade otimizada.

No entanto o processo de gerenciamento de capacidade não é o mesmo que a performance do processo. As capacidades requeridas como determinado pelos objetivos de negócios e de TI podem não ser aplicadas no mesmo nível em todo o ambiente de TI, ou seja, não de forma consistente ou somente para um limitado número de sistemas ou unidades. A medição de performance como visto nos próximos parágrafos é essencial para determinar a performance atual da empresa nos seus processos de TI.

Figura 13 - Modelo de Maturidade Genérico

0 Inexistente – Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada.

1 Inicial / *Ad hoc* – Existem evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem enfoques *Ad Hoc* que tendem a ser aplicados individualmente ou caso-a-caso. O enfoque geral de gerenciamento é desorganizado.

2 Repetível, porém Intuitivo – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixado com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e conseqüentemente erros podem ocorrer.

3 Processo Definido – Procedimentos foram padronizados, documentados e comunicados através de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados mas existe a formalização das práticas existentes.

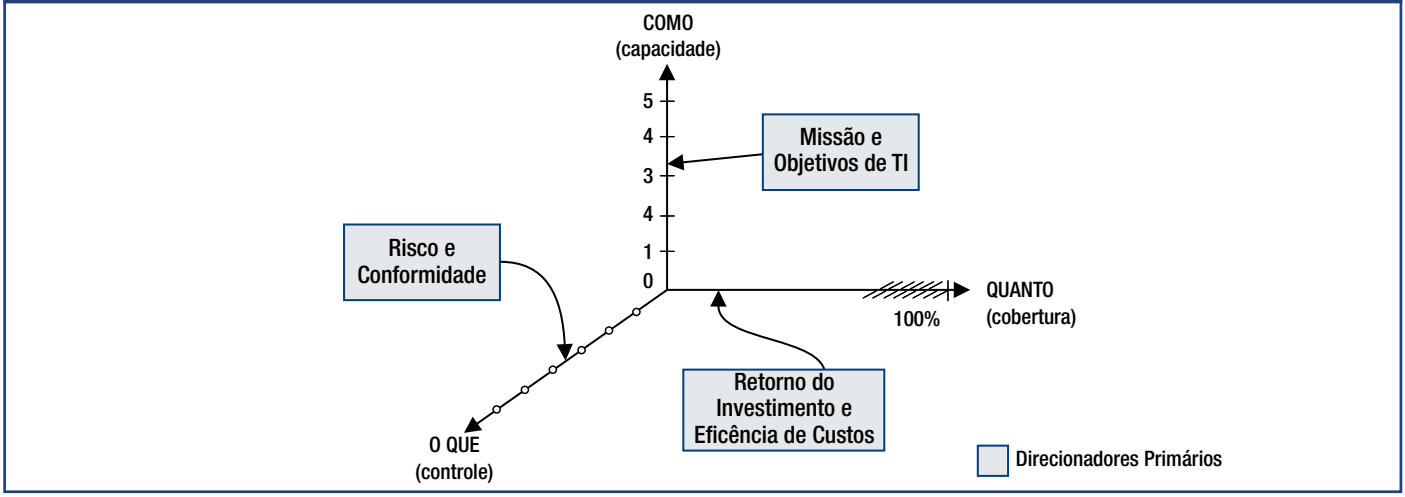
4 Gerenciado e Mensurável – A gerencia monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão debaixo de um constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.

5 Otimizado – Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida em adaptar-se.

Embora uma capacidade apropriadamente aplicada já reduza riscos, a organização ainda precisa analisar quais os controles necessários para assegurar que os riscos sejam mitigados e que valor é obtido em linha com o apetite de risco e objetivos de negócios. Esses controles são guiados pelos objetivos de controle do COBIT. O Apêndice III provê um modelo de maturidade de controles internos que ilustram a maturidade de uma empresa em relação ao estabelecimento e performance dos controles internos. Às vezes a análise é iniciada em resposta a vários direcionamentos externos, mas preferencialmente deve ser inserida e documentada pelos processos PO6 Comunicar as Diretrizes e Expectativas da Diretoria e ME2 Monitorar e Avaliar os Controles Internos do COBIT.

Capacidade, cobertura e controle são todas a dimensões do processo de maturidade, como ilustrado na **figura 14.**

Figura 14 - As três Dimensões da Maturidade



O modelo de maturidade é uma forma de medir quão bom os processos de gerenciamento são, ou seja, quão capazes eles são. O quanto devem ser desenvolvidos ou capacitados deveria primariamente depender dos objetivos de TI e sua conexão como as necessidades de negócios que eles suportam. O quanto dessa capacidade é realmente entregue depende largamente do retorno que a organização deseja do investimento. Por exemplo, existem processos e sistemas críticos que precisam de um gerenciamento da segurança maior e mais restrito do que outros que são menos críticos. Por outro lado, o grau de sofisticação dos controles que precisam ser aplicados em um processo é mais direcionado pelo apetite de risco da organização e pelos requisitos aplicáveis de conformidade.

A escala do modelo de maturidade ajudará os profissionais a explicar aos gerentes onde existem deficiências no gerenciamento do processo de TI e definir metas de onde querem estar. O correto nível de maturidade será influenciado pelos objetivos de negócios, o ambiente operacional e as práticas do mercado. Especificamente, o nível de maturidade gerencial dependerá da dependência da empresa em TI, de sua sofisticação tecnológica e, mais importante, do valor da informação.

Um ponto de referência estratégico para uma empresa aprimorar o gerenciamento e o controle dos processos de TI pode ser encontrado ao se atentar para os recentes padrões internacionais e boas práticas reconhecidas. As práticas mais atuais podem se tornar o nível esperado de performance para o futuro e portanto são úteis para planejar onde a empresa espera estar com o passar do tempo.

Os modelos de maturidade são construídos a partir do modelo qualitativo genérico (veja **Figura 13**) no qual os princípios dos seguintes atributos são adicionados de maneira crescente através dos níveis:
- Consciência e comunicação
- Políticas, planos e procedimentos
- Ferramentas e automação
- Habilidades e especialização
- Responsabilidade e responsabilização
- Definição de objetivos e medição

A tabela de atributos de maturidade na **Figura 15** relaciona as características de como os processos de TI são gerenciados e descreve como eles evoluem de um processo inexistente para um otimizado. Esses atributos podem ser usados para uma avaliação mais abrangente, análise de deficiências e plano de aprimoramento.

Em resumo, os modelos de maturidade fornecem um perfil genérico de estágios através dos quais cada empresa pode evoluir em gerenciamento e controle de processos de TI. Eles são:
- Um conjunto de requisitos e aspectos que habilitam os diferentes níveis de maturidade
- Uma escala onde a diferença pode ser facilmente medida
- Uma escala que pode ser utilizada para comparações pragmáticas
- Uma base para definir as posições "como está" e de "como será"
- Suporte para a análise de deficiências a fim de determinar o que precisa ser feito para atingir o nível escolhido
- Considerada no conjunto, uma visão de como a área de TI é gerenciada na organização

Os modelos de maturidade do CobiT enfocam a maturidade mas não necessariamente a abrangência e profundidade dos controles. Eles não são um número para ser atingido, tampouco são desenhados para ser uma base formal de certificação com níveis que criam requisitos mínimos difíceis de atingir. No entanto, são desenhados para serem sempre aplicáveis, fornecendo níveis com descrições que uma empresa pode reconhecer como os que melhor se adequam aos seus processos. O nível correto é determinado pelo tipo de organização, ambiente e estratégia.

A abrangência e a profundidade do controle e como a capacidade é utilizada e entregue são decisões de custo-benefício. Por exemplo, um alto nível de gerenciamento de segurança pode ter que ser enfatizado apenas nos sistemas mais críticos da organização. Outro exemplo seria a escolha entre uma revisão semanal e um controle contínuo automatizado.

Finalmente, embora altos níveis de maturidade aumentem o controle sobre os processos, a organização ainda precisa analisar, com base nos riscos e direcionamento de valor, quais mecanismos devem ser aplicáveis. Os objetivos genéricos de negócios e de TI definidos nessa metodologia ajudarão na análise. Os mecanismos de controle são guiados pelos objetivos de controle do CobiT e enfocam o que é feito no processo; os modelos de maturidade primariamente focam em quão bem os processos são gerenciados. O Apêndice III apresenta um modelo de maturidade genérico que demonstra o estágio do ambiente de controle e o estabelecimento de controles internos de uma empresa.

Um ambiente de controle apropriadamente implementado é obtido quando se observam todos os três aspectos da maturidade (capacidade, abrangência e controle). Melhorar a maturidade reduz riscos e aprimora a eficiência, levando a uma menor quantidade de erros, processos mais previsíveis e uso eficiente dos recursos sob o ponto de vista de custos.

MEDIÇÃO DE PERFORMANCE

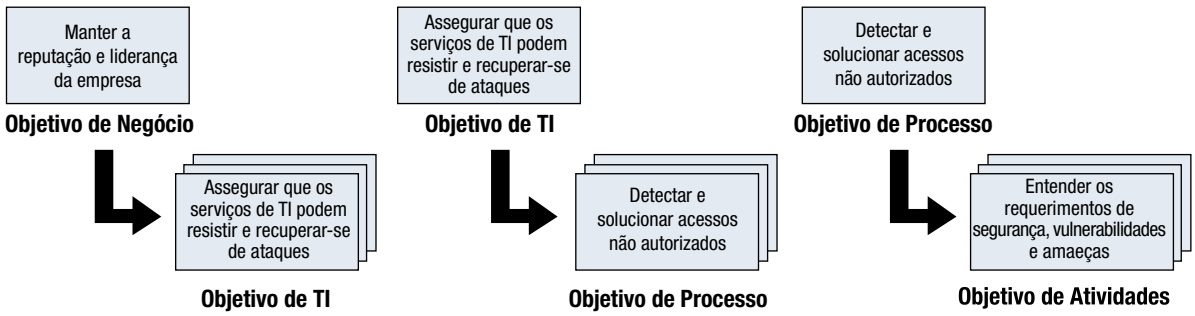
Os objetivos e métricas são definidos no CobiT em três níveis:
- Objetivos e métricas de TI que definem o que os negócios esperam de TI e como medir isso
- Objetivos e métricas dos processos que definem o que os processos de TI precisam entregar para suportar os objetivos de TI e como medir isso
- Objetivos e métricas de atividades que estabelecem o que precisa acontecer dentro do processo para atingir a requerida performance e como medir isso

Consciência e Comunicação	Políticas, Planos e Procedimentos	Ferramentas e Automação	Habilidades e Especialização	Responsabilidade e Responsabilização	Definição de Objetivos e Métricas
1 Reconhecimento da necessidade do processo está surgindo. Existe uma comunicação esporádica das questões.	Existem enfoques *ad hoc* para processos e práticas. O processo e as políticas são indefinidas.	Algumas ferramentas podem existir; o uso é baseado em ferramentas padrões de microinformática. Não existe um enfoque planejado para uso de ferramentas.	Habilidades requeridas para o processo não são identificadas. Um plano de treinamento não existe e não ocorre treinamento formal.	Não existe definição de responsabilização e responsabilidade. Pessoas assumem propriedade de questões baseadas em suas próprias iniciativas de maneira reativa.	Os objetivos não são claros e não são utilizadas métricas.
2 Existe consciência da necessidade de agir. A gerencia comunica as questões genéricas.	Processos similares e comuns surgem, mas são amplamente intuitivos devido a habilidades individuais. Alguns aspectos do processo são repetíveis, podendo existir alguma documentação e entendimento informal da política e procedimentos.	Existe um enfoque comum para o uso de ferramentas mas está baseado em soluções desenvolvidas por pessoas chaves. Ferramentas de mercado podem ter sido adquiridas, mas provavelmente não utilizadas corretamente e podem ser de mercado.	Habilidades mínimas requeridas para áreas críticas são identificadas. Treinamento provido em resposta a necessidades, ao invés de baseado num plano concordado, ocorre treinamento informal baseado no dia-a-dia de trabalho.	Indivíduos assumem sua responsabilidade e são usualmente responsabilizados, mesmo que isto não esteja formalmente acordado. Existe confusão sobre responsabilidades quando ocorrem problemas e uma cultura de acusação tende a existir.	Alguma definição de objetivos ocorre; algumas métricas financeiras são estabelecidas mas são conhecidas somente pelos executivos. Existe um monitoramento inconsistente em áreas isoladas.
3 Existe um entendimento da necessidade de agir. O gerenciamento é mais formal e estruturado em sua comunicação.	O uso de boas práticas surge. O processo, políticas e procedimentos são definidos e documentados para todas as atividades chaves.	Foi definido um plano para o uso e padronização de ferramentas para automatizar o processo. Ferramentas são utilizadas para seus propósitos básicos, mas pode não ser totalmente de acordo com o plano concordado e podem não ser integradas entre si.	As habilidades requeridas são definidas e documentadas para todas as áreas. Um plano formal de treinamento foi desenvolvido, mas o treinamento formal ainda é baseado em iniciativas individuais.	A responsabilidade e responsabilização por processos estão definidas e proprietários de processos são identificados. O proprietário do processo possivelmente não tem total autoridade para exercer suas responsabilidades.	Alguns objetivos efetivos e métricas são definidos, mas não são comunicados e existe uma clara ligação com os objetivos de negócios. Processos de mensuração surgem mas não são consistentemente aplicados. Idéias relacionadas a um balanced scorecard de TI são adotadas, como a aplicação intuitiva de análise de causa de problemas.
4 Existe um entendimento de todos os requerimentos. Técnicas de comunicação maduras são aplicadas e ferramentas de comunicação padrão são utilizadas.	O processo é sólido e completo; boas práticas internas são aplicadas. Todos aspectos do processo são documentados e repetíveis. Políticas foram aprovadas e assinadas pela gerencia. Padrões para desenvolvimento e manutenção de processos e procedimentos são adotados e seguidos.	Ferramentas são implementadas de acordo com um plano padrão e algumas foram integradas com outras ferramentas relacionadas. Ferramentas são usadas nas principais áreas para automatizar o gerenciamento de processos e monitoramento de atividades e controles críticos.	Habilidades requeridas para todas as áreas são rotineiramente atualizadas, capacitação é assegurada para todas áreas críticas e certificações são encorajadas. Técnicas de treinamento maduras são aplicadas de acordo com o planejado e o compartilhamento de informação é encorajado. Todos especialistas internos são envolvidos e a efetividade do plano de treinamento é avaliada.	A responsabilidade e responsabilização são aceitas e funcionam de uma forma que habilita os proprietários de processos a executarem suas responsabilidades. A cultura de recompensas em uso motiva ações positivas.	Eficiência e efetividade são medidas e comunicadas, ligadas com os objetivos de negócios e com o plano estratégico de TI. O balanced scorecard de TI foi implementado em algumas áreas com exceções observadas pela gerencia e análises de causas de problemas são padronizadas. O aprimoramento contínuo está surgindo.
5 Existe um entendimento avançado dos requerimentos. Existe uma comunicação proativa das questões baseado em tendências, técnicas de comunicação maduras são aplicadas e ferramentas integradas são utilizadas.	Boas práticas externas e padrões são aplicadas. A documentação de processos evoluiu para ferramentas automatizadas de trabalho. Processos, políticas e procedimentos são padronizados e integrados para possibilitar o gerenciamento e aprimoramento.	Um conjunto de ferramentas padronizadas são usadas em toda empresa. Ferramentas são totalmente integradas com outras ferramentas integradas para suportar os processos de maneira completa. Ferramentas são usadas para suportar o aprimoramento do processo e automaticamente detectar exceções dos controles.	A organização formalmente encoraja a melhoria contínua de habilidades, baseado numa clara definição dos objetivos pessoais e organizacionais. Boas práticas externas para treinamento e educação são usadas, bem como conceitos e técnicas de ponta. O compartilhamento do conhecimento é uma cultura da empresa e sistemas baseados em conhecimento estão sendo entregues. Especialistas externos e líderes de mercado são utilizados para orientação.	Proprietários de processos recebem poder necessário para fazer decisões e agir. A aceitação da responsabilidade foi cascateada na inteira organização de uma maneira consistente.	Existe um sistema de mensuração de performance integrado ligando a performance de TI com os objetivos de negócio, através da aplicação geral do *balanced scorecard* de TI. Exceções são ampla e consistentemente observadas pela gerência e a análise de causa de problemas é aplicada. Contínua melhoria é um modo de vida.

Figura 15 - Tabela de Atributos de Maturidade

Os objetivos são definidos de cima para baixo de maneira que os objetivos de negócios determinarão vários objetivos de TI que irão suportá-los. Um objetivo de TI é atingido através de um processo ou por interação de um determinado número de processos. Portanto, os objetivos de TI ajudam em diferentes objetivos de processos. Por sua vez, cada objetivo de processo requer um determinado número de atividades estabelecendo assim os objetivos da atividade. A figura 16 fornece um exemplo do relacionamento dos objetivos de negócios, TI, processos e atividades.

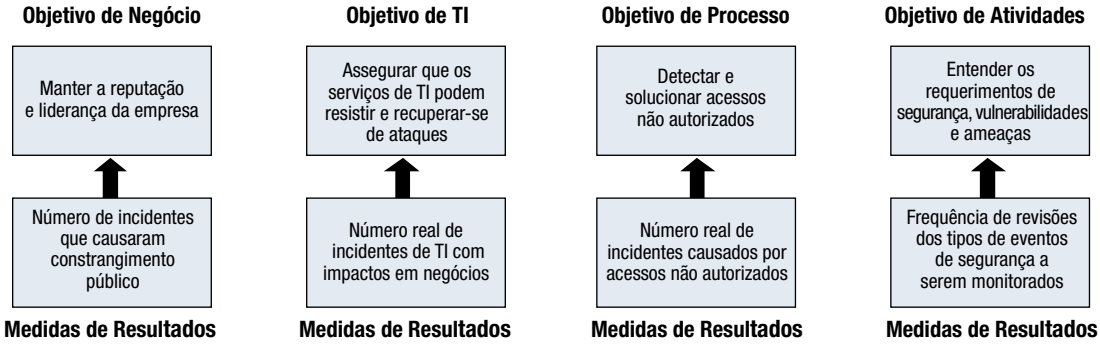
Figura 16 - Exemplo de Relacionamento de Objetivos



Os termos KGI e KPI usados em versões prévias do CobiT foram trocados por 2 tipos de métricas:

- Medidas de resultados (saídas), anteriormente indicadores-chaves de objetivos (KGIs), indicam se os objetivos foram atingidos. Esses podem ser medidos somente após os fatos e portanto são chamados de indicadores históricos *(lag indicators)*.
- Indicadores de performance, anteriormente indicadores-chaves de performance (KPIs), indicam se os objetivos serão possivelmente atingidos. Eles são medidos antes que os resultados sejam claros e portanto são chamados de indicadores futuros *(lead indicators)*.

Figura 17 - Possível Medida do Resultado para o Exemplo na Figura 16



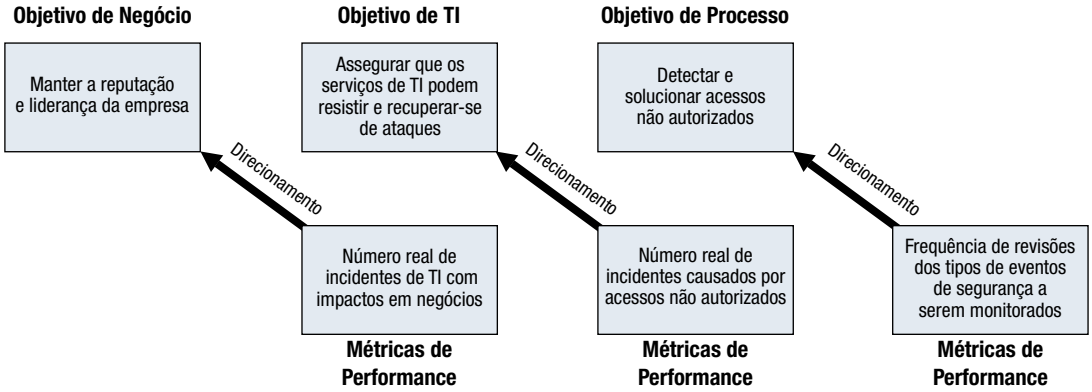
As medidas de resultados no nível menor tornam-se indicadores de performance para o nível maior. Como exemplificado na figura 16, uma medida de resultado indicando que a detecção e a solução de um acesso não autorizado estão nas metas irá também indicar que muito provavelmente os serviços de TI podem resistir a ataques e se recuperar deles. As medidas de resultados tornam-se um indicador de performance para o objetivo de nível superior. A Figura 18 ilustra como as medidas de resultados do exemplo tornam-se métricas de performance.

As medidas de resultados obtidas definem as medições que informam a gerência, depois dos fatos, se a função, os processos e a atividade de TI atingiram seus objetivos. Os medidores de resultados de funções de TI às vezes são expressos em termos de critérios de informação:

- Disponibilidade da informação necessária para suportar as necessidades de negócios
- Ausência de riscos de integridade e confidencialidade
- Eficiência de custos de processos e operação
- Confirmação de fidedignidade, efetividade e conformidade

Os indicadores de performance definem as medidas que determinam quão bem negócios, função de TI ou processo de TI estão sendo executados para permitir que os objetivos sejam atingidos. Eles são indicadores futuros ,*"lead indicators"*, quanto a se os objetivos serão atingidos, direcionando portanto os objetivos de maior nível. Eles às vezes medem a disponibilidade de apropriadas capacidades, práticas e habilidades, bem como os resultados de atividades relacionadas. Por exemplo, um serviço entregue por TI é um objetivo para TI mas é um indicador de performance e de capacidade para o negócio. É por isso que os indicadores de performance às vezes são chamados de direcionadores de performance, particularmente nos *"balanced scorecards"*.

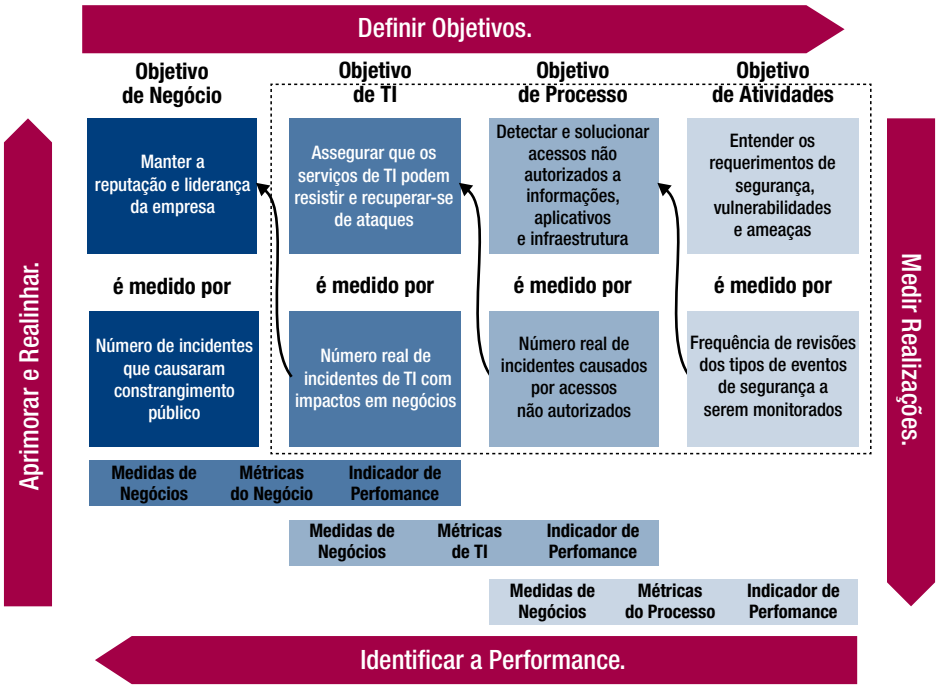
Figura 18 - Possíveis Direcionadores de Performance para o Exemplo na Figura 16



Portanto as métricas providas são tanto uma medida de resultados obtidos de uma função de TI, processo ou atividade de TI que elas medem, quando um indicador de performance direcionando um objetivo de maior nível de negócios, função de TI ou processo de TI.

A **Figura 19** ilustra o relacionamento entre os objetivos de negócios, TI, processos e atividades e suas diferentes métricas. Do canto superior esquerdo ao canto superior direito, são ilustrados os objetivos em cascata. Abaixo do objetivo está demonstrada a medida de resultados. As setas menores mostram que a mesma métrica é um indicador de performance para um objetivo de maior nível.

Figura 19 - Relacionamento entre Processos, Objetivos e Métricas (DS5)



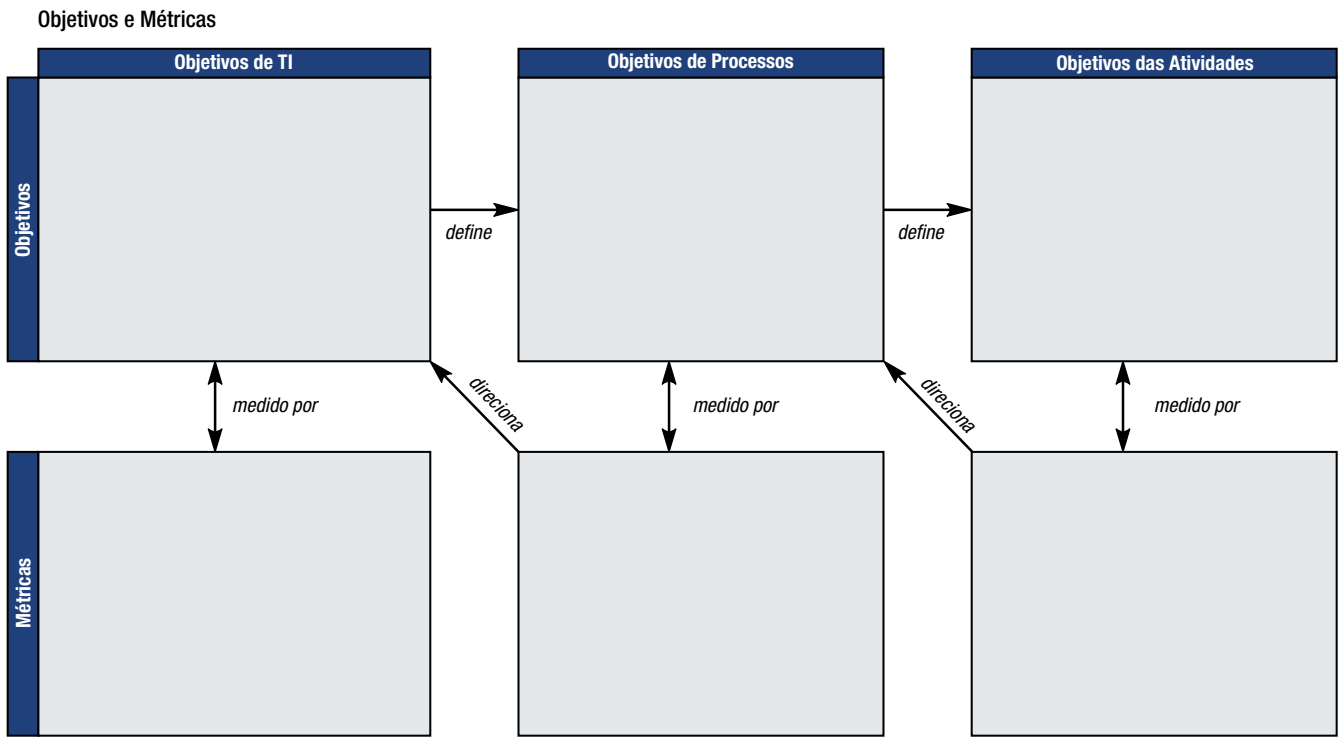
O exemplo acima provem do DS5 Garantir a segurança dos serviços. O CobiT oferece métricas somente para os resultados obtidos dos objetivos de TI como delineado pelas linhas tracejadas. Embora eles também são indicadores de performance de TI para os objetivos de negócios, o CobiT não fornece medidas de resultados para objetivos de negócios.

Os objetivos de negócios e de TI usados na seção de objetivos e métricas do CobiT, incluindo o seu relacionamento, são apresentados no Apêndice I. Para cada processo de TI no CobiT os objetivos e métricas são apresentados como indicado na figura 20.

As métricas foram desenvolvidas com as seguintes características em mente:

- Um índice elevado de preocupação com resultados versus o esforço (i.e., atenção na performance e em atingir os objetivos quando comparado com o esforço para capturá-los)
- Internamente comparável (i.e. um percentual de uma base ou números no tempo)
- Comparável externamente independente do tamanho da empresa ou mercado de atuação
- É melhor ter algumas boas métricas (pode até ser uma muito boa que poderia ser influenciada por diferentes meios) do que uma longa lista de métricas de baixa qualidade.
- Fácil de mensurar, não sendo confundida com metas

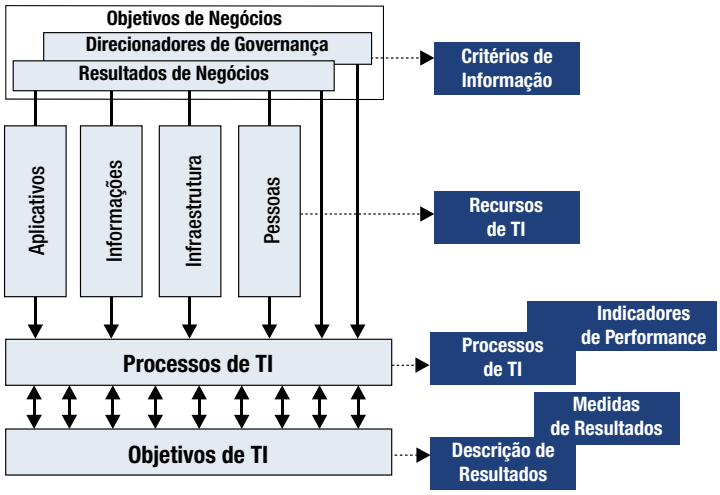
Figura 20 - Apresentação dos Objetivos e Métricas



A Estrutura do modelo CobiT

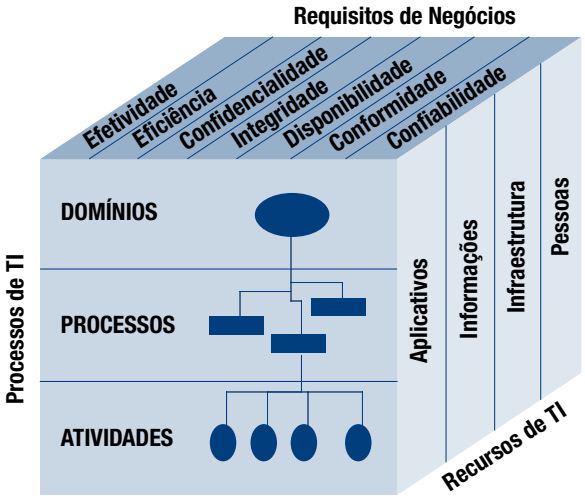
O modelo CobiT une os requisitos de negócios para informação e governança aos objetivos da função de serviços de TI. O modelo de processos do CobiT permite que as atividades de TI e os recursos que as suportam sejam serem apropriadamente gerenciados e controlados com base nos objetivos de controle de CobiT, bem como alinhados e monitorados usando os objetivos e métricas do CobiT, como ilustrado na **Figura 21**.

Figura 21 - Gerenciamento, Controle, Alinhamento e Monitoramento do CobiT



Em resumo, os recursos de TI são gerenciados pelos processos de TI para atingir os objetivos de TI que respondem aos requisitos de negócios. Este é o princípio básico do modelo CobiT, como ilustrado pelo cubo do CobiT (**Figura 22**).

Figura 22 - Figura do COBIT



Em maiores detalhes, todo o modelo COBIT pode ser mostrada graficamente como demonstrado na **figura 23**, com o modelo de processos do COBIT de 4 domínios contendo 34 processos genéricos, gerenciando os recursos de TI para entregarem as informações para a área de negócios de acordo com os requerimentos de negócios e governança.

Aceitabilidade Geral do COBIT

O COBIT é baseado na análise e na harmonização dos padrões e boas práticas de TI existentes, adequando-se aos princípios de governança geralmente aceitos. Ele está posicionado em alto nível, direcionado por requisitos de negócios, abrange todas as atividades de TI e concentra-se no *que* deveria ser obtido e não em *como* atingir uma efetiva governança, gerenciamento e controle. Sendo assim, ele age como um integrador das práticas de governança de TI e influencia a Alta Direção, gerências de negócios e de TI, profissionais de governança, avaliação e segurança, profissionais de auditoria de TI e de controles. Ele é desenhado para ser complementar e utilizado com outros padrões e boas práticas.

A implementação de boas práticas deve ser consistente com a governança e o ambiente de controle da organização, apropriado para a organização e integrada a outros métodos e práticas utilizadas. Padrões e boas práticas não são uma panacéia. Sua efetividade depende d como foram implementados e mantidos atualizados. Eles são mais úteis quando aplicados como um conjunto de princípios e um ponto de partida para produzir procedimentos específicos. Para evitar que as práticas fiquem só no papel, a gerência e os funcionários devem entender o que fazer, como fazer e porque isso é importante.

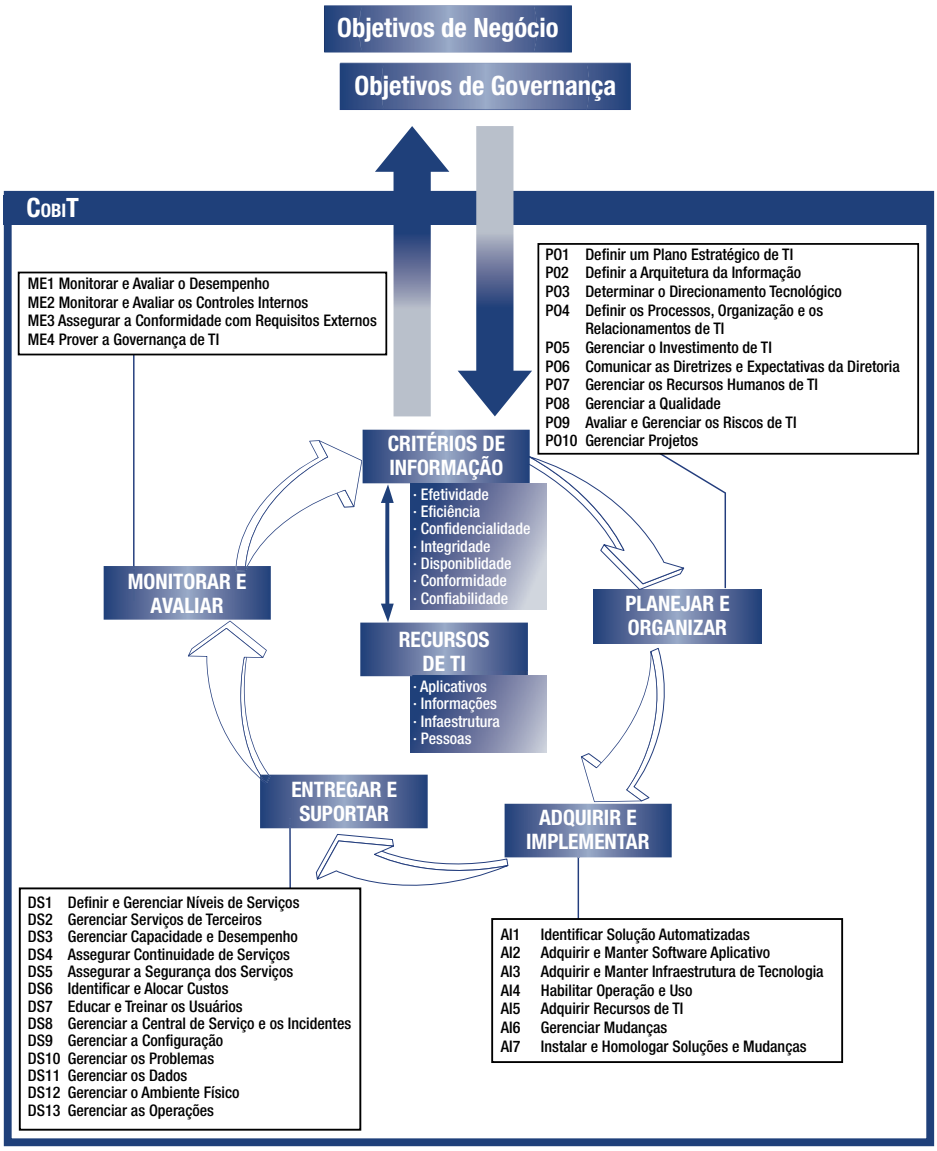
Para atingir o alinhamento das boas práticas com os requisitos de negócios é recomendável que o COBIT seja utilizado num alto nível, provendo uma metodologia de controle geral com base em um modelo de processos de TI que deve servir genericamente para toda empresa. Práticas específicas e padrões cobrindo áreas específicas podem ser mapeados com a metodologia COBIT, provendo assim um material de orientação.

O COBIT influencia diferentes usuários:
- **Alta Direção:** Para obter valor dos investimentos de TI, balancear os riscos e controlar o investimento em um ambiente de TI às vezes imprevisível
- **Executivos de negócios:** Para assegurar que o gerenciamento e o controle dos serviços de TI oferecidos internamente e por terceiros estejam funcionando de modo adequado
- **Executivos de TI:** Para prover os serviços de TI de que o negócio precisa para suportar a estratégia de negócios de maneira controlada e gerenciada
- **Auditores:** Para substanciar suas opiniões e/ou prover recomendações sobre controles internos para os executivos

O COBIT foi desenvolvido e é mantido por um instituto de pesquisa independente e sem fins lucrativos, contando com a experiência de seus membros associados, especialistas e profissionais de controle e segurança. O seu conteúdo baseia-se em uma contínua pesquisa das boas práticas de TI e é atualizado continuamente, provendo um recurso objetivo e prático para todos os tipos de usuários.

O COBIT é orientado para os objetivos e escopo da governança de TI, assegurando que a metodologia de controle seja compreensiva, alinhada com os princípios de governança de organizações e, portanto, aceitável para Alta Direção, executivos, auditores e reguladores. Um mapa demonstrando como os objetivos de controles do COBIT são mapeados com as cinco áreas de foco da governança de TI e das atividades de controle do COSO é demonstrado no Apêndice II.

Figura 23 - Visão Geral do Modelo do CobiT



A **Figura 24** resume como os vários elementos do modelo CobiT podem ser mapeados com as áreas de foco de governança de TI.

Figura 24 - Modelo CobiT e as Áreas Foco da Governança de TI

	Objetivos	Métricas	Práticas	Modelos de Maturidade
Alinhamento Estratégico	P	P		
Entrega de Valor		P	S	P
Gerenciamento de Risco		S	P	S
Gerenciamento de Recursos		S	P	P
Gerenciamento de Performance	P	P		S

P = Ferramenta Primária S = Ferramenta Secundária

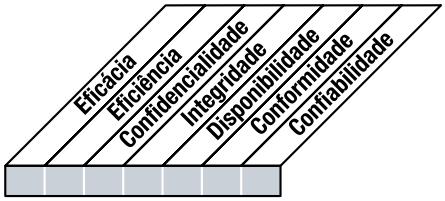
COMO UTILIZAR ESTE LIVRO

Navegação pelo Modelo COBIT

Para cada um dos processos de TI do COBIT é apresentado uma descrição em conjunto com os principais objetivos e métricas no formato de cascata (**Figura 25**).

Figura 25 - Navegação COBIT

Em cada processo de TI, são fornecidos objetivos de controle como declarações de ações genéricas com o mínimo de boas práticas gerenciais para garantir que o processo esteja mantido sob controle.



Controle sobre o seguinte processo de TI:

Nome do processo

que satisfaça aos seguintes requisitos do negócio para a TI:

sumário do objetivo de TI mais importante

com foco em:

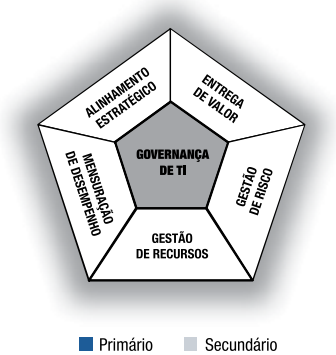
sumário dos objetivos de processos mais importantes

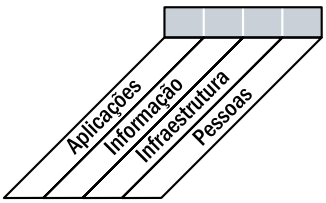
é alcançado por:

objetivos da atividade

e medido por:

métricas chaves





Visão Geral dos Principais Componentes do COBIT

O modelo COBIT é formado pelos seguintes componentes principais, apresentados no restante desta publicação e organizado por 34 processos de TI, mostrando uma visão geral de como controlar, gerenciar e mensurar cada processo. Cada processo é coberto por quatro seções e cada uma delas é apresentada em cerca de uma página, como segue:

- A seção 1 **(Figura 25)** contém uma descrição do processo que resume os objetivos do processo, apresentada no formato de cascata. Esta página também demonstra o mapeamento dos critérios de informação, recursos de TI e áreas de foco de governança de TI. A letra P indica um relacionamento primário e a letra S indica um secundário.
- A seção 2 apresenta os objetivos de controle desse processo.
- A seção 3 apresenta os processos de entrada e saída, tabela RACI, objetivos e métricas.
- A seção 4 apresenta o modelo de maturidade do processo.

Outro modo de visualizar a performance do processo é avaliar se:
· As entradas do processo são o que o proprietário do processo precisa dos outros.
· A descrição dos objetivos de controle do processo define o que o proprietário do processo deve fazer.
· As saídas do processo são aquelas que o proprietário do processo tem que entregar.
· Os objetivos e métricas demonstram como o processo deve ser medido.
· A tabela RACI define o que precisa ser delegado e para quem.
· O modelo de maturidade demonstra o que precisa ser feito para o aprimoramento.

As responsabilidades na tabela RACI são categorizadas para todos os processos, como segue:
· *Chief executive officer* (CEO)
· *Chief financial officer* (CFO)
· Executivo de Negócio
· *Chief information officer* (CIO)
· Proprietário do Processo de Negócio
· Chefe de Operações
· Responsável por Arquitetura
· Responsável por Desenvolvimento
· Responsável pela Administração de TI (nas grandes empresas, é o responsável por funções como recursos humanos, orçamentos e controles internos)
· *Project management officer* (PMO) ou função equivalente
· Conformidade, auditoria, riscos e segurança (grupos como responsabilidades por controles mas não de operações de TI)

Certos processos têm papéis especializados específicos do processo, por exemplo, gerenciar a central de serviços e os incidentes do DS8.

Deve ser observado que embora o material tenha sido coletado de centenas de especialistas, seguindo rigorosa pesquisa e revisão, as entradas, as saídas, as responsabilidades, as métricas e os objetivos são ilustrativos e não uma receita completa ou exaustiva. Eles fornecem uma base de conhecimento especializado a partir da qual cada organização deve selecionar o que se aplica de maneira eficiente e eficaz considerando-se a estratégia, os objetivos e as políticas da organização.

Os Usuários dos Componentes do CobiT

A gerência pode utilizar o material CobiT para avaliar os processos de TI usando as metas de negócios e as metas de TI detalhadas no Apêndice I para visando esclarecer dos processos de TI e os modelos de maturidade de processo para avaliar a performance atual.

Responsáveis pela implementação e auditores podem identificar os requisitos de controle aplicáveis a partir dos objetivos de controles e das responsabilidades pelas atividades apresentadas na tabela RACI associada.

Todos os usuários em potencial podem se beneficiar da utilização do conteúdo do CobiT como um enfoque geral para o gerenciamento e governança de TI em conjunto com os seguintes padrões mais detalhados:
· ITIL para entrega de serviços
· CMM para entrega de soluções
· ISO 17799 para segurança da informação
· PMBOK ou PRINCE2 para gerenciamento de projetos

Apêndices

As seguintes seções adicionais de referência estão disponíveis no final deste livro:
I. Tabelas Relacionando os Objetivos e Processos (três tabelas)
II. Mapeamento dos Processos de TI com as Áreas Foco de Governança de TI, COSO, Recursos de TI do CobiT e Critérios de Informação do CobiT
III. Modelo de Maturidade para Controles Internos
IV. Material de Referência Principal do CobiT
V. Referência cruzada entre a 3ª edição do CobiT e o CobiT 4.1
VI. Enfoque de Pesquisa e Desenvolvimento
VII. Glossário
VIII. O CobiT e os Produtos Relacionados

Planejar e Organizar

P01 Definir um Plano Estratégico de TI

P02 Definir a Arquitetura da Informação

P03 Determinar as Diretrizes de Tecnologia

P04 Definir os Processos, a Organização e os Relacionamentos de TI

P05 Gerenciar o Investimento de TI

P06 Comunicar Metas e Diretrizes Gerenciais

P07 Gerenciar os Recursos Humanos de TI

P08 Gerenciar a Qualidade

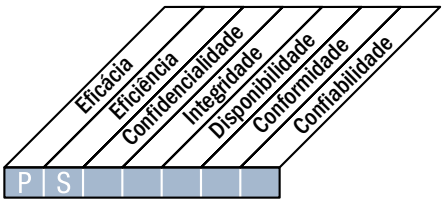
P09 Avaliar e Gerenciar os Riscos de TI

P010 Gerenciar Projetos

DESCRIÇÃO DE PROCESSO

PO1 Definir um Plano Estratégico de TI

O planejamento estratégico de TI é necessário para gerenciar todos os recursos de TI em alinhamento com as prioridades e estratégias de negócio. A função de TI e as partes interessadas pelo negócio são responsáveis por garantir a otimização do valor a ser obtido do portfólio de projetos e serviços. O plano estratégico deve melhorar o entendimento das partes interessadas no que diz respeito a oportunidades e limitações da TI, avaliar o desempenho atual e esclarecer o nível de investimento requerido. A estratégia e as prioridades de negócio devem ser refletidas nos portfólios e executadas por meio de planos táticos de TI que estabeleçam objetivos concisos, tarefas e planos bem definidos e aceitos por ambos, negócio e TI.



Controle sobre o seguinte processo de TI:

Definir um plano estratégico de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

sustentar ou estender a estratégia de negócio e os requisitos de governança e, ao mesmo tempo, ser transparente quanto aos benefícios, custos e riscos.

com foco em:

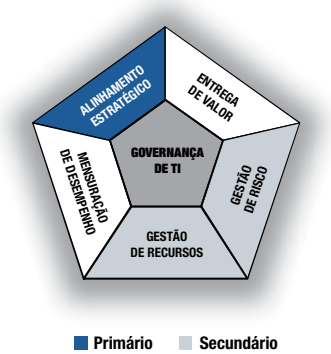
incorporar TI e gerenciamento de negócio na tradução dos requisitos de negócio em ofertas de serviços e no desenvolvimento de estratégias para entregar estes serviços de maneira eficaz e transparente.

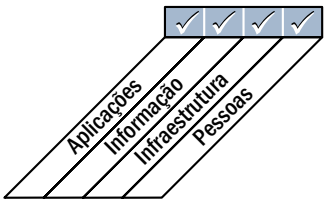
é alcançado por:

- Comprometimento da Alta Direção e da Direção do Negócio no alinhamento do planejamento estratégico de TI com as necessidades atuais e futuras;
- Entendimento da capacidade atual de TI;
- Estabelecimento de um esquema de priorização de objetivos de negócio, que quantifique os requisitos de negócio;

e medido por:

- Percentual dos objetivos de TI no plano estratégico de TI que sustentam o plano estratégico de negócio;
- Percentual de projetos no portfólio de projetos de TI que podem ser diretamente relacionados ao plano tático de TI;
- Demora entre a atualização do plano estratégico de TI e a atualização dos planos táticos de TI.





Objetivos de Controle Detalhados

PO1 Definir um Plano Estratégico de TI

PO1.1 Gerenciamento de Valor da TI
Trabalhar com a Direção do Negócio para assegurar que o portfólio de investimentos em TI da empresa contenha programas baseados em sólidos estudos de caso de negócio. Reconhecer que há investimentos obrigatórios, sustentáveis e discricionários que diferem em complexidade e grau de liberdade na alocação de fundos. Os processos de TI devem prover a entrega eficaz e eficiente dos componentes de TI e prévia advertência de qualquer desvio do plano, incluindo custo, cronograma ou funcionalidade, que possa afetar os resultados esperados dos programas. Os serviços de TI devem ser executados em conformidade com acordos de níveis de serviço (service level agreeement, SLA) equilibrados e controláveis. A responsabilidade pelo alcance dos benefícios e o controle dos custos deve ser claramente atribuída e monitorada. Estabelecer avaliação adequada, transparente, repetível e comparável de estudos de caso de negócio, incluindo valor financeiro, o risco de não fornecer uma capacidade e o risco de não atingir os benefícios esperados.

PO1.2 Alinhamento entre TI e Negócio
Estabelecer processos de educação bi-direcional e envolvimento recíproco no planejamento estratégico para atingir o alinhamento e a integração de negócios e TI. Mediar os imperativos de negócios e de TI para que as prioridades sejam mutuamente aceitas.

PO1.3 Avaliação da Capacidade e Desempenho Correntes
Avaliar a capacidade e o desempenho atuais das entregas de soluções e serviços para estabelecer um modelo com o qual os requisitos futuros podem ser comparados.
Definir o desempenho em termos da contribuição de TI com os objetivos de negócio, funcionalidades, estabilidade, complexidade, custos, pontos fortes e fragilidades.

PO1.4 Plano Estratégico de TI
Criar um plano estratégico que defina, em cooperação com as partes interessadas relevantes, como a TI contribuirá com os objetivos estratégicos da organização (metas) e quais os custos e riscos relacionados. Esse plano estratégico deve contemplar como a TI aplicará os programas de investimentos e como dará sustentação à entrega operacional de serviços. O plano deve definir como os objetivos serão atingidos e medidos e deve ser formalmente liberado para implementação pelas partes interessadas. O plano estratégico de TI deve contemplar o orçamento operacional e de investimento, as fontes de recursos financeiros, a estratégia de fornecimento, a estratégia de aquisição e requisitos legais e regulamentares. O plano estratégico deve ser suficientemente detalhado para possibilitar a definição dos planos táticos de TI.

PO1.5 Planos Táticos de TI
Criar um portfólio de planos táticos de TI derivados do plano estratégico de TI. Esses planos táticos devem descrever quais são as iniciativas de TI requeridas, quais os recursos necessários e como o uso de recursos e os benefícios alcançados serão monitorados e administrados. Os planos táticos devem ser suficientemente detalhados de forma a permitir o desenvolvimento de planos de projetos. Gerenciar ativamente o conjunto de planos e iniciativas táticas de TI através de análise do portfólio de projetos e serviços. Isso contempla o acompanhamento frequente de requisitos e recursos, comparando-os ao alcance de metas estratégicas e táticas e os benefícios esperados, e tomando-se as ações apropriadas em caso de desvios.

PO1.6 Gerenciamento do Portfólio de TI
Gerenciar ativamente com as áreas de negócio o portfólio dos programas de investimentos de TI necessários para atingir os objetivos estratégicos específicos de negócio, através de identificação, definição, avaliação, priorização, seleção, início, gerenciamento e controle de programas. Isso inclui esclarecer os resultados de negócio desejados, assegurar que os objetivos do programa sustentem o alcance dos resultados, entender o escopo completo do esforço necessário para atingir os resultados, atribuir responsabilidades com medidas de suporte, definir projetos dentro do programa, alocar recursos e fundos, delegar autoridade e atribuir responsabilidades pelos projetos no lançamento do programa.

Diretrizes de Gerenciamento

PO1 Definir um Plano Estratégico de TI

Origem	Entrada
PO5	Relatórios de custo/benefício;
PO9	Avaliação de riscos;
PO10	Portfólio de projetos de TI atualizado;
DS1	Requisitos novos ou atualizados de serviços; Portfólio de serviços de TI atualizado;
*	Estratégia e prioridades de negócios;
*	Portfólio de programas;
ME1	Informações de desempenho para planejamento de TI;
ME4	Relatórios de status de governança de TI; Direcionamento estratégico corporativo para TI

Saída	Destino						
Planejamento estratégico de TI;	PO2.....PO6		PO8	PO9	AI1	DS1	
Planejamento tático de TI;	PO2.....PO6			PO9	AI1	DS1	
Portfólio de projetos de TI;	PO5	PO6	PO10	AI6			
Portfólio de serviços de TI;	PO5	PO6	PO9	DS1			
Estratégia de fornecimento de TI;	DS2						
Estratégia de aquisição de TI	AI5						

Tabela RACI

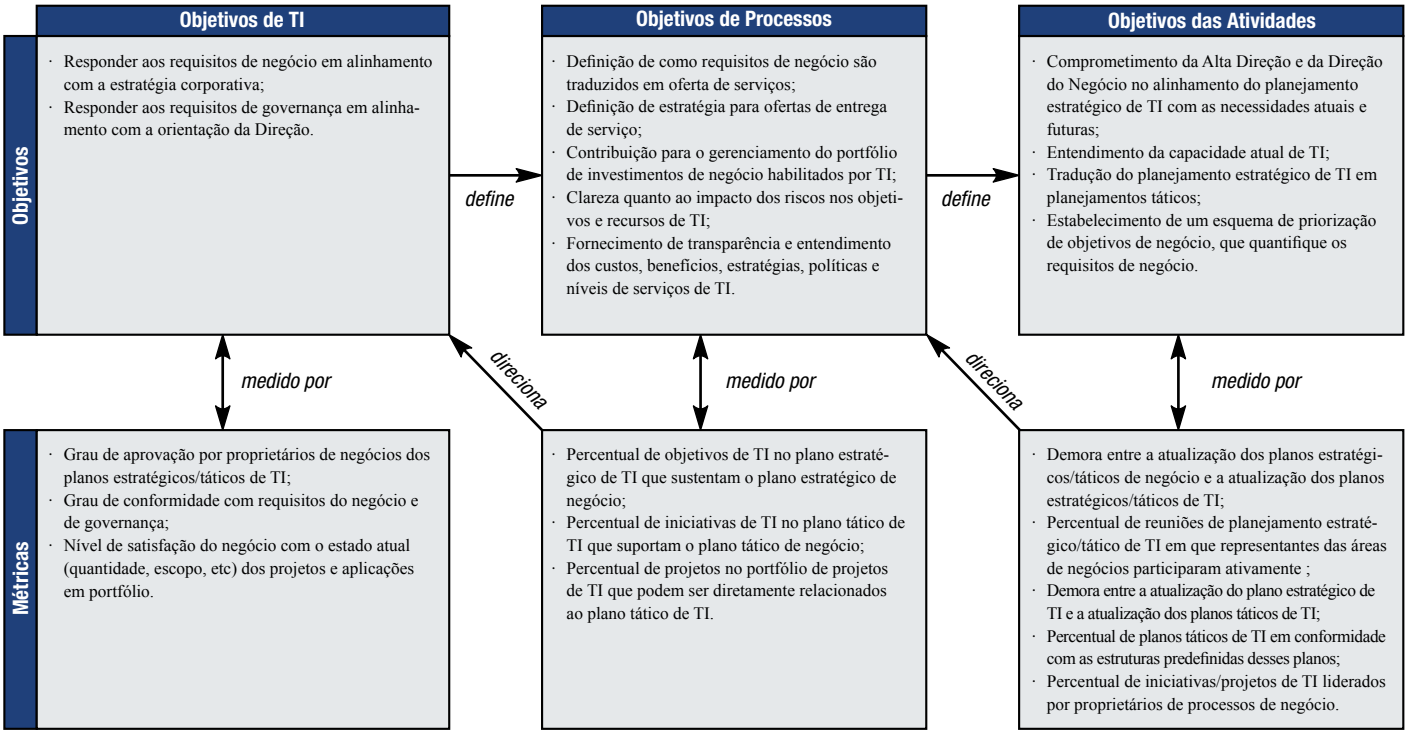
Funções

Atividades

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Vincular objetivos de negócio com objetivos de TI;	C	I	A/R	R	C						
Identificar as dependências críticas e o desempenho atual;	C	C	R	A/R	C	C	C	C	C		C
Produzir um plano estratégico de TI;	A	C	C	R	I	C	C	C	C	I	C
Produzir um plano tático de TI;	C	I		A	C	C	C	C	C	R	I
Analisar o portfólio de programas e gerenciar portfólio de projetos e serviços	C	I	I	A	R	R	C	R	C	C	I

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado (I).* Nota de tradução: (R) Responsible, (A) Accountable

Objetivos e Métricas



Modelo de Maturidade

PO1 Definir um Plano Estratégico de TI

O gerenciamento do processo de ***"Definir um plano estratégico de TI"*** que satisfaça ao requisito do negócio para a TI de ***"sustentar ou estender a estratégia de negócio e requisitos de governança e, ao mesmo tempo, ser transparente quanto aos benefícios, custos e riscos"*** é:

0 Inexistente quando
O plano estratégico de TI não é executado. A Direção não está conscientizada de que o planejamento estratégico de TI é necessário para sustentar as metas de negócio.

1 Inicial/ *Ad hoc* quando
A necessidade de um planejamento estratégico de TI é conhecida pela Direção de TI. O planejamento de TI é realizado caso a caso, em resposta a um requisito específico de negócio. O planejamento estratégico de TI é ocasionalmente discutido nas reuniões da Direção de TI. O alinhamento de requisitos de negócio, aplicações e tecnologia ocorre de forma reativa ao invés de seguir uma estratégia corporativa. A posição estratégica de risco é identificada informalmente projeto a projeto.

2 Repetível, porém Intuitivo quando
O planejamento estratégico de TI é compartilhado com a Direção do Negócio conforme a necessidade. A atualização dos planos de TI acontece em resposta aos pedidos da Direção. As decisões estratégicas são tomadas projeto a projeto, sem consistência com uma estratégia corporativa. Os riscos e benefícios do usuário nas principais decisões estratégicas são determinados de forma intuitiva.

3 Processo Definido quando
Uma política define quando e como realizar um planejamento estratégico de TI. O planejamento estratégico de TI segue uma abordagem estruturada, que é documentada e conhecida por todo o pessoal envolvido. O processo do planejamento de TI é razoavelmente discutido e assegura que um planejamento adequado seja realizado. Entretanto, a implementação do processo fica a critério de cada Direção e não há procedimentos para examinar o processo. A estratégia geral de TI inclui uma definição consistente dos riscos que a organização aceita correr por ser inovadora ou por seguir tendências. As estratégias de recursos financeiros, técnicos e humanos influenciam cada vez mais na aquisição de novos produtos e tecnologias. O planejamento estratégico de TI é discutido nas reuniões de gerenciamento do negócio.

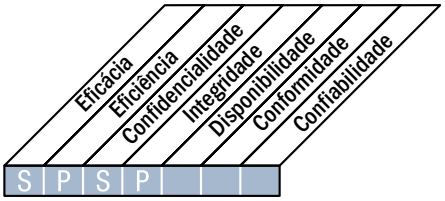
4 Gerenciado e Mensurável quando
O planejamento estratégico de TI é uma prática padrão cujas exceções são detectadas pela Direção. O planejamento estratégico de TI é uma função da Direção com nível sênior de responsabilidade. A Direção é capaz de monitorar o processo de planejamento estratégico de TI, tomar decisões baseadas nesse processo e medir sua efetividade. Os planejamentos de TI, de curto e longo prazo são cascateados de cima para baixo na organização, com atualizações quando necessário. A estratégia de TI e a estratégia global da organização estão se tornando gradativamente mais coordenadas por abordar processos de negócio, capacidades de valor agregado e alavancar o uso de aplicativos e tecnologias na reengenharia dos processos de negócios. Há um processo bem definido para determinar o uso dos recursos internos e externos no desenvolvimento de sistema e operações.

5 Otimizado quando
O planejamento estratégico de TI é um processo documentado e dinâmico, sempre considerado no estabelecimento dos objetivos de negócio, e resulta em valor de negócio identificável através dos investimentos em TI. As considerações de risco e o valor agregado são continuamente atualizados no processo de planejamento estratégico de TI. Planos realísticos de TI de longo prazo são desenvolvidos e constantemente atualizados para refletir mudanças na tecnologia e no desenvolvimento relativos ao negócio. Comparações com normas confiáveis e bem conhecidas do mercado são realizadas e integradas ao processo de formulação de estratégias *(benchmarking)*. O planejamento estratégico inclui uma análise de como as novas tecnologias podem criar novas capacidades de negócio e melhorar a vantagem competitiva da organização.

DESCRIÇÃO DE PROCESSO

P02 Definir a Arquitetura da Informação

Os sistemas de informação devem criar e atualizar regularmente um modelo de informação do negócio e definir os sistemas apropriados para otimizar o uso dessa informação. Isso abrange o desenvolvimento de um dicionário de dados corporativo com as regras de sintaxe de dados, o esquema de classificação de dados e os níveis de segurança da organização. Esse processo melhora a qualidade de decisão do gerenciamento certificando-se de que informações seguras e confiáveis sejam fornecidas e permite racionalizar os recursos de sistemas de informação para atender às estratégias de negócio de forma apropriada. Esse processo de TI também é necessário para permitir um maior grau de responsabilização pela integridade e a segurança dos dados e melhorar a efetividade e o controle do compartilhamento da informação através das aplicações e entidades.



Controle sobre o seguinte processo de TI:

Definir a arquitetura da informação

que satisfaça aos seguintes requisitos do negócio para a TI:

ser ágil em atender aos requisitos, fornecer informação confiável e consistente e integrar completamente as aplicações nos processos de negócio

com foco em:

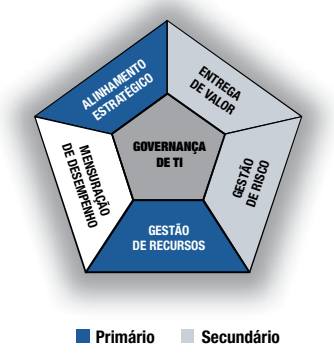
estabelecer um modelo de dados de negócio que incorpore um esquema de classificação de dados para assegurar integridade e consistência de todos os dados

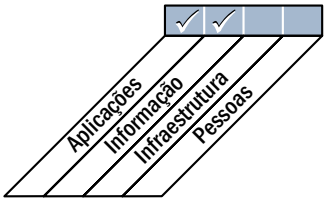
é alcançado por:

- Garantia da precisão da arquitetura da informação e do modelo de dados
- Estabelecimento da propriedade dos dados
- Classificação da informação utilizando um esquema de classificação acordado

e medido por:

- Percentual de elementos de dados redundantes ou duplicados
- Percentual de aplicações que não estão em conformidade com a arquitetura da informação
- Frequência de atividades de validação dos dados





OBJETIVOS DE CONTROLE DETALHADOS

PO2 Definir a Arquitetura da Informação

PO2.1 Modelo de Arquitetura da Informação da Organização
Estabelecer e manter um modelo de informação da organização que permita o desenvolvimento de aplicações e atividades de apoio à decisão consistentes com os planos de TI, conforme descrito no PO1. O modelo facilita a criação, o uso e o compartilhamento otimizados da informação pelo negócio para manter a integridade e ser flexível, funcional, com boa relação custo-benefício, rápido, seguro e resistente a falhas.

PO2.2 Dicionário de Dados Corporativos e Regras de Sintaxe de Dados
Manter um dicionário de dados corporativos que incorpore as regras de sintaxe de dados da organização. Este dicionário permite o compartilhamento dos elementos de dados entre aplicativos e sistemas, promove um entendimento comum de dados entre a TI e os usuários do negócio, e previne a criação de elementos de dados incompatíveis.

PO2.3 Esquema de Classificação de Dados
Estabelecer um esquema de classificação de dados aplicável a toda a organização com base na importância e na confidencialidade dos dados corporativos (por exemplo: público, confidencial, altamente secreto). Esse esquema inclui detalhes sobre os proprietários dos dados, definição de níveis apropriados de segurança, controle de proteção, uma breve descrição dos requisitos de retenção e destruição dos dados, importância e confidencialidade. É utilizado como base para aplicação de controles, tais como controles de acesso, arquivamento ou criptografia.

PO2.4 Gerenciamento de Integridade
Definir e implementar procedimentos que assegurem a integridade e consistência de todos os dados armazenados na forma eletrônica, tais como banco de dados, data warehouses e arquivos de dados.

Diretrizes de Gerenciamento

PO2 Definir a Arquitetura da Informação

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI;
AI1	Estudo de viabilidade dos requisitos de negócio;
AI7	Revisão pós-implementação;
DS3	Informação de desempenho e capacidade;
ME1	Dados de desempenho para planejamento de TI

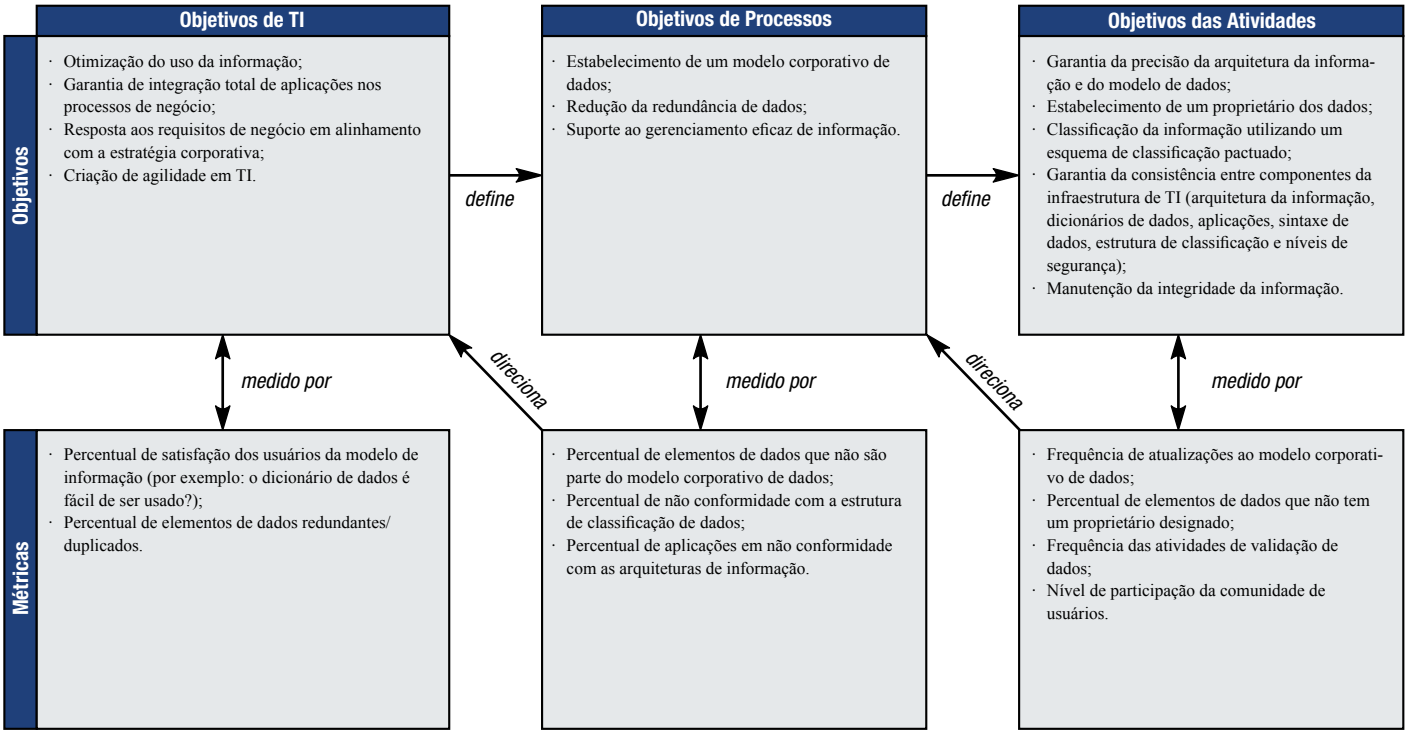
Saída	Destino						
Estrutura de classificação de dados;	AI2						
Plano otimizado de sistemas de negócio;	PO3	AI2					
Dicionário de dados;	AI2	DS11					
Arquitetura da informação;	PO3	DS5					
Classificações atribuídas a dados;	DS1	DS4	DS5	DS11	DS12		
Procedimentos e ferramentas de classificação	*						

Tabela RACI

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Criar e manter o modelo de informação corporativa;		C	I	A	C		R	C	C		C
Criar e manter os dicionários de dados corporativos;				I	C		A/R	R			C
Estabelecer e manter uma estrutura de classificação de dados;	I	C	A	C	C	I	C	C			R
Fornecer aos proprietários de dados procedimentos e ferramentas para classificação dos sistemas de informação;	I	C	A	C	C	I	C	C			R
Utilizar o modelo de informação, dicionário de dados e estrutura de classificação para planejar sistemas otimizados	C	C	I	A	C		R	C			I

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

PO2 Definir a Arquitetura da Informação

O gerenciamento do processo de ***"Definir a Arquitetura da Informação"*** que satisfaça ao requisito do negócio para a TI de ***"ser ágil em responder aos requisitos, fornecer informação confiável e consistente e integrar completamente as aplicações aos processos de negócio"*** é:

0 Inexistente quando
Não há conscientização da importância da arquitetura da informação na organização. O conhecimento, o parecer técnico e as responsabilidades necessárias para desenvolver esta arquitetura não existem na organização.

1 Inicial/ *Ad hoc* quando
A gerência reconhece a necessidade de uma arquitetura da informação. O desenvolvimento de alguns componentes de uma arquitetura da informação ocorre de forma *ad hoc*. As definições abrangem dados ao invés de informação e são direcionadas pelas ofertas de fornecedores de software aplicativo. Há comunicação esporádica e inconsistente sobre a necessidade de uma arquitetura da informação.

2 Repetível, porém Intuitivo quando
Um processo de arquitetura da informação começa a surgir e procedimentos similares, ainda que informais e intuitivos, são seguidos por diferentes pessoas dentro da organização. As pessoas adquirem habilidades em desenvolver arquitetura de informação através de experiências práticas e repetidas aplicações de técnicas. Requisitos táticos impulsionam o desenvolvimento de componentes da arquitetura da informação por indivíduos.

3 Processo Definido quando
A importância da arquitetura da informação é entendida e aceita e a responsabilidade por sua entrega é estabelecida e claramente divulgada. Os procedimentos, ferramentas e técnicas, embora não sofisticados, têm sido padronizados e documentados e fazem parte das atividades de treinamento informal. Foram desenvolvidas políticas básicas da arquitetura de informação, incluindo alguns requisitos estratégicos, porém a conformidade com políticas, padrões e ferramentas não é imposta de maneira consistente. Uma área de administração de dados foi recentemente definida e formalmente estabelecida, determinando os padrões organizacionais e dando início aos relatórios sobre a entrega e o uso da arquitetura de informação. Ferramentas automatizadas estão começando a ser empregadas, mas os processos e as regras utilizados são definidos por meio de ofertas de fornecedores de software de banco de dados. Atividades formais de treinamentos são definidas, documentadas e aplicadas consistentemente.

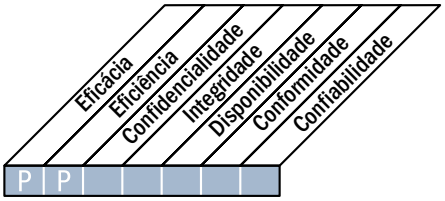
4 Gerenciado e Mensurável quando
O desenvolvimento e a imposição da arquitetura da informação são completamente sustentados por métodos e técnicas formais. A responsabilização pelo desempenho dos processos de desenvolvimento da arquitetura é imposta, e o sucesso da arquitetura de informação é medido. Ferramentas automáticas de apoio são difundidas amplamente, mas ainda não estão integradas. Métricas básicas foram identificadas, e foi estabelecido um sistema de mensuração. O processo de definição da arquitetura de informação é proativo e com foco no atendimento das necessidades futuras do negócio. A organização de administração dos dados está ativamente envolvida em todos os esforços de desenvolvimento de aplicações para assegurar consistência. Um repositório automatizado está completamente implementado. Modelos de dados mais complexos são implementados para alavancar a informação contida nos bancos de dados. Os sistemas de informações executivas e sistemas de apoio a decisões aproveitam a informação disponível.

5 Otimizado quando
A arquitetura da informação é imposta de forma consistente em todos os níveis da organização. O valor da arquitetura de informação é continuamente enfatizado no negócio. A equipe de TI tem a habilidade e a especialização necessárias para desenvolver e manter uma arquitetura de informação robusta e reativa que reflita todas as necessidades do negócio. A informação fornecida pela arquitetura de informação é aplicada de forma consistente e extensiva. Melhores práticas da indústria no desenvolvimento e na manutenção da arquitetura da informação são extensivamente utilizadas, incluindo um processo de melhoria contínua. Está definida uma estratégia para utilizar a informação por meio da tecnologia de armazenamento de dados *(datawarehousing)* e de pesquisa de dados *(data mining)*. A arquitetura da informação é aprimorada continuamente e leva em consideração a informação não tradicional dos processos, organizações e sistemas.

Descrição de Processo

PO3 Determinar as Diretrizes da Tecnologia

Os responsáveis pelos serviços de informação determinam um direcionamento tecnológico que suporta o negócio. Isso demanda a criação de um plano de infraestrutura tecnológica e um conselho de arquitetura que estabeleça e gerencie expectativas claras e realistas do que a tecnologia pode oferecer em termos de produtos, serviços e mecanismos de entrega. O plano é atualizado regularmente e abrange aspectos como arquitetura de sistemas, direcionamento tecnológico, plano de aquisições, padrões, estratégias de migração e contingência. Isso permite respostas rápidas a mudanças em um ambiente competitivo, economia de escala em equipes e em investimentos de sistemas de informação, bem como melhor interoperabilidade entre plataformas e aplicações.



Controle sobre o seguinte processo de TI:

Determinar as Diretrizes da Tecnoclogia

que satisfaça aos seguintes requisitos do negócio para a TI:

ter sistemas aplicativos, recursos e capacidades padronizados, integrados, estáveis, com boa relação custo-benefício, que atendam os requisitos atuais e futuros do negócio

com foco em:

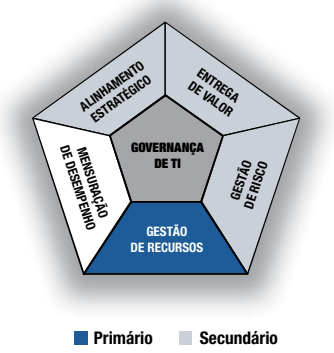
definir e implementar um plano de infraestrutura, arquitetura e padrões de tecnologia que reconheça e aproveite as oportunidades tecnológicas

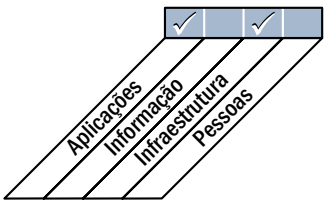
é alcançado por:

- Estabelecimento de um fórum para direcionar a arquitetura e verificar a sua conformidade;
- Estabelecimento de um plano equilibrado de infraestrutura tecnológica com relação aos requisitos, custos e riscos;
- Definição dos padrões de infraestrutura tecnológica com base nos requisitos da arquitetura da informação.

e medido por:

- Quantidade e tipo de desvios do plano de infraestrutura tecnológica
- Frequência de revisão/atualização do planejamento de infraestrutura tecnológica
- Quantidade de plataformas de tecnologia por área da organização





OBJETIVOS DE CONTROLE DETALHADOS

PO3 Determinar as Diretrizes da Tecnologia

PO3.1 Planejamento da Diretriz Tecnológica
Analisar as tecnologias existentes e emergentes e planejar qual direcionamento é apropriado para realizar a estratégia de TI e a arquitetura de sistemas do negócio. Identificar também no plano quais as tecnologias com potencial para gerar oportunidades de negócio. O plano deve contemplar a arquitetura de sistemas, o direcionamento tecnológico, estratégias de migração e aspectos contingenciais dos componentes de infraestrutura.

PO3.2 Plano de Infraestrutura Tecnológica
Criar e manter um plano de infraestrutura tecnológica adequado aos planos tático e estratégico de TI. O plano está baseado no direcionamento tecnológico e inclui acordos de contingência e direcionamento para a aquisição de recursos tecnológicos. Considera mudanças no ambiente competitivo, economia de escala em investimentos em pessoal e sistemas de informação, assim como melhorias na interoperabilidade entre plataformas e aplicações.

PO3.3 Monitoramento de Regulamentos e Tendências Futuras
Estabelecer um processo para monitorar as tendências das áreas de negócio, tecnologia, infraestrutura, legal e regulatória. Incorporar as consequências dessas tendências ao desenvolvimento do plano de infraestrutura de tecnologia de TI.

PO3.4 Padrões Tecnológicos
Prover soluções tecnológicas seguras, eficazes e consistentes, em toda a organização, estabelecer um fórum de tecnologia para prover diretrizes tecnológicas, aconselhamento sobre a infraestrutura de produtos, orientação na seleção da tecnologia e avaliar a conformidade com estes padrões e diretrizes. Este fórum direciona os padrões e práticas tecnológicos com base na relevância para o negócio, nos riscos e na conformidade com requisitos externos.

PO3.5 Conselho de Arquitetura de TI
Estabelecer um conselho de arquitetura de TI para prover diretrizes de arquitetura, orientar a aplicação e verificar a conformidade. Esta entidade norteia o projeto da arquitetura de TI assegurando que sejam implementadas as estratégias de negócio e considerados os requisitos de conformidade e continuidade. Está relacionado/vinculado ao PO2 *Definição da arquitetura da informação.*

Diretrizes de Gerenciamento

PO3 Determinar as Diretrizes da Tecnologia

Origem	Entrada
PO1	Planejamento estratégico e tático de TI;
PO2	Plano otimizado de sistemas de negócio; Arquitetura da informação;
AI3	Atualizações para padrões tecnológicos;
DS3	Informação de desempenho e capacidade

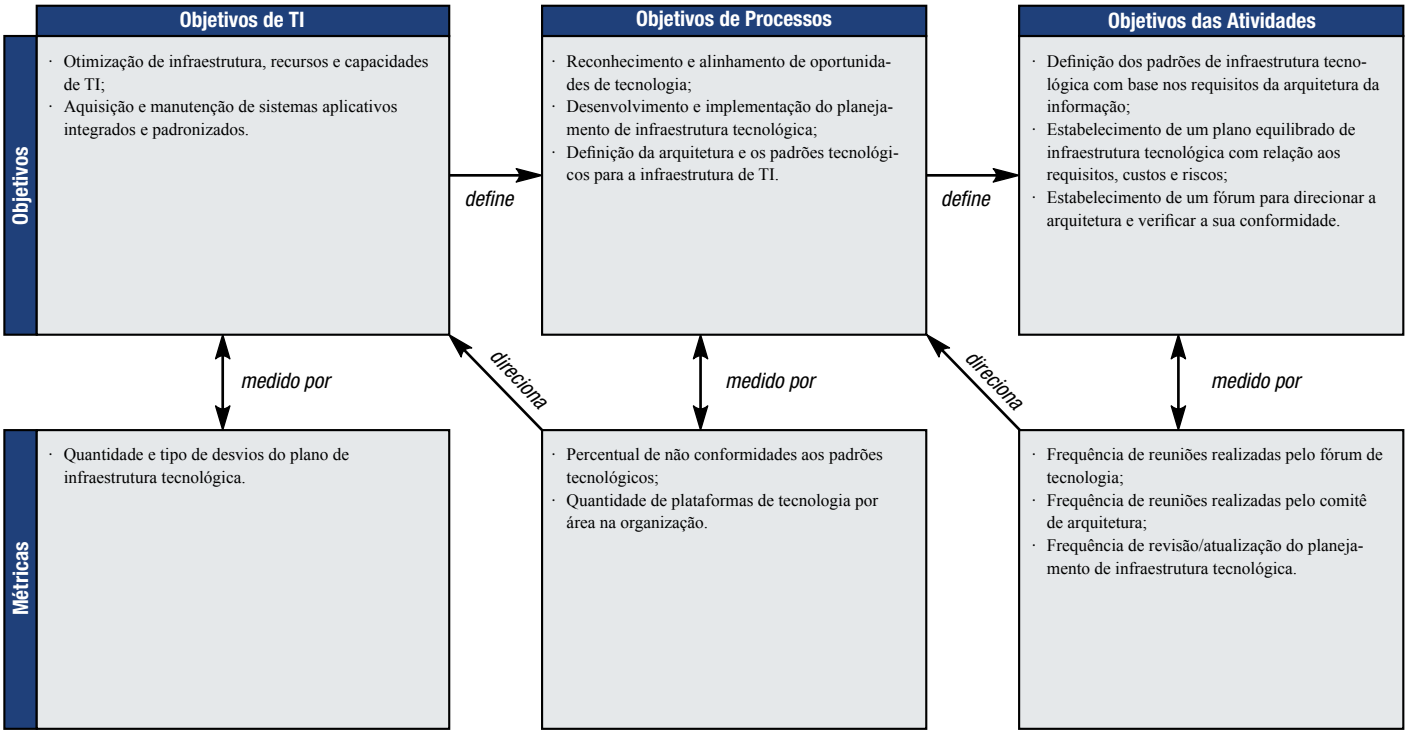
Saída	Destino						
Oportunidades tecnológicas;	AI3						
Padrões tecnológicos;	AI1	AI3	AI7	DS5			
Atualizações periódicas do "estado da tecnologia";	AI1	AI2	AI3				
Planejamento da infraestrutura tecnológica;	AI3						
Requisito de infraestrutura	PO5						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Criar e manter um planejamento de infraestrutura tecnológica;		I	I	A		C	R	C	C		C
Criar e manter padrões tecnológicos;				A		C	R	C	I	I	I
Publicar padrões tecnológicos;		I	I	A		I	R	I	I	I	I
Monitorar evolução tecnológica;		I	I	A		C	R	C		C	C
Definir uso (futuro) (estratégico) de novas tecnologias		C	C	A		C	R	C		C	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

PO3 Determinar as Diretrizes da Tecnologia

O gerenciamento do processo de ***"Determinar as diretrizes da tecnologia"*** que satisfaça ao requisito do negócio para a TI de ***"ter sistemas aplicativos, recursos e capacidades padronizados, integrados, estáveis, com boa relação custo-benefício, que atendam aos requisitos atuais e futuros do negócio"*** é:

0 Inexistente quando
Não há conscientização da importância de um planejamento de infraestrutura de tecnologia para a entidade. O conhecimento e a habilidade necessários para desenvolver tal plano de infraestrutura tecnológica não existem. Há uma carência de entendimento de que o planejamento das mudanças tecnológicas é fundamental para alocar recursos com eficácia.

1 Inicial/ *Ad hoc* quando
A Direção reconhece a necessidade do planejamento de infraestrutura de tecnologia. Os desenvolvimentos de componentes de tecnologia e implementações de tecnologias emergentes são *ad hoc* e isolados. Existe uma abordagem reativa e focada operacionalmente no planejamento da infraestrutura. O direcionamento da tecnologia é guiado pelos planos de evolução muitas vezes contraditórios de fornecedores de *hardware*, *softwares* de sistemas e aplicativos. A comunicação do impacto em potencial das mudanças na tecnologia é inconsistente.

2 Repetível, porém Intuitivo quando
A necessidade e a importância de um plano tecnológico são comunicadas. O planejamento é tático e direcionado à geração de soluções técnicas para os problemas técnicos, ao invés de se concentrar no uso da tecnologia para satisfazer às necessidades do negócio. A avaliação das mudanças tecnológicas é deixada a cargo de diferentes indivíduos que seguem processos intuitivos, porém similares. As pessoas adquirem suas habilidades de planejamento tecnológico através de aprendizado prático e repetidas aplicações de técnicas. Técnicas e padrões comuns estão sendo criados para o desenvolvimento de componentes de infraestrutura.

3 Processo Definido quando
A Direção está ciente da importância do plano de infraestrutura tecnológica. O processo de desenvolvimento do plano de infraestrutura tecnológica é razoavelmente discutido e está alinhado ao plano estratégico de TI. Existe um plano de infraestrutura tecnológica definido, documentado e comunicado, mas aplicado de forma inconsistente. O direcionamento da infraestrutura tecnológica inclui um entendimento do quanto a organização quer manter a liderança ou recuar no uso da tecnologia, com base nos riscos e em alinhamento com a estratégia da organização. Fornecedores-chave são selecionados com base no entendimento de seus planos de longo prazo de desenvolvimento de tecnologias e produtos e em conformidade com o direcionamento da organização. Há treinamento formal e comunicação de papéis e responsabilidades.

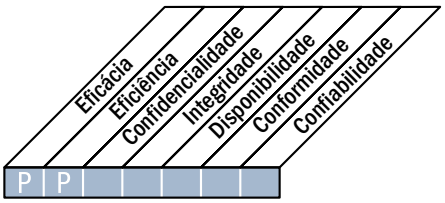
4 Gerenciado e Mensurável quando
A Direção garante o desenvolvimento e a manutenção do plano de infraestrutura tecnológica. A equipe de TI tem a especialização e as habilidades necessárias para desenvolver um plano de infraestrutura tecnológica. O impacto em potencial do surgimento e de mudanças de tecnologias é levado em consideração. A Direção pode identificar desvios do plano e antever problemas. A responsabilidade pelo desenvolvimento e manutenção de um plano de infraestrutura tecnológica foi atribuída. O processo de desenvolvimento do plano de infraestrutura tecnológica é sofisticado e responde à mudança. Boas práticas internas foram introduzidas no processo. A estratégia de recursos humanos está alinhada com o direcionamento tecnológico para garantir que a equipe de TI possa administrar mudanças de tecnologia. Para introduzir novas tecnologias são definidos planos de migração. Terceirizações e parcerias estão sendo utilizadas para obter conhecimentos e habilidades necessários. A Direção analisou a aceitação do risco relativo ao avanço ou recuo no uso da tecnologia para o desenvolvimento de novas oportunidades de negócio ou a melhoria da eficiência operacional.

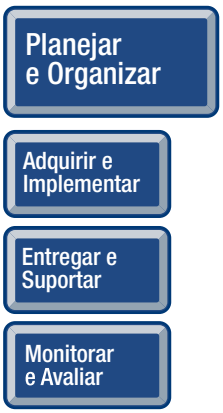
5 Otimizado quando
Existe uma atividade de pesquisa para investigar as tecnologias emergentes e em evolução e realizar comparações da organização com os padrões do seu segmento *(benchmarking)*. O direcionamento do planejamento de infraestrutura tecnológica é guiado por padrões e desenvolvimentos internacionais e do segmento e não pelos apresentados por fornecedores de tecnologia. O impacto em potencial sobre o negócio devido a uma mudança tecnológica é revisado em nível de Diretoria. Há aprovação executiva formal de mudanças ou novos direcionamentos tecnológicos. A entidade tem um plano de infraestrutura tecnológica robusto que reflete os requisitos de negócio e reativo, podendo ser modificado para refletir mudanças no ambiente de negócio. Há um processo de melhoria contínua do plano de infraestrutura tecnológica. As melhores práticas do segmento são extensivamente empregadas para determinar o direcionamento técnico.

DESCRIÇÃO DE PROCESSO

PO4 Definir os Processos, Organização e Relacionamentos de TI

Uma organização de TI é definida considerando os requisitos de pessoal, habilidades, funções, autoridade, papéis e responsabilidades, rastreabilidade e supervisão. Essa organização deve fazer parte de uma estrutura de processos de TI que assegure transparência e controle, assim como o envolvimento de executivos sênior e a Direção do negócio. Um comitê estratégico deve assegurar a supervisão da Direção de TI, e um ou mais comitês dos quais as áreas de negócio e TI participem devem definir a priorização dos recursos de TI em linha com as necessidades do negócio. Os processos, as políticas administrativas e os procedimentos precisam estar estabelecidos para todas as funções, com especial atenção às de controle, garantia da qualidade, gestão de risco, segurança da informação, propriedade de sistemas e dados e segregação de funções. Para assegurar o rápido atendimento das exigências do negócio, a TI deve ser envolvida nos processos de decisão relevantes.





Controle sobre o seguinte processo de TI:

Definir os processos, a organização e os relacionamentos de TI

que satisfaça aos seguintes requisitos de negócio para a TI:

ser ágil em resposta à estratégia de negócio e, ao mesmo tempo, atender aos requisitos de Governança e fornecer pontos de contatos definidos e competentes

com foco em:

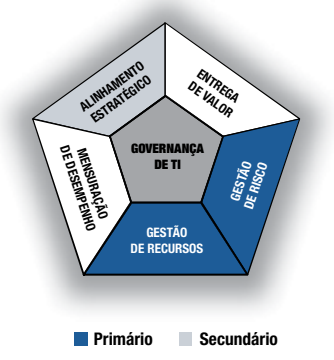
estabelecer estruturas organizacionais de TI transparentes, flexíveis e responsivas e definir e implementar processos de TI com proprietários (de sistemas e dados), papéis e responsabilidades integrados aos processos de negócio e processos de decisão.

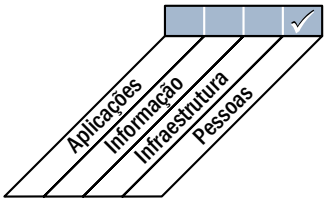
é alcançado por:

· Definição de uma estrutura de processos de TI
· Estabelecimento de conselhos e estruturas organizacionais apropriadas
· Definição de papéis e responsabilidades

e medido por:

· Percentual de funções com posições e descrições de autoridade documentadas;
· Número de unidades/processos de negócios não suportados pela organização de TI, mas que deveriam ser suportados de acordo com a estratégia;
· Número de atividades centrais de TI realizadas fora da organização de TI e que não são aprovadas ou submetidas aos padrões organizacionais de TI





OBJETIVOS DE CONTROLE DETALHADOS

PO4 Definir os Processos, Organização e Relacionamentos de TI

PO4.1 Estrutura de Processos de TI
Definir um modelo de processos de TI para executar o plano estratégico de TI. Este modelo inclui uma estrutura de processos e relacionamentos de TI (por exemplo, gerenciar falhas ou interposições de processos), definição de um proprietário, maturidade, medição de desempenho, melhorias, conformidade, metas de qualidade e planos para atingi-las. O modelo provê integração entre os processos de TI, gestão de portfólio corporativo, processos de negócio e mudanças nos processos. O modelo de processos de TI deve estar integrado a um sistema de gestão da qualidade e a uma estrutura de controles internos.

PO4.2 Comitê Estratégico de TI
Estabelecer um comitê estratégico de TI em nível de Diretoria. Esse comitê assegura que a governança de TI seja devidamente considerada como parte da governança corporativa, aconselha sobre o direcionamento estratégico e analisa os principais investimentos, em nome de toda a Direção.

PO4.3 Comitê Executivo de TI
Estabelecer um comitê executivo (ou equivalente) composto pelas Diretorias Executiva, Negócios e TI para:
· Determinar prioridades dos programas de investimentos em TI em linha com as estratégias e prioridades do negócio
· Monitorar o estado atual dos projetos e resolver conflitos de recursos
· Monitorar níveis de serviço e suas melhorias

PO4.4 Posicionamento Organizacional da área de TI
Posicionar a área de TI na estrutura geral organizacional através de um modelo que efetivamente considere sua importância e as necessidades de contingência, considerando a importância da TI para a estratégia de negócio e o nível de dependência operacional. A linha de reporte do CIO deve ser proporcional à importância da TI dentro do negócio.

PO4.5 Estrutura Organizacional de TI
Estabelecer uma estrutura organizacional interna e externa de TI que reflita as necessidades do negócio. Adicionalmente estabelecer um processo para revisar periodicamente a estrutura organizacional de TI e ajustar os requisitos de pessoal e estratégias de fornecimento para atender aos objetivos de negócio esperados e a possíveis situações de mudança.

PO4.6 Definição de Papéis e Responsabilidades
Definir e comunicar para o pessoal de TI e usuários finais seus respectivos papéis e responsabilidades, que especifiquem a autoridade, responsabilidade e responsabilização, com o objetivo de atender às necessidades da organização.

PO4.7 Responsabilidade pela Garantia de Qualidade
Atribuir responsabilidade pelo desempenho da função de garantia de qualidade *(QA, quality assurance)*, e prover a esse grupo conhecimento e sistemas adequados de controle e comunicação. Garantir que o posicionamento na organização, o dimensionamento da responsabilidade e tamanho do grupo de QA atendam aos requisitos da organização

PO4.8 Responsabilidade por Riscos, Segurança e Conformidade
Incluir nas funções de negócio a propriedade e a responsabilidade pelos riscos relacionados a TI a um nível sênior apropriado. Definir e atribuir papéis críticos para o gerenciamento dos riscos de TI, incluindo a responsabilidade específica pela segurança da informação, segurança física e conformidade. Estabelecer responsabilidade no nível organizacional pelo gerenciamento de risco e segurança para questões de nível organizacional.
Pode ser preciso atribuir responsabilidades adicionais de gerenciamento de segurança ao nível de um sistema específico para lidar com questões de segurança relacionadas. Obter direcionamento da Diretoria sobre os níveis específicos de risco de TI aceitáveis e aprovação de quaisquer riscos residuais

PO4.9 Proprietários de Dados e Sistemas
Estabelecer procedimentos e disponibilizar ferramentas que possibilitem tratar as responsabilidades dos proprietários dos dados e sistemas de informação. Os proprietários tomam decisões sobre a classificação da informação e dos sistemas e os protegem em conformidade com essa classificação.

PO4.10 Supervisão
Implementar técnicas de supervisão adequadas na área de TI para assegurar que os papéis e as responsabilidades sejam adequadamente exercidos, avaliar se todo o pessoal tem autoridade e recursos suficientes para exercer seus papéis e responsabilidades e revisar de forma geral os indicadores-chave de desempenho.

PO4.11 Segregação de Funções
Implementar uma separação de papéis e responsabilidades que reduza a possibilidade de um único indivíduo subverter um processo crítico. A gerência também deve se certificar de que o pessoal esteja executando apenas tarefas autorizadas relevantes aos seus respectivos cargos e posições.

PO4.12 Recrutamento de pessoal de TI
Avaliar os requisitos de recrutamento regularmente ou com base em grandes mudanças nos ambientes de TI, operacional ou de negócio para garantir que a área de TI tenha quantidade suficiente de pessoal para suportar de forma adequada os objetivos e metas de negócios.

PO4.13 Pessoal Chave de TI
Definir e identificar o pessoal-chave de TI (ex., pessoal para reposição/backup) e minimizar o excesso de confiança em um único indivíduo executando uma função crítica.

PO4.14 Políticas e Procedimentos para Pessoal Contratado
Definir e implementar políticas e procedimentos para controlar as atividades de consultores e outros contratados da área de TI visando assegurar a proteção dos ativos de informação da organização e o cumprimento das exigências contratuais firmadas.

PO4.15 Relacionamentos
Estabelecer e manter uma estrutura otimizada de coordenação, comunicação e conexão entre a função de TI e diversos outros interesses dentro ou fora da área de TI; por exemplo, Diretoria, unidades de negócios, usuários individuais, fornecedores, profissionais de segurança, gerentes de risco, gerenciamento de pessoal terceirizado e externo e o grupo de conformidade corporativa *(compliance)*.

Página intencionalmente deixada em branco

Diretrizes de Gerenciamento

PO4 Definir os Processos, Organização e Relacionamentos de TI

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI;
PO7	Políticas e procedimentos de RH para TI; Matriz de habilidades em TI; Descrição de cargos;
PO8	Ações de melhoria de qualidade;
PO9	Planos de ação para remediação de riscos de TI;
ME1	Planos de ação para remediações;
ME2	Relatórios sobre eficácia de controles de TI;
ME3	Catálogo de requisitos legais e regulatórios relacionados com a entrega de serviços de TI;
ME4	Melhorias da estrutura de processos

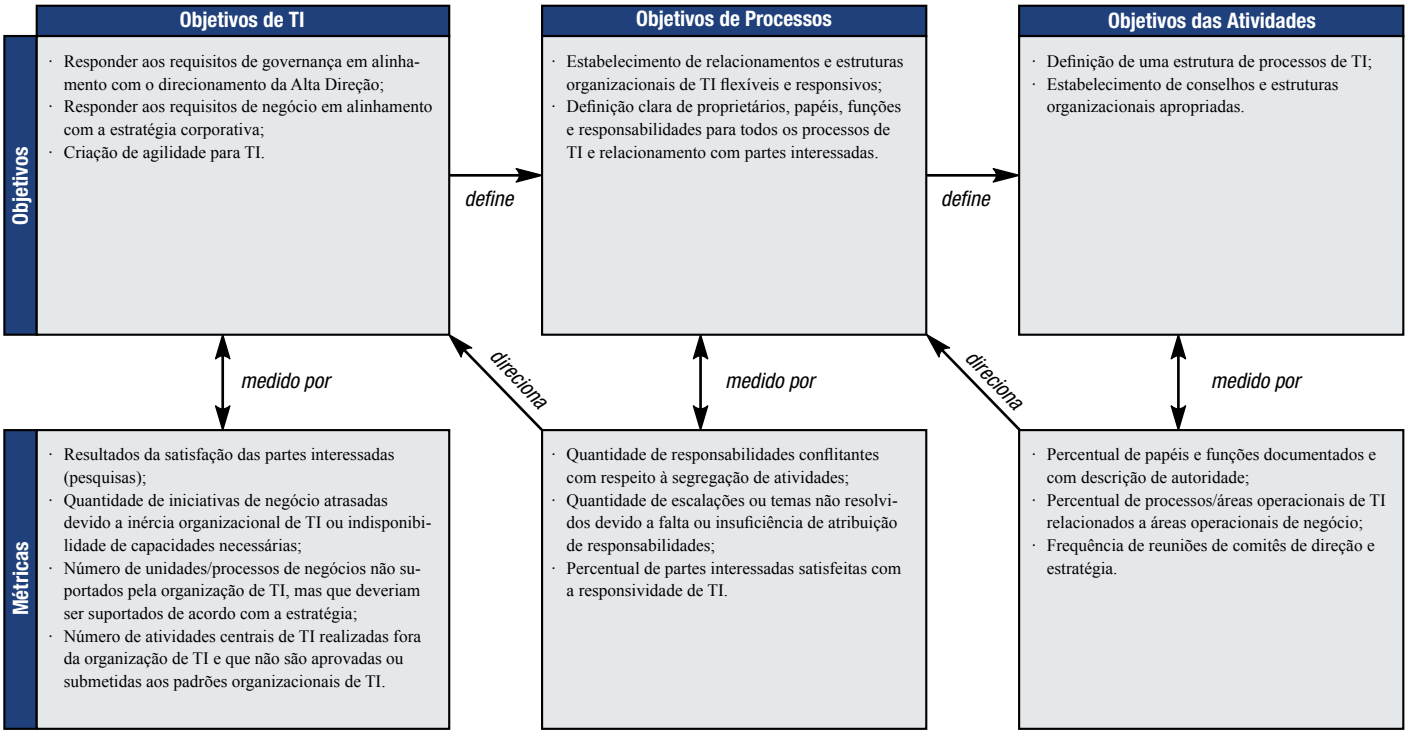
Saída	Destino						
Estrutura de processos de TI;	ME4						
Proprietários formais dos sistemas;	AI7	DS6					
Organização e relacionamentos de TI;	PO7						
Estrutura de processos de TI, papéis, funções e responsabilidades documentadas;	ALL						
Documentação de papéis, funções e responsabilidades	PO7						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Estabelecer a estrutura organizacional de TI, incluindo comitês e relacionamentos com partes interessadas e fornecedores;	C	C	C	A		C	C	C	R	C	I
Projetar a estrutura de processos de TI;	C	C	C	A		C	C	C	R	C	C
Identificar os proprietários dos sistemas;		C	C	A	C	R	I	I	I	I	I
Identificar os proprietários dos dados;		I	A	C	C	I	R	I	I	I	C
Estabelecer e implementar papéis, funções e responsabilidades de TI, incluindo supervisão e segregação de atividades		I	I	A	I	C	C	C	R	C	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

PO4 Definir os Processos, Organização e Relacionamentos de TI

Gerenciamento do processo de ***"Definir o Processo, Organização e Relacionamentos de TI"*** que satisfaçam aos requisitos de negócio para TI em ***"ser ágil em resposta à estratégia de negócio e, ao mesmo tempo, atender aos requisitos de Governança e fornecer pontos de contatos definidos e competentes"*** é:

0 Inexistente quando
A organização de TI não está estabelecida de forma eficiente com foco nos objetivos do negócio.

1 Inicial / *Ad hoc* quando
As áreas e atividades de TI são reativas e implementadas de maneira inconsistente. A TI é envolvida apenas nos estágios finais dos projetos de negócio. A área de TI é considerada uma área de apoio, sem uma perspectiva geral da organização. Há um entendimento implícito da necessidade de uma organização de TI, entretanto os papéis e responsabilidades não são formalizados nem impostos.

2 Repetível, porém Intuitivo quando
A área de TI é organizada para responder taticamente, porém de forma inconsistente, às necessidades dos clientes e relacionamento com fornecedores. A necessidade de uma organização estruturada e um gerenciamento de fornecedores é comunicada, mas as decisões ainda são dependentes em termos de conhecimento e habilidades de pessoas-chave. Estão surgindo técnicas básicas para controlar a organização de TI e os relacionamentos com fornecedores.

3 Processo Definido quando
Existem definições de papéis e responsabilidades da organização de TI e de terceiros. A organização de TI é desenvolvida, documentada, comunicada e alinhada com a estratégia de TI. O ambiente de controle interno é definido. Há formalização dos relacionamentos com outras partes, incluindo comitês executivos, auditoria interna e gerenciamento de fornecedores. A organização de TI é funcionalmente completa. Há definições das funções a serem desempenhadas pelo pessoal de TI e daquelas a serem desempenhadas pelos usuários. Os requisitos e habilidades essenciais do pessoal de TI são definidos e atendidos. Há uma definição formal dos relacionamentos com usuários e terceiros. A segregação de papéis e responsabilidades é definida e implementada.

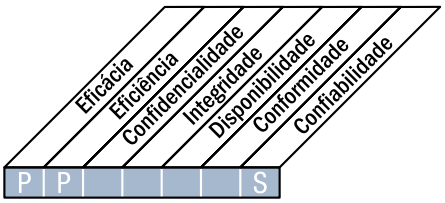
4 Gerenciado e Mensurável quando
A organização de TI responde às mudanças de forma proativa e contempla todos os papéis necessários para atender às exigências do negócio. A Direção da área de TI, os proprietários dos processos e as responsabilidades são definidos e equilibrados. As melhores práticas internas têm sido aplicadas na organização das funções de TI. A Direção da área de TI tem habilidades e técnicas apropriadas para definir, implementar e monitorar a organização e os relacionamentos desejados. As métricas mensuráveis para apoiar os objetivos de negócio e fatores críticos de sucesso definidos pelos usuários são padronizadas. Há um inventário de habilidades disponível para apoiar a alocação de profissionais em projetos e o desenvolvimento profissional. O equilíbrio entre as habilidades e os recursos disponíveis internamente e aqueles exigidos pelas organizações externas está definido e é mantido. A estrutura organizacional da TI reflete apropriadamente as necessidades do negócio através da oferta de serviços alinhados com os processos de negócio estratégicos ao invés de tecnologias isoladas.

5 Otimizado quando
A estrutura organizacional de TI é flexível e adaptável e são aplicadas as melhores práticas do mercado. Há amplo uso de tecnologia para auxiliar e monitorar o desempenho da organização de TI e seus processos. A tecnologia está à altura da complexidade e da distribuição geográfica da organização. Existe um contínuo processo de melhoria estabelecido.

Descrição do Processo

PO5 Gerenciar o Investimento de TI

Estabelecer e manter uma estrutura para gerenciar os programas de investimentos em TI que contemple custos, benefícios, prioridade dentro do orçamento, um processo formal de definição orçamentária e gerenciamento de acordo com o orçamento. As partes interessadas são consultadas para identificar e controlar os custos totais e os benefícios dentro dos contextos estratégicos e táticos da TI e iniciar ações de correção quando necessário. O processo promove a parceria entre a TI e as partes interessadas do negócio, permite o uso eficaz e eficiente dos recursos de TI, provê transparência, atribui responsabilidade pelo custo total de propriedade *(TCO, Total Cost of Ownership)*, realização dos benefícios do negócio e do retorno sobre os investimentos em TI.



Controle sobre o seguinte processo de TI:

Gerenciar o investimento de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

melhorar continua e visivelmente a relação custo-benefício da TI e sua contribuição para a lucratividade do negócio com serviços integrados e padronizados que atendam às expectativas do usuário final.

com foco em:

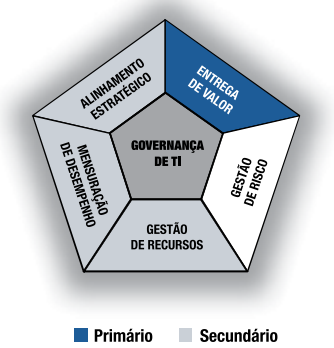
decidir o portfólio e investimentos em TI de forma eficaz e eficiente e elaborar e rastrear os orçamentos de TI em linha com estratégias de TI e decisões de investimento

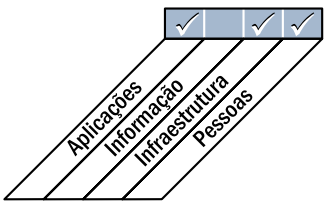
é alcançado por:

- Previsão e alocação de orçamentos
- Definição do critério de investimento formal (ROI – Retorno sobre Investimento, período de recuperação de investimento, NPV – Valor Presente Líquido)
- Medição e avaliação do valor de negócio comparado à previsão.

e medido por:

- Redução percentual do custo unitário dos serviços de TI entregues
- Percentual de desvio do valor orçamentário comparado com o orçamento total
- Percentual dos gastos de TI expressos através de motivadores de valor de negócio (por exemplo: aumento de vendas/serviços devido ao aumento da conectividade)





OBJETIVOS DE CONTROLE DETALHADOS

PO5 Gerenciar o Investimento de TI

PO5.1 Estrutura da Administração Financeira
Estabelecer e manter uma estrutura financeira para gerenciar investimentos e custos de bens e serviços de TI através de portfólios de investimentos, estudos de caso e orçamentos de TI.

PO5.2 Priorização dentro do Orçamento de TI
Implementar um processo de tomada de decisão para priorizar a alocação dos recursos de TI em operações, projetos e manutenção visando maximizar a contribuição da TI na otimização dos retornos do programa de investimentos em TI e outros serviços e recursos da TI.

PO5.3 Processo de Orçamento de TI
Estabelecer um processo para preparar e controlar um orçamento que reflita as prioridades estabelecidas pelo portfólio de programas de investimentos de TI da organização, incluindo os custos contínuos de operação e manutenção da infraestrutura atual. O processo deve sustentar o desenvolvimento do orçamento de TI total, bem como o desenvolvimento de orçamentos para programas individuais, com ênfase especial nos componentes de TI de tais programas. O processo deve permitir revisão, refinação e aprovação contínuas do orçamento de TI total e de todos os orçamentos de programas individuais.

PO5.4 Gerenciamento de Custo
Implementar um processo de gerenciamento de custo comparando os custos e benefícios reais. Os custos devem ser monitorados e relatados. Se houver desvios, devem ser identificados a tempo, avaliados os impactos destes sobre os programas e ações corretivas apropriadas precisam ser tomadas junto com o patrocinador do negócio desses programas. Quando necessário, o estudo de caso *(business case)* deve ser atualizado.

PO5.5 Gerenciamento de Benefícios
Implementar um processo de monitoramento dos benefícios de prover e manter capacidades de TI apropriadas. Devem ser identificadas, pactuadas, monitoradas e reportadas as contribuições esperadas de TI para com os resultados de negócio, tanto como um componente de programas de investimento em TI quanto como parte da operação de suporte regular. Os relatórios devem ser revisados e ações apropriadas devem ser definidas e implantadas onde houver oportunidade para melhorar a contribuição de TI. O programa de estudo de caso deve ser atualizado quando afetado por mudanças na contribuição da TI ou por projetos relacionados.

Diretrizes de Gerenciamento

PO5 Gerenciar o Investimento de TI

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI; Portfólio de projetos e serviços de TI;
PO3	Requisitos de Infraestrutura;
PO10	Portfólio de projetos de TI atualizado;
AI1	Estudo de viabilidade dos requisitos de negócio;
AI7	Revisão pós-implementação;
DS3	Planejamento de desempenho e capacidade (requisitos);
DS6	Aspectos financeiros de TI;
ME4	Resultados de negócio esperados a partir dos Investimentos em negócios habilitados por TI

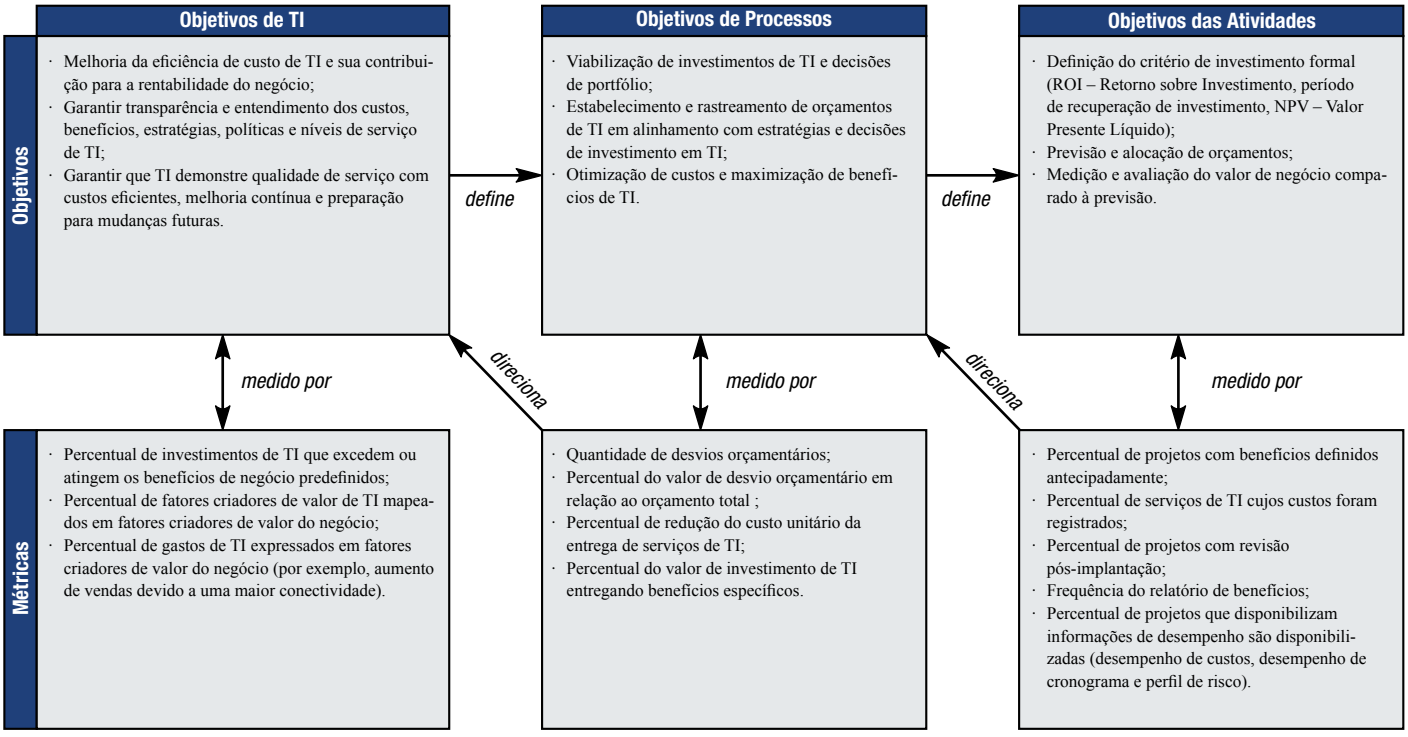
Saída	Destino						
Relatórios de custo/benefício;	PO1	AI2	DS6	ME1	ME4		
Orçamentos de TI;	DS6						
Portfólio de serviços de TI atualizado;	DS1						
Portfólio de projetos de TI atualizado	PO10						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Manter portfólio de programas;	A	R	R	R	C					I	I
Manter portfólio de projetos;	I	C	A/R	A/R	C		C	C		C	I
Manter portfólio de serviços;	I	C	A/R	A/R	C	C				C	I
Estabelecer e manter o processo orçamentário de TI;	I	C	C	A		C	C	C	R	C	
Identificar, comunicar e monitorar os investimentos em TI, custos e valor para o negócio	I	C	C	A/R		C	C	C	R	C	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

PO5 Gerenciar o Investimento de TI

O gerenciamento do processo de ***"Gerenciar o Investimento de TI"*** que satisfaça ao requisito do negócio para a TI de "***melhorar continuamente e visivelmente a relação custo-benefício da TI e sua contribuição para a lucratividade do negócio com serviços integrados e padronizados que satisfaçam às expectativas do usuário final"*** é:

0 Inexistente quando
Não há consciência da importância da seleção do investimento e orçamento de TI. Não há monitoramento ou rastreamento dos investimentos e gastos em TI.

1 Inicial/ *Ad hoc* quando
A organização reconhece a necessidade de gerenciar o investimento em TI, mas essa necessidade é comunicada inconsistentemente. A alocação das responsabilidades pela seleção de investimento e desenvolvimento orçamentário de TI é feita de forma *ad hoc*. Acontecem implementações isoladas de seleção de investimento e orçamento de TI e são documentadas informalmente. Os investimentos de TI são justificados de forma *ad hoc*. Ocorrem decisões orçamentárias reativas e focadas operacionalmente.

2 Repetível, porém Intuitivo quando
Há um entendimento implícito da necessidade de seleção de investimento e orçamento de TI. A necessidade de um processo orçamentário e de seleção é comunicada. A conformidade depende da iniciativa de algumas pessoas da organização. Estão surgindo técnicas comuns para desenvolver componentes do orçamento de TI. São tomadas decisões orçamentárias táticas e reativas.

3 Processo Definido quando
As políticas e os processos de investimento e orçamento são definidos, documentados e comunicados e contemplam aspectos tecnológicos e de negócio fundamentais. O orçamento de TI está alinhado aos planos de negócio e à estratégia de TI. Os processos de orçamento e seleção de investimentos de TI são formalizados, documentados e comunicados. Estão surgindo treinamentos formais, mas ainda são baseados fundamentalmente em iniciativas individuais. A aprovação formal das seleções de investimentos e orçamento de TI é estabelecida. A equipe de TI tem habilidades e experiência necessárias para elaborar o orçamento de TI e recomendar investimentos em TI apropriados.

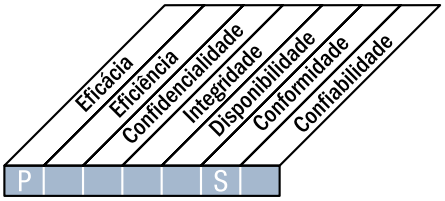
4 Gerenciado e Mensurável quando
A responsabilidade pela definição de orçamento e seleção de investimento é atribuída a uma pessoa específica. As variações orçamentárias são identificadas e resolvidas. Análises formais de custo são executadas abrangendo custos diretos e indiretos das operações existentes, bem como investimentos propostos, considerando todos os custos incidentes sobre o ciclo de vida total. É usado um processo orçamentário proativo e padronizado. O impacto da migração de custos oriundos do desenvolvimento e da operação de hardware e software para a integração de sistemas e recursos humanos de TI é reconhecido nos planos de investimento. Os benefícios e retornos são calculados em termos financeiros e não financeiros.

5 Otimizado quando
As melhores práticas da indústria são utilizadas para comparar custos e identificar abordagens para a eficácia dos investimentos. São usadas análises de desenvolvimento tecnológico no processo orçamentário e de seleção de investimento. O processo de gerenciamento de investimento é melhorado continuamente com base nas lições aprendidas pela análise do desempenho real do investimento. As decisões de investimentos incorporam tendências de melhoria de preço/desempenho. As alternativas de financiamento são formalmente investigadas e avaliadas no contexto da estrutura de capitais existente na organização, valendo-se de métodos formais de avaliação. Há identificação proativa de variações. Uma análise dos custos e benefícios a longo prazo do ciclo de vida total é incorporada às decisões de investimentos.

Descrição do Processo

PO6 Comunicar Metas e Diretrizes Gerenciais

A Direção deve desenvolver uma estrutura de controle de TI corporativo e definir e comunicar políticas. Um programa de comunicação contínuo aprovado e apoiado pela Direção deve ser implementado para articular missão, metas, políticas, procedimentos etc. A comunicação apoia o alcance dos objetivos de TI e assegura a consciência e o entendimento dos negócios, dos riscos de TI, dos objetivos e das diretrizes. O processo deve assegurar conformidade com leis e regulamentos relevantes.



Controle sobre o seguinte processo de TI:

Comunicar as diretrizes e expectativas da Diretoria

que satisfaça aos seguintes requisitos do negócio para a TI:

manter as informações precisas e atualizadas nos serviços de TI atuais e futuros, bem como as responsabilidades e os riscos associados

com foco em:

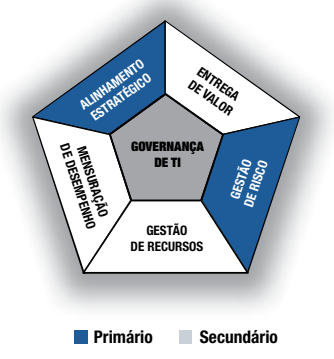
fornecer políticas, procedimentos, diretrizes e outras documentações de forma precisa, compreensível e aprovada para as partes interessadas, incorporada a uma estrutura de controles de TI

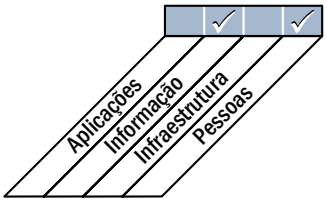
é alcançado por:

· Definição de uma estrutura de controle de TI
· Desenvolvimento e implementação de políticas de TI
· Imposição de políticas de TI

e medido por:

· Quantidade de interrupções no negócio devido a interrupções em serviços de TI
· Percentual de partes interessadas que entendem a estrutura corporativa de controle de TI
· Percentual das partes interessadas que não estão em conformidade com a política





Objetivos de Controle Detalhados

PO6 Comunicar Metas e Diretrizes Gerenciais

PO6.1 Política de TI e Ambiente de Controle
Definir os elementos de um ambiente de controle de TI alinhados com o estilo operacional e a filosofia de gerenciamento da empresa. Entre esses elementos estão as expectativas e os requisitos de entrega de valor dos investimentos de TI, o grau de aceitação de risco, a integridade, os valores éticos, a competência do pessoal e a responsabilização. O ambiente de controle está baseado em uma cultura que sustenta a entrega de valor e, ao mesmo tempo, controla os riscos significativos, incentiva o trabalho em equipe e a cooperação entre equipes, promove a conformidade, promove o processo de melhoria contínua e lida com os desvios (incluindo falhas) de forma adequada.

PO6.2 Risco de TI Corporativo e Estrutura Interna de Controle
Desenvolver e manter uma estrutura que estabeleça uma abordagem corporativa completa dos riscos e controles de TI e o alinhamento com as políticas e o ambiente de controle de TI e com a estrutura de riscos e controles da organização.

PO6.3 Gerenciamento de Políticas de TI
Desenvolver e manter um conjunto de políticas para apoiar a estratégia de TI. Essas políticas devem incluir os objetivos das políticas, papéis e responsabilidades, processos de exceções, abordagem de conformidade, referências a procedimentos, padrões e diretrizes. Sua relevância deve ser regularmente aprovada e ratificada.

PO6.4 Distribuição da Política
Assegurar que as políticas de TI sejam impostas e distribuídas para todo o pessoal relevante, se consolidando e sendo parte integrante das operações corporativas.

PO6.5 Comunicação dos Objetivos e Diretrizes de TI
Comunicar visando a conscientização e entendimento dos objetivos e direcionamentos de negócios e TI de todas as partes interessadas e usuários apropriados na organização.

Diretrizes de Gerenciamento

PO6 Comunicar Metas e Diretrizes Gerenciais

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI; Portfólio de projetos e serviços de TI;
PO9	Diretrizes para a gestão de riscos de TI;
ME2	Relatórios sobre a eficácia de controles de TI

Saída	Destino
Estrutura corporativa de controles de TI;	ALL
Políticas de TI	ALL

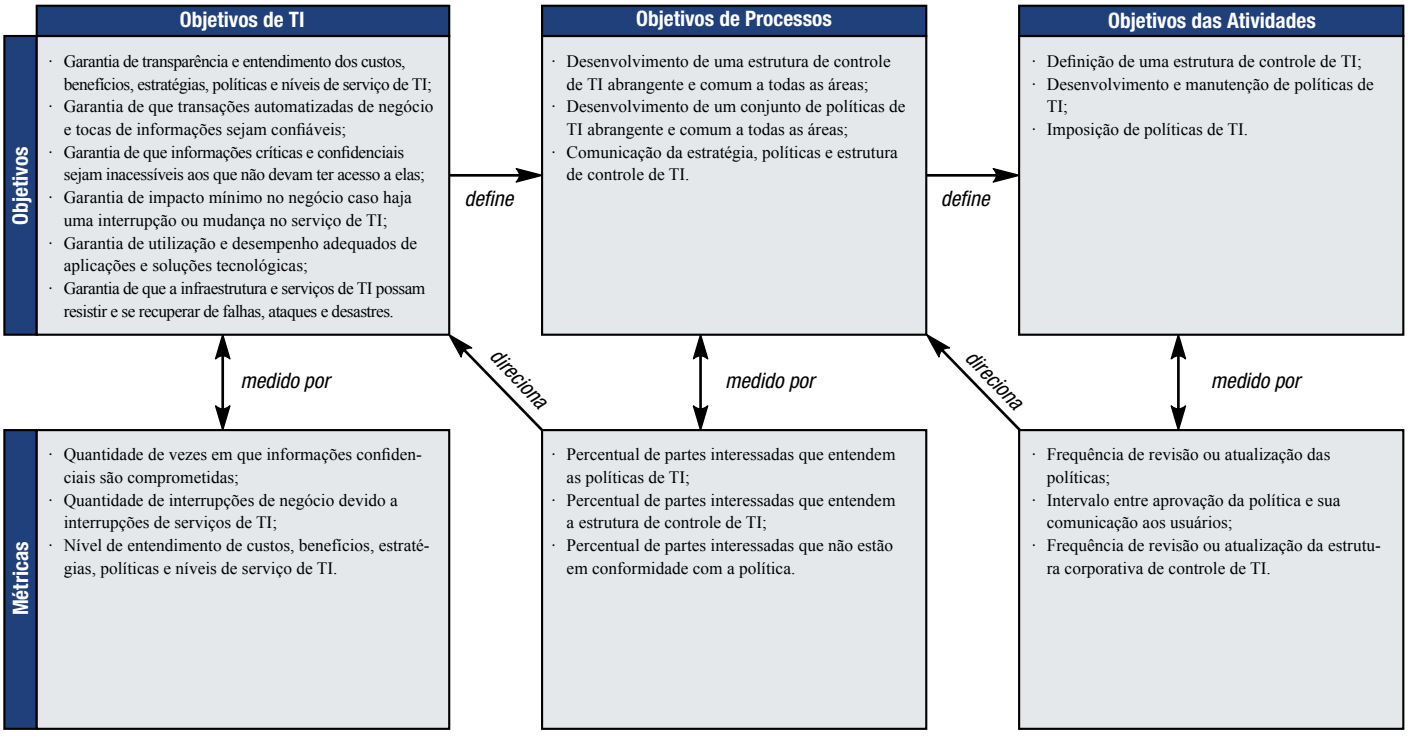
Tabela RACI

Funções

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Estabelecer e manter a estrutura e ambiente de controle de TI;	I	C	I	A/R	I	C		C	C		C
Desenvolver e manter as políticas de TI;	I	I	I	A/R		C	C	C	R		C
Comunicar a estrutura de controle, os objetivos e as diretrizes de TI	I	I	I	A/R					R		C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

PO6 Comunicar Metas e Diretrizes Gerenciais

O gerenciamento do processo de ***"Comunicar metas e diretrizes gerenciais"*** que satisfaça ao requisito de negócio para a TI de ***"manter as informações precisas e atualizadas nos serviços de TI atuais e futuros, bem como as responsabilidades e os riscos associados"*** é:

0 Inexistente quando
A Direção não estabeleceu um ambiente de controle da informação. Não há reconhecimento da necessidade de estabelecer um conjunto de políticas, padrões, procedimentos e processos de conformidade.

1 Inicial/*Ad hoc* quando
A Direção é reativa no tratamento dos requisitos do ambiente de controle da informação. As políticas, os procedimentos e os padrões são desenvolvidos e comunicados quando necessário *(ad hoc)*, impulsionados por casos específicos. Os processos de desenvolvimento, comunicação e conformidade são informais e inconsistentes.

2 Repetível, porém Intuitivo quando
A Direção tem um entendimento implícito das necessidades e dos requisitos de um ambiente de controle de informação eficaz, mas as práticas são muito informais. A Direção tem comunicado a necessidade de políticas de controle, padrões e procedimentos, porém o desenvolvimento fica a critério de cada uma das Direções de Área. A qualidade é reconhecida como uma filosofia desejável a ser seguida, mas as práticas são deixadas a cargo de cada uma das Direções de Área. O treinamento é executado individualmente, conforme a necessidade.

3 Processo Definido quando
Um ambiente completo de gestão da qualidade e controle da informação é desenvolvido, documentado e comunicado pela Direção, o qual inclui uma estrutura de políticas, padrões e procedimentos.
O processo de desenvolvimento de política é estruturado, mantido e conhecido pelas equipes, e as políticas, os padrões e os procedimentos existentes são razoavelmente divulgados e cobrem temas-chave. A Direção considera a importância da consciência da segurança de TI e inicia programas de conscientização. Há treinamento formal disponível para apoiar o ambiente de controle da informação, mas não é rigorosamente aplicado. Embora exista uma estrutura de desenvolvimento completa para o controle de políticas e padrões, há um monitoramento inconsistente da conformidade. Existe uma estrutura de desenvolvimento geral. As técnicas para promover a conscientização de segurança têm sido padronizadas e formalizadas.

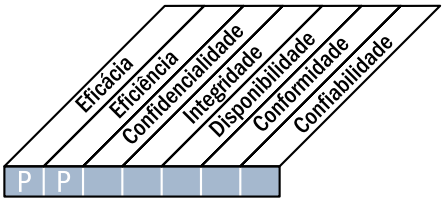
4 Gerenciado e Mensurável quando
A Direção assume a responsabilidade de comunicar as políticas de controle interno, delega responsabilidades e aloca recursos suficientes para manter o ambiente em alinhamento com mudanças significativas. Foi estabelecido um ambiente de controle de informação proativo que contempla o comprometimento com a qualidade e a conscientização da segurança de TI. Um conjunto completo de políticas, procedimentos e padrões tem sido desenvolvido, mantido e comunicado e é uma combinação de boas práticas internas. Foi estabelecida uma estrutura para implementação e subsequente verificação de conformidade.

5 Otimizado quando
O ambiente de controle de informação está alinhado com a visão e a estrutura de gerenciamento estratégico, é frequentemente revisado, atualizado e continuamente melhorado. Especialistas internos e externos são designados para assegurar que as melhores práticas industriais estejam sendo adotadas com relação a diretrizes de controle e técnicas de comunicação. O monitoramento, a autoavaliação e a verificação de conformidade estão sendo difundidos na organização. A tecnologia é utilizada para manter as bases de conhecimento de política e conscientização e para otimizar a comunicação através de ferramentas de automação comercial e de treinamento em computador.

Descrição do Processo

PO7 Gerenciar os Recursos Humanos de TI

Adquirir, manter e motivar uma força de trabalho competente para criar e entregar serviços de TI para o negócio. Isso é alcançado seguindo práticas definidas e acordadas de recrutamento, treinamento, avaliação de desempenho, promoção e desligamento. Esse processo é crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas.



Controle sobre o seguinte processo de TI:

Gerenciar os Recursos Humanos de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

ter pessoas competentes e motivadas para criar e entregar serviços de TI

com foco em:

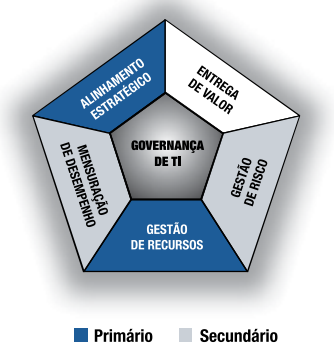
admitir e treinar pessoal, motivar através de planos de carreira claros, atribuir funções coerentes com as habilidades, estabelecer um processo de revisão, criar descrições de cargos e assegurar a consciência da dependência de indivíduos.

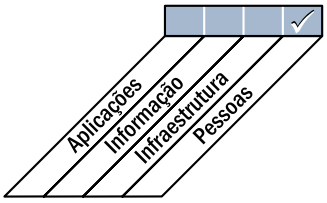
é alcançado por:

- Revisão do desempenho do pessoal
- Admissão e treinamento do pessoal de TI para sustentarem os planos táticos de TI
- Mitigar o risco de dependência excessiva de recursos-chave

e medido por:

- Nível de satisfação das partes interessadas com as experiências e habilidades da equipe de TI
- Rotatividade da equipe de TI
- Percentual da equipe de TI certificado de acordo com as necessidades da função





Objetivos de Controle Detalhados

PO7 Gerenciar os Recursos Humanos de TI

PO7.1 Recrutamento e Retenção de Pessoal
Assegurar que os processos de recrutamento de pessoal estejam alinhados com as políticas e os procedimentos de pessoal da organização (por exemplo, admissão, ambiente de trabalho positivo e orientação). Implementar processos para assegurar que a organização tenha uma força de trabalho de TI apropriada e com as habilidades necessárias para atingir os objetivos da organização.

PO7.2 Competências Pessoais
Verificar regularmente se o pessoal tem as competências necessárias para exercer suas funções com base na formação, no treinamento e/ou na experiência. Definir os requisitos centrais de competência em TI e verificar se estão sendo mantidos através de programas de qualificação e certificação onde apropriado.

PO7.3 Preenchimento de Vagas
Definir, monitorar e supervisionar funções, responsabilidades e estrutura de compensação do pessoal, incluindo a necessidade de adesão aos processos e políticas do gerenciamento, ao código de ética profissional e às práticas profissionais. O nível de supervisão deve estar alinhado com a importância da posição e a extensão das responsabilidades atribuídas.

PO7.4 Treinamento do Pessoal
Prover ao pessoal de TI treinamento apropriado para manter conhecimento, especializações, habilidades, conscientização sobre controles internos e segurança no nível exigido para atingir os objetivos organizacionais.

PO7.5 Dependência de Indivíduos
Minimizar a exposição à dependência crítica de pessoas-chave através de captação do conhecimento (documentação), compartilhamento de conhecimento, planejamento da sucessão e desenvolvimento de possíveis substitutos para o papel e a função determinados.

PO7.6 Procedimentos de Liberação de Pessoal
Incluir análise de antecedentes no processo de recrutamento de TI. A extensão e a frequência de revisão periódica dessas análises dependem da confidencialidade e/ou da importância da função e devem ser aplicadas aos funcionários, prestadores de serviço e fornecedores.

PO7.7 Avaliação de Desempenho Profissional
Exigir periodicamente a realização de avaliação dos objetivos individuais derivados dos objetivos da organização, padrões estabelecidos e responsabilidades específicas do cargo. Os funcionários devem receber orientação de desempenho e conduta sempre que apropriado.

PO7.8 Mudança e Desligamento de Cargo
Deliberar ações expedientes conforme mudanças de cargo, especialmente no caso de desligamentos. A transferência de conhecimento precisa ser providenciada, as responsabilidades redistribuídas e os direitos de acesso eliminados, para que os riscos sejam minimizados e seja assegurada a continuidade da função.

Diretrizes de Gerenciamento

PO7 Gerenciar os Recursos Humanos de TI

Origem	Entrada
PO4	Organização e relacionamentos de TI; Documentação de papéis, funções e responsabilidades;
AI1	Estudo de viabilidade dos requisitos de negócio

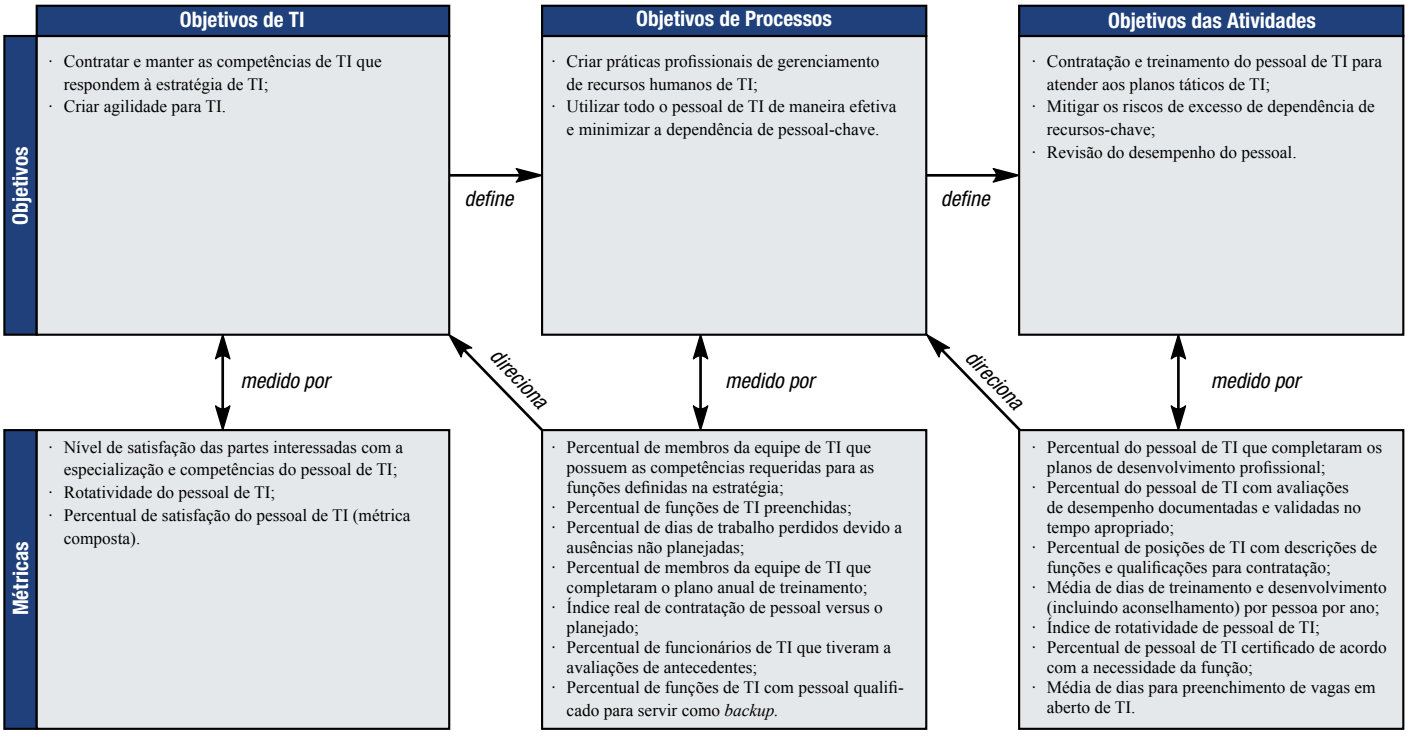
Saída	Destino						
Políticas e procedimentos de RH para TI;	PO4						
Matriz de habilidades em TI;	PO4	PO10					
Descrição de cargos;	PO4						
Habilidades e competências de usuários, incluindo treinamento;	DS7						
Requisitos de treinamentos específicos;	DS7						
Papéis, funções e responsabilidades	ALL						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Identificar habilidades, descrição de cargos, faixas salariais e comparações de desempenho individual com o mercado *(benchmarks)* para TI;		C		A		C	C	C	R	C	
Executar políticas e procedimentos de RH relevantes para TI (recrutamento, contratação, compensação, treinamento, avaliação, promoção e desligamento)				A		R	R	R	R	R	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

PO7 Gerenciar os Recursos Humanos de TI

O gerenciamento do processo de ***"Gerenciar os Recursos Humanos de TI"*** que satisfaça ao requisito do negócio para a TI de ***"ter pessoas competentes e motivadas para criar e entregar serviços de TI"*** é:

0 Inexistente quando
Não há conscientização sobre a importância de alinhamento do gerenciamento de recursos humanos de TI com o processo de planejamento tecnológico da organização. Não há pessoa ou grupo formalmente responsável pelo gerenciamento dos recursos humanos de TI.

1 Inicial/*Ad hoc* quando
A administração reconhece a necessidade de gerenciamento dos recursos humanos de TI. O processo de gerenciamento de recursos humanos é informal e reativo. O processo de recursos humanos de TI está operacionalmente focado na admissão e no gerenciamento de pessoal de TI. Está sendo desenvolvida consciência do impacto das rápidas mudanças tecnológicas e de negócios e das soluções cada vez mais complexas que resultam em necessidade de novas habilidades e níveis mais elevados de competência.

2 Repetível, porém Intuitivo quando
Há uma abordagem tática na admissão e no gerenciamento do pessoal de TI impulsionada pelas necessidades específicas de projetos, ao invés do entendimento da diferença de disponibilidades interna e externa de pessoal especializado. É realizado treinamento informal para o pessoal novo, que a partir de então recebe treinamento somente quando necessário.

3 Processo Definido quando
Existe um processo definido e documentado para o gerenciamento dos recursos humanos de TI. Há um plano de gerenciamento de recursos humanos de TI. Existe uma abordagem estratégica para admissão e gerenciamento do pessoal de TI. Um plano de treinamento formal é projetado para atender às necessidades dos recursos humanos de TI. É estabelecido um programa de reciclagem visando expandir as habilidades técnicas e de gerenciamento de negócio.

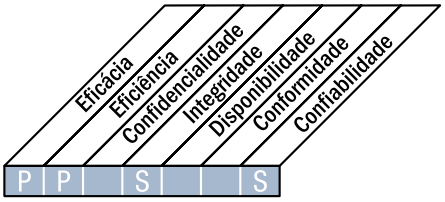
4 Gerenciado e Mensurável quando
A responsabilidade pelo desenvolvimento e a manutenção de um plano de gerenciamento de recursos humanos de TI está atribuída a uma pessoa ou grupo de pessoas com experiência e habilidades para desenvolver e manter o plano. O processo de desenvolvimento e gerenciamento do plano de gerenciamento de recursos humanos de TI responde às mudanças. A organização tem medidas padronizadas que permitem identificar desvios do plano de gerenciamento de recursos humanos de TI, com ênfase especial no gerenciamento do aumento e da rotatividade de pessoal de TI. São estabelecidas revisões de desempenho e compensação, comparações com outras organizações de TI e com as melhores práticas da indústria. O gerenciamento de recursos humanos de TI é proativo e considera planos de desenvolvimento de carreira.

5 Otimizado quando
O plano de gerenciamento de recursos humanos de TI é constantemente atualizado para atender às exigências de mudança do negócio. O gerenciamento de recursos humanos de TI é integrado com o planejamento tecnológico, assegurando ótimo desenvolvimento e uso das habilidades disponíveis de TI. O gerenciamento de recursos humanos de TI está integrado e em consonância com a direção estratégica da entidade. Os componentes do gerenciamento de recursos humanos de TI estão de acordo com as melhores práticas da indústria, tais como revisão do desempenho e compensação, participação em fóruns da indústria, transferência do conhecimento, treinamento e orientação. Os programas de treinamento são desenvolvidos para todos os novos produtos e padrões tecnológicos antes da aplicação na organização.

Descrição do Processo

PO8 Gerenciar a Qualidade

Deve ser desenvolvido e mantido um sistema de gestão da qualidade, que inclua padrões e processos comprovados de desenvolvimento e aquisição. Isso é feito através de planejamento, implementação e manutenção de um sistema de gestão de qualidade que gere requisitos, procedimentos e políticas de qualidade claros. Requisitos de qualidade devem ser definidos e comunicados em indicadores quantificáveis e atingíveis. A melhoria contínua pode ser alcançada por constante monitoramento, análise e atuação sobre desvios e na comunicação dos resultados às partes interessadas. A gestão da qualidade é essencial para assegurar que a TI esteja fornecendo valor para o negócio, melhoria contínua e transparência para as partes interessadas.



Controle sobre o seguinte processo de TI:

Gerenciar a Qualidade

que satisfaça aos seguintes requisitos do negócio para a TI:

melhorar continuamente e de forma mensurável a qualidade dos serviços entregues pela TI

com foco em:

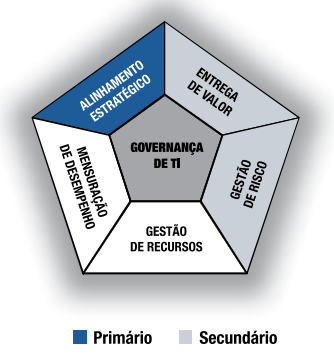
definir um sistema de gerenciamento de qualidade (SGQ), monitorar continuamente o desempenho baseado em objetivos predefinidos e implementar um programa de melhoria contínua dos serviços de TI

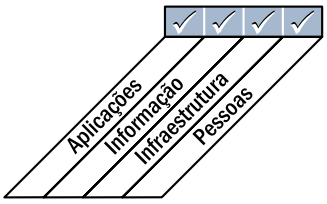
é alcançado por:

- Definição de práticas e padrões de qualidade
- Monitoração e revisão dos desempenhos interno e externo comparado às práticas e padrões de qualidade definidas
- Melhoria contínua do SGQ

e medido por:

- Percentual das partes interessadas satisfeitas com a qualidade da TI (avaliado segundo a importância)
- Percentual dos processos de TI formalmente revisados pelo processo de garantia de qualidade periodicamente e que atingem metas e objetivos de qualidade
- Percentual dos processos que recebem revisões de garantia de qualidade *(QA-Quality Assurance)*





Objetivos de Controle Detalhados

PO8 Gerenciar a Qualidade

PO8.1 Sistema de Gerenciamento de Qualidade (SGQ)
Estabelecer e manter um SGQ que forneça uma abordagem padronizada, formal e contínua de gerenciamento da qualidade e alinhada com os requisitos de negócios. O SGQ identifica os requisitos e critérios de qualidade, processos-chave de TI (incluindo sequência e interação), políticas, critérios e métodos para definir, detectar, corrigir e prevenir não-conformidades. O SGQ deve definir a estrutura organizacional para a gestão da qualidade, abrangendo papéis, tarefas e responsabilidades. Todas as áreas-chave desenvolvem seus planos de qualidade em linha com os critérios e políticas e mantêm um histórico dos dados. Monitorar e medir a efetividade e a aceitação do SGQ e melhorá-lo quando necessário.

PO8.2 Padrões e Práticas de Qualidade de TI
Identificar e manter práticas, procedimentos e padrões para os processos-chave de TI de forma a orientar a organização para alcançar as intenções do SGQ. Utilizar as melhores práticas da indústria como referência na melhoria e personalização das práticas de qualidade da organização.

PO8.3 Padrões de Desenvolvimento e Aquisição
Adotar e manter padrões para todos os desenvolvimentos e aquisições que sigam o ciclo de vida da entrega final e incluir liberações formais para os marcos-chave *(milestones)* de acordo com critérios de aceitação definidos. Questões a considerar incluem padrões de codificação, convenção de nomes, formato de arquivos, padrões de projeto de arquitetura e dicionário de dados, padrões de interface de usuário, interoperabilidade, eficiência no desempenho de sistemas, escalabilidade, padrões de desenvolvimento e testes, validações comparadas com requisitos, planos de teste, testes unitários, testes de regressão e testes integrados.

PO8.4 Foco no Cliente
Assegurar que a gestão de qualidade tenha como foco o cliente determinando seus requisitos e os mantenha alinhados com os padrões e práticas de TI. Papéis e responsabilidades definidos para a resolução de conflitos entre usuário/cliente e a organização de TI.

PO8.5 Melhoria Contínua
Um plano geral de qualidade que promove a melhoria continua é mantido e comunicado regularmente.

PO8.6 Medição, Monitoramento e Revisão da Qualidade
Definir, planejar e implementar métricas para monitorar continuamente o atendimento ao SGQ, bem como o valor que o SGQ fornece. Medição, monitoramento e armazenamento de informações devem ser utilizados pelo proprietário do processo para tomar medidas corretivas e preventivas.

Diretrizes de Gerenciamento

PO8 Gerenciar a Qualidade

Origem	Entrada
PO1	Planejamento estratégico de TI;
PO10	Planejamentos detalhados de projetos;
ME1	Planos de ação para remediações

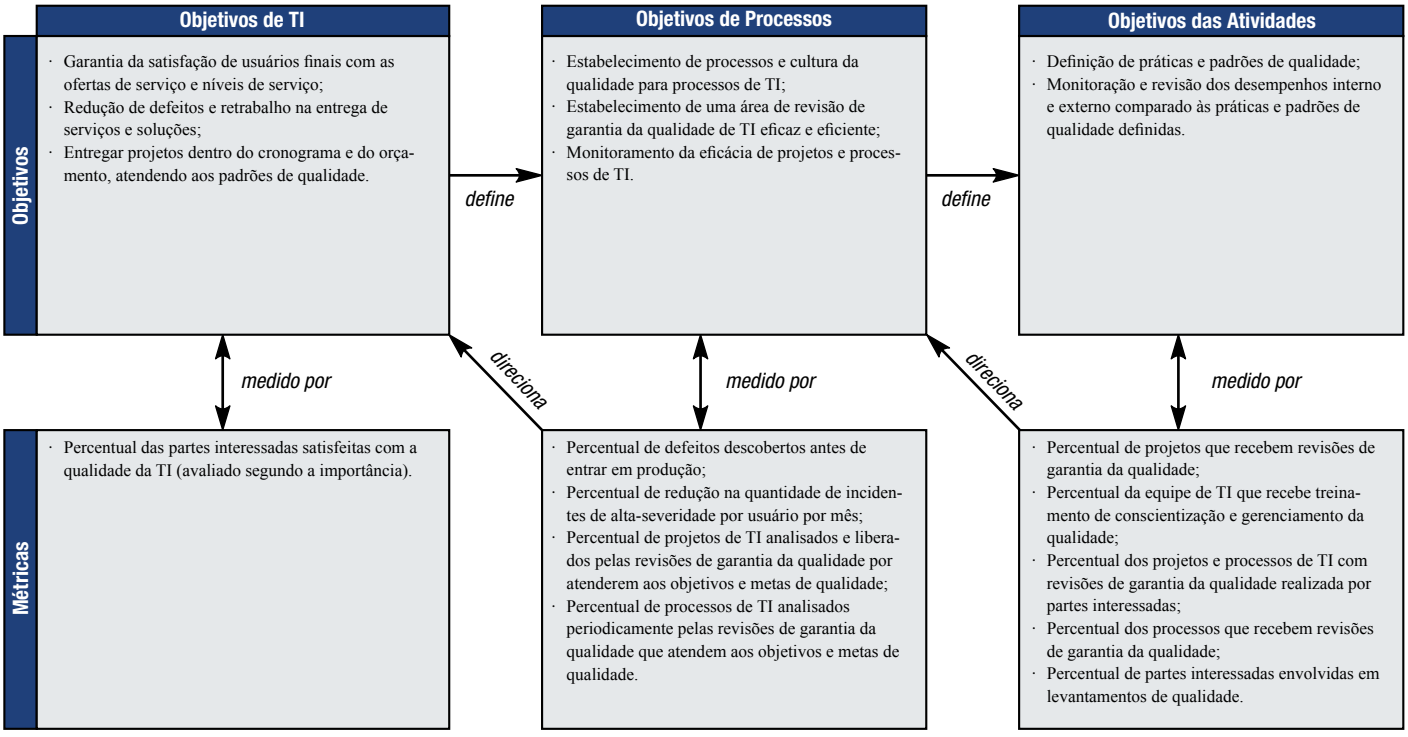
Saída	Destino						
Padrões para aquisição;	AI1	AI2	AI3	AI5	DS2		
Padrões para desenvolvimento;	PO10	AI1	AI2	AI3	AI7		
Padrões de qualidade e requisitos de métricas;	ALL						
Ações de melhoria da qualidade	PO4	AI6					

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir um sistema de gerenciamento da qualidade (SGQ);	C		C	A/R	I	I	I	I	I	I	C
Estabelecer e manter um sistema de gerenciamento da qualidade;	I	I	I	A/R	I	C	C	C	C	C	C
Criar e comunicar padrões de qualidade para a organização;		I		A/R	I	C	C	C	C	C	C
Criar e manter o planejamento de qualidade para melhoria contínua;				A/R	I	C	C	C	C	C	C
Medir, monitorar e revisar criticamente a conformidade com os objetivos de qualidade				A/R	I	C	C	C	C	C	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

PO8 Gerenciar a Qualidade

O gerenciamento do processo de ***"Gerenciar a Qualidade"*** que satisfaça ao requisito do negócio para a TI de ***"melhorar continuamente e de forma mensurável a qualidade dos serviços entregues pela TI"*** é:

0 Inexistente quando
A organização carece de um processo de planejamento de SGQ (Sistema de Gerenciamento da Qualidade) e de uma metodologia de ciclo de desenvolvimento de sistema. A Direção Geral e a Direção de TI não reconhecem a necessidade de um programa de qualidade. Os projetos e operações nunca são revisados com base na qualidade.

1 Inicial/*Ad hoc* quando
Há consciência por parte da Direção da necessidade de um SGQ. O SGQ é impulsionado por indivíduos onde ele se faz necessário. A Direção faz julgamentos informais acerca da qualidade.

2 Repetível, porém Intuitivo quando
Um programa está sendo estabelecido para definir e monitorar as atividades do SGQ dentro da TI. As atividades de SGQ estão focadas em iniciativas de projetos e processos de TI e não nos processos de toda a organização.

3 Processo Definido quando
Um processo de SGQ definido é comunicado pela Direção e envolve a Direção de TI e das áreas usuárias. Um programa de ensino e treinamento é implantado para orientar todos os níveis da organização sobre a qualidade. Expectativas básicas de qualidade foram definidas e compartilhadas entre os projetos e na organização da TI. Ferramentas e práticas de controle de qualidade comuns começam a ser utilizadas. Pesquisas de satisfação com a qualidade são planejadas e realizadas ocasionalmente.

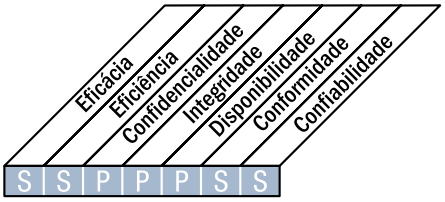
4 Gerenciado e Mensurável quando
O SGQ é considerado em todos os processos, aqueles que dependem de terceiros. Uma base de conhecimento padronizada está sendo estabelecida por métricas de qualidade. Métodos de análise de custo benefício são utilizados para justificar as iniciativas do SGQ. Começam a ser feitas comparações com a indústria e concorrentes *(benchmarking)*. Um programa de ensino e treinamento foi instituído para ensinar qualidade a todos os níveis da organização. Ferramentas e práticas estão sendo padronizadas, e análises de causa-raiz são aplicadas periodicamente. Levantamentos de satisfação da qualidade são constantemente realizados. Há um programa padronizado para medição de qualidade implantado e bem estruturado. A Direção de TI está consolidando uma base de conhecimento para métricas de qualidade.

5 Otimizado quando
O SGQ está integrado e é imposto em todas as atividades da TI. Os processos de SGQ são flexíveis e adaptáveis às mudanças no ambiente de TI. A base de conhecimento para métricas de qualidade está otimizada com as melhores práticas externas. Uma comparação com padrões externos *(benchmarking)* é rotineiramente realizada. A pesquisa de satisfação com a qualidade é um processo que leva à análise da causa-raiz e a ações de melhoria. Há garantia formal quanto ao nível do processo de controle de qualidade.

Descrição do Processo

PO9 Avaliar e Gerenciar os Riscos de TI

Criar e manter uma estrutura de gestão de risco. Esta estrutura documenta um nível comum e acordado de riscos de TI, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis.



Controle sobre o seguinte processo de TI:

Avaliar e gerenciar os riscos de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

analisar e comunicar os riscos de TI e seus possíveis impactos nos processos e objetivos de negócio

com foco em:

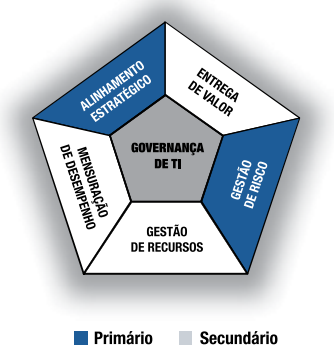
desenvolver uma estrutura de gerenciamento de risco integrada às estruturas corporativa e operacional de gerenciamento de risco, avaliação, mitigação e comunicação de risco residual

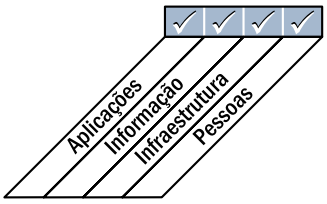
é alcançado por:

- Garantia de que o gerenciamento de risco esteja completamente integrado aos processos gerenciais, interna e externamente, e seja aplicado de forma consistente
- Realização de avaliações de risco
- Recomendação e comunicação de planos de ação de remediação dos riscos.

e medido por:

- Percentual de objetivos críticos de TI cobertos pela avaliação de risco
- Percentual de riscos críticos de TI identificados que tenham planos de ação desenvolvidos
- Percentual dos planos de ação de gestão de risco aprovados para implementação





Objetivos de Controle Detalhados

PO9 Avaliar e Gerenciar os Riscos de TI

PO9.1 Alinhamento da gestão de riscos de TI e de Negócios
Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).

PO9.2 Estabelecimento do Contexto de Risco
Estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados.

PO9.3 Identificação de Eventos
Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.

PO9.4 Avaliação de Risco
Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização.

PO9.5 Resposta ao Risco
Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.

PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco
Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo a identificação de custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a Alta Direção.

Diretrizes de Gerenciamento

PO9 Avaliar e Gerenciar os Riscos de TI

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI; Portfólio de serviços de TI;
PO10	Plano de gerenciamento de risco de projetos;
DS2	Riscos de fornecedores;
DS4	Resultados dos testes de contingência;
DS5	Vulnerabilidades e ameaças de segurança;
ME1	Histórico de eventos e tendências de riscos;
ME4	Grau aceitável corporativo de riscos de TI

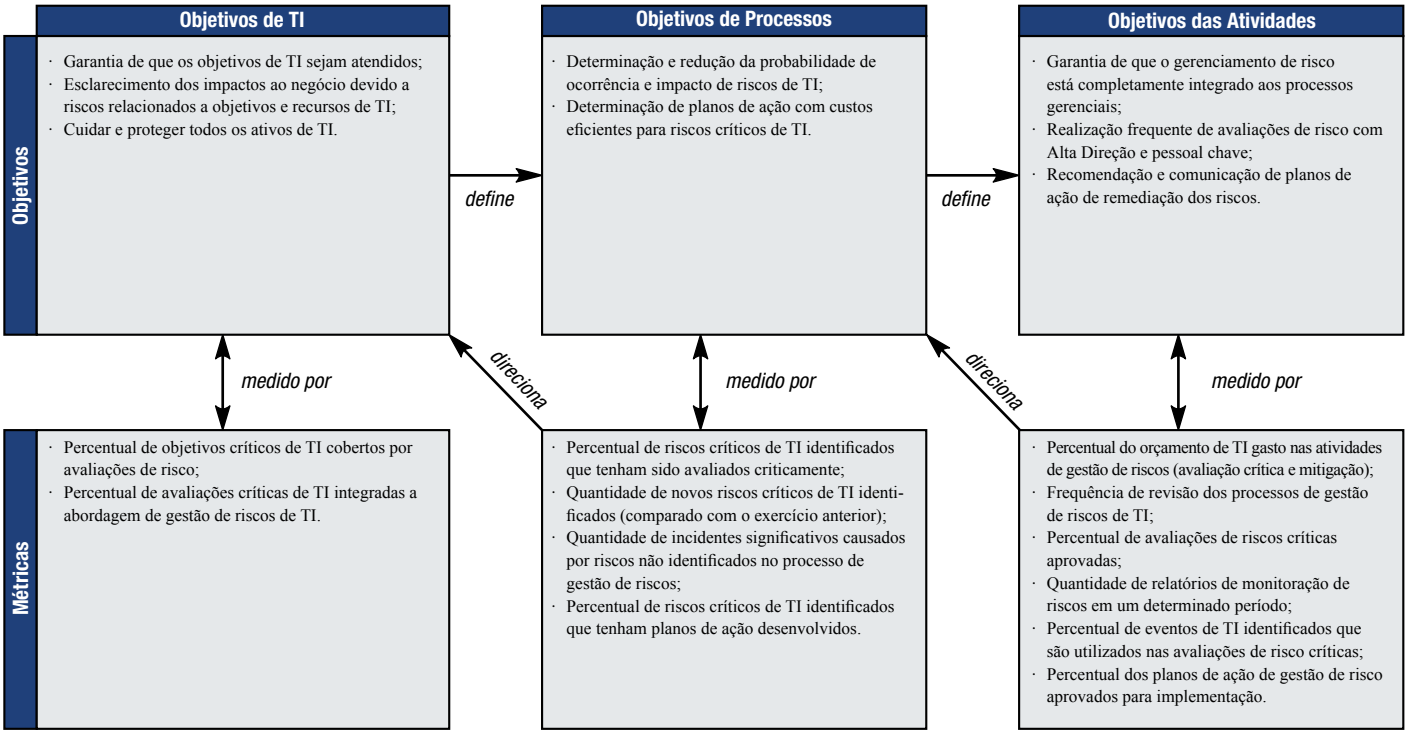
Saída	Destino						
Avaliação crítica de riscos;	PO1	DS4	DS5	DS12	ME4		
Relatório de riscos;	ME4						
Diretrizes para a gestão de riscos de TI;	PO6						
Planos de ação para remediação de riscos de TI	PO4	AI6					

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Promover o alinhamento da gestão de riscos (por exemplo: avaliação de riscos);	A	R/A	C	C	R/A	I					I
Entender os objetivos estratégicos de negócio relevantes;		C	C	R/A	C	C					I
Entender os objetivos de processos de negócio relevantes;				C	C	R/A					I
Identificar objetivos internos de TI e estabelecer contexto de risco;					R/A		C	C	C		I
Identificar eventos associados com objetivos [alguns eventos são orientados ao negócio (negócio é A); alguns são orientados a TI (TI é A, negócio é C)];	I			A/C	A	R	R	R	R		C
Avaliar criticamente os riscos associados com eventos;				A/C	A	R	R	R	R		C
Avaliar respostas aos eventos;	I	I	A	A/C	A	R	R	R	R		C
Planejar e priorizar as atividades de controle;	C	C	A	A	R	R	C	C	C		C
Aprovar e assegurar o financiamento de planos de ações para riscos;		A	A		R	I	I	I	I		I
Manter e monitorar os planos de ações para riscos	A	C	I	R	R	C	C	C	C	C	R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

PO9 Avaliar e Gerenciar os Riscos de TI

O gerenciamento do processo de ***"Avaliar e Gerenciar os Riscos de TI"*** que satisfaça ao requisito do negócio para a TI de ***"analisar e comunicar os riscos de TI e seus potenciais impactos nos processos e objetivos de negócio"*** é:

0 Inexistente quando
Não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços de TI.

1 Inicial/ *Ad hoc* quando
Os riscos de TI são considerados de forma *ad hoc*. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Avaliações de risco são às vezes identificadas em um plano de projeto, mas raramente atribuídas aos gerentes correspondentes. Riscos específicos relacionados a TI, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de TI que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de TI são importantes e devem ser considerados.

2 Repetível, porém Intuitivo quando
Existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns gerentes de projeto. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.

3 Processo Definido quando
Uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos–chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela gestão de riscos estão definidas nas descrições de cargo.

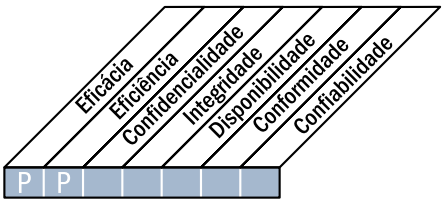
4 Gerenciado e Mensurável quando
A avaliação e a gestão de risco são procedimentos padronizados. As exceções do processo de gestão de risco são relatadas à Diretoria de TI. A gestão de risco de TI é uma responsabilidade da Alta Direção. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de TI. O comitê executivo é avisado das mudanças no ambiente de negócios e de TI que podem afetar consideravelmente os cenários de riscos relacionados a TI. A Diretoria é capaz de monitorar a posição do risco e tomar decisões fundamentadas no nível de exposição aceitável. Todos os riscos identificados têm um responsável definido, e o comitê executivo e a Diretoria de TI estabeleceram os níveis de risco que a organização irá tolerar. A área de TI desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos. A área de TI aloca recursos para um projeto de gestão de risco operacional a fim de reavaliar periodicamente os riscos. Um banco de dados de gestão de risco é estabelecido, e uma parte dos processos de gerenciamento de risco está começando a ser automatizada. A área de TI estuda estratégias de mitigação de riscos.

5 Otimizado quando
O gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. É recebida orientação de lideranças da área, e a organização de TI participa de grupos de discussão para troca de experiências. A gestão de risco está totalmente integrada às operações de negócio e de TI, é bem aceita e envolve extensivamente os usuários dos serviços de TI. A Direção de TI detecta e age quando grandes decisões operacionais e de investimentos de TI são tomadas sem considerar o plano de gestão de risco. A Direção de TI avalia continuamente as estratégias de mitigação de risco.

Descrição do Processo

PO10 Gerenciar Projetos

Estabelecer um programa e uma estrutura de gestão de projeto para o gerenciamento de todos os projetos de TI. Essa estrutura deve assegurar a correta priorização e a coordenação de todos os projetos. A estrutura deve incluir um plano mestre, atribuição de recursos, definição dos resultados a serem entregues, aprovação dos usuários, uma divisão por fases de entrega, garantia da qualidade, um plano de teste formal e uma revisão pós-implementação para assegurar a gestão de risco do projeto e a entrega de valor para o negócio. Esta abordagem reduz o risco de custos inesperados e de cancelamentos de projeto, aperfeiçoa a comunicação, melhora o envolvimento das áreas de negócio e dos usuários finais, assegura o valor e a qualidade dos resultados do projeto e maximiza a contribuição para os programas de investimentos em TI.



Controle sobre o seguinte processo de TI:

Gerenciar Projetos

que satisfaça aos seguintes requisitos do negócio para a TI:

entregar resultados de projetos dentro do tempo, do orçamento e da qualidade acordados

com foco em:

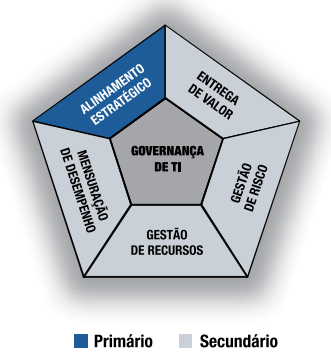
aplicar aos projetos de TI um programa definido e uma abordagem de gestão de projetos que permitam a participação das partes interessadas e a monitoração do andamento e dos riscos do projeto

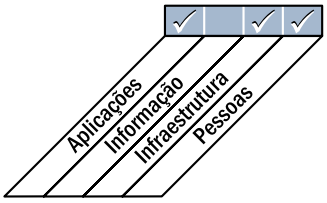
é alcançado por:

- Definição e implantação de programas, estruturas e abordagens de projeto
- Publicação de diretrizes de gestão de projeto
- Realização de planejamento de projeto para todo o portfólio de projetos

e medido por:

- Percentual de projetos que atendem às expectativas das partes interessadas (prazo, orçamento e escopo – ponderados de acordo com a importância)
- Percentual de projetos que foram revisados após a implementação
- Percentual de projetos que seguem os padrões e as práticas de gerenciamento de projetos





Objetivos de Controle Detalhados

PO10 Gerenciar Projetos

PO10.1 Estrutura de Gestão de Programas
Manter o programa de projetos (relacionados ao portfólio de programas de investimentos em TI) identificando, definindo, avaliando, priorizando, selecionando, iniciando, gerenciando e controlando projetos. Assegurar que os projetos sustentem os objetivos dos programas. Coordenar as atividades e interdependências de múltiplos projetos, gerenciar a contribuição de todos os projetos de um programa para os resultados esperados e resolver requisitos e conflitos de recursos.

PO10.2 Estrutura de Gestão de Projetos
Estabelecer e manter uma estrutura de gestão de projetos que defina o escopo e a abrangência dos projetos gerenciados, bem como os métodos a serem adotados e aplicados a cada projeto iniciado. A estrutura e as metodologias de suporte devem ser integradas aos processos de gerenciamento de programas.

PO10.3 Abordagem da Gestão de Projetos
Estabelecer uma abordagem de gestão de projetos adequada ao tamanho, à complexidade e aos requisitos regulatórios de cada projeto. A estrutura de governança de projeto deve incluir os papéis, as responsabilidades e o acompanhamento dos resultados do patrocinador do programa, patrocinador do projeto, comitê diretor, coordenador e gerente do projeto e os mecanismos pelos quais eles podem cumprir com essas responsabilidades (como relatórios e revisões de estágios do projeto). Assegurar que todos os projetos de TI tenham patrocinadores com autoridade suficiente para serem seus proprietários dentro do programa estratégico geral.

PO10.4 Comprometimento das Partes Interessadas
Obter comprometimento e participação das partes interessadas afetadas na definição e na execução do projeto dentro do contexto do programa de investimento geral de TI.

PO10.5 Declaração do Escopo do Projeto
Definir e documentar a natureza e o escopo do projeto, visando confirmar e desenvolver um entendimento comum do escopo do projeto com as partes interessadas e quanto ao relacionamento com outros projetos de um programa de investimento em TI. A definição deve ser formalmente aprovada pelo patrocinador do programa e pelo patrocinador do projeto antes de seu início.

PO10.6 Fase de Início do Projeto
Assegurar que a fase de início do projeto seja formalmente aprovada e comunicada a todas as partes interessadas. A aprovação da fase de início deve ser baseada nas decisões da governança do programa. A aprovação das fases subsequentes deve ser baseada na revisão e na aceitação dos resultados entregues da fase anterior e na aprovação de um estudo de caso atualizado na próxima revisão geral do programa. No caso de uma sobreposição de fases, deve ser estabelecido um ponto de aprovação pelos patrocinadores do programa e do projeto para autorizar a continuidade.

PO10.7 Plano Integrado de Projeto
Estabelecer um plano integrado de projeto formalizado e aprovado (que abranja recursos de negócio e de sistemas de informação) para orientar a execução e o controle em todas as etapas do projeto. As atividades e interdependências de múltiplos projetos dentro de um programa devem ser entendidas e documentadas. O plano de projeto deve passar por manutenção durante todas as etapas do projeto. O plano de projeto e as alterações feitas nele devem ser aprovados de acordo com a estrutura de governança do programa e do projeto.

PO10.8 Recursos do Projeto
Definir responsabilidades, relacionamentos, autoridades e critérios de desempenho para os membros da equipe de projeto e especificar a base de aquisição e atribuição de funcionários e/ou prestadores de serviço competentes para o projeto. A contratação de produtos e serviços necessários para cada projeto deve ser planejada e gerenciada para atingir os objetivos do projeto utilizando as práticas de contratação da organização.

PO10.9 Gestão de Risco do Projeto
Eliminar ou minimizar riscos específicos associados a cada projeto através de um processo sistemático de planejamento, identificação, análise, resposta, monitoramento e controle de áreas ou eventos com potencial para causar mudanças indesejadas. Os riscos identificados pelo processo de gestão de projeto e os resultados esperados do projeto devem ser estabelecidos e centralmente registrados.

PO10.10 Plano de Qualidade de Projeto
Preparar um plano de gestão de qualidade que descreva o sistema de qualidade de projeto e como será implementado. O plano deve ser formalmente revisado e aceito por todas as partes envolvidas e então incorporado ao plano integrado de projeto.

PO10.11 Controle de Mudança de Projeto
Estabelecer um sistema de controle de mudança para cada projeto, de forma que todas as mudanças feitas no escopo original do projeto (como custo, cronograma, escopo e qualidade) sejam devidamente revisadas, aprovadas e incorporadas ao plano de projeto integrado em alinhamento com a estrutura de governança de programa e projeto.

PO10.12 Planejamento de métodos de validação
Identificar as atividades necessárias para suportar a validação de novos sistemas (ou suas modificações) durante o planejamento do projeto e incluí-las no plano integrado do projeto. As tarefas devem assegurar que os controles internos e aspectos de segurança atendam aos requisitos definidos.

PO10.13 Medição de Desempenho, Monitoramento e Reporte do Projeto
Avaliar o desempenho do projeto em comparação com critérios-chave (como escopo, cronograma, qualidade, custo e risco). Identificar qualquer desvio do plano. Avaliar o impacto dos desvios sobre o projeto e o programa. Reportar os resultados às principais partes interessadas. Recomendar, implementar e monitorar ações corretivas quando necessárias, em alinhamento com a estrutura de governança de projeto e programa.

PO10.14 Conclusão do Projeto
Exigir que, ao final de cada projeto, as partes interessadas apurem se o projeto gerou os resultados e benefícios planejados. Identificar e comunicar quaisquer atividades de destaque necessárias para obter os resultados esperados do projeto e os benefícios do programa. Identificar e documentar as lições aprendidas para usá-las em projetos e programas futuros.

Página intencionalmente deixada em branco

Diretrizes de Gerenciamento

PO10 Gerenciar Projetos

Origem	Entrada
PO1	Portfólio de projetos de TI;
PO5	Portfólio de projetos de TI atualizado;
PO7	Matriz de habilidades em TI;
PO8	Padrões para desenvolvimento;
AI7	Revisão pós-implementação

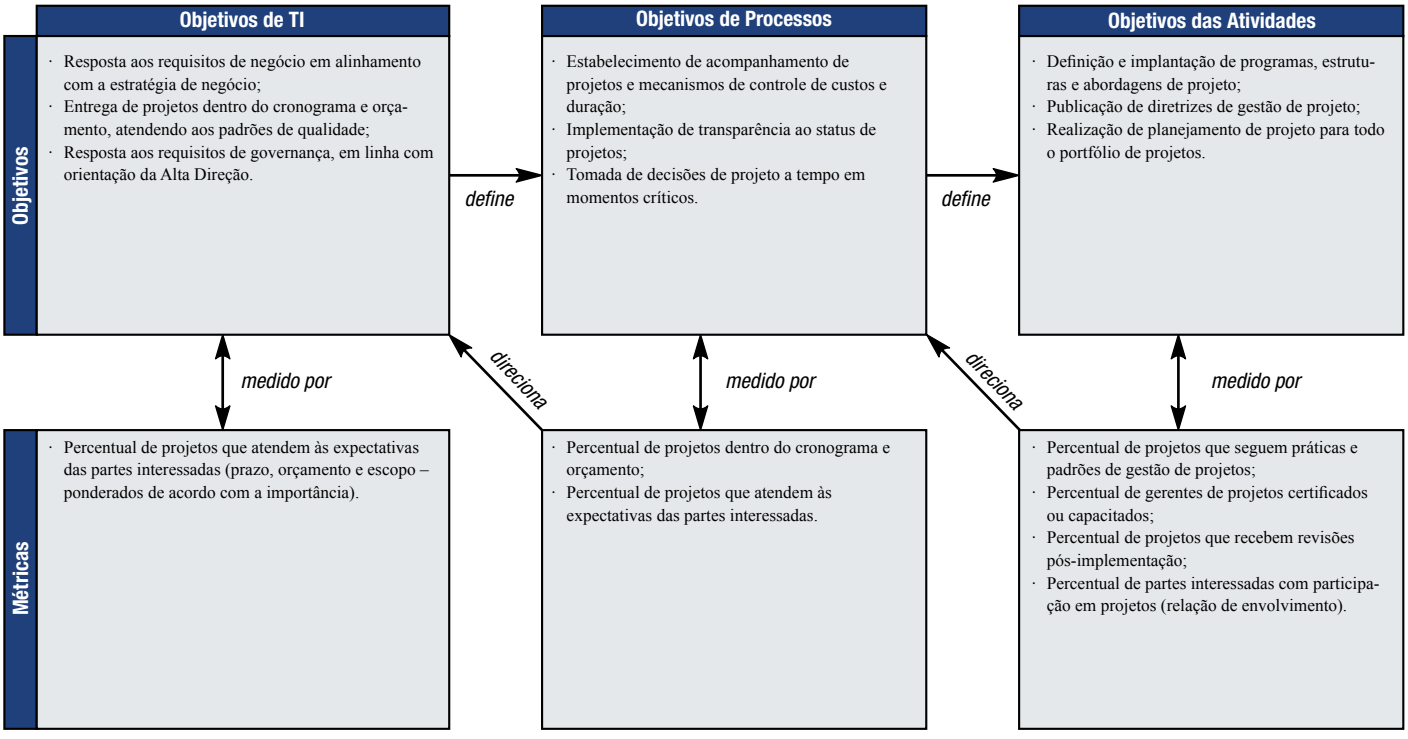
Saída	Destino						
Relatórios de desempenho de projetos;	ME1						
Plano de gerenciamento de risco de projetos;	PO9						
Diretrizes de gerenciamento de projetos;	AI1... AI7						
Planejamento detalhado de projetos;	PO8	AI1... AI7		DS6			
Portfólio de projetos de TI atualizado	PO1	PO5					

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir uma estrutura de gerenciamento de programas e portfólios para os investimentos de TI;	C	C	A	R						C	C
Estabelecer e manter uma estrutura de gerenciamento de projetos;	I	I	I	A/R	I	C	C	C	C	R	C
Estabelecer e manter um sistema de gerenciamento, monitoramento e acompanhamento de projetos de TI;	I	I	I	R		C	C	C	C	A/R	C
Criar cronogramas, planos de qualidade, orçamentos, planos de comunicação e planos de gerenciamento de riscos para projetos;			C	C	C	C	C	C	C	A/R	C
Assegurar a participação e compromisso das partes interessadas;	I		A	R	C						C
Assegurar o controle eficaz de projetos e de mudanças em projetos;			C	C		C	C	C		A/R	C
Definir e implementar uma metodologia de revisão e qualidade em projetos			I	C				I		A/R	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

PO10 Gerenciar Projetos

O gerenciamento do processo de ***"Gerenciar Projetos"*** que satisfaça ao requisito do negócio para a TI de ***"entregar resultados de projetos dentro do tempo, do orçamento e da qualidade acordados"*** é:

0 Inexistente quando
Técnicas de gerenciamento de projeto não são utilizadas e a organização não considera os impactos de negócio associados ao gerenciamento equivocado e as falhas no desenvolvimento de projetos.

1 Inicial/ *Ad hoc* quando
O uso de abordagens e técnicas de gestão de projeto dentro da TI é uma decisão a critério da Direção de TI. Há falta de comprometimento da Direção de TI com a propriedade e a gestão de projeto. Decisões críticas de gestão de projeto são tomadas sem o envolvimento do gestor de negócio ou dos usuários. Há pouco ou nenhum envolvimento dos clientes e usuários na definição dos projetos de TI. Não existe uma organização clara dentro da TI para o gerenciamento de projetos. Papéis e responsabilidades da gestão de projetos não estão definidos. Projetos, cronogramas e marcos são definidos superficialmente. A alocação de horas de pessoal e os custos do projeto não são controlados e comparados com os orçamentos.

2 Repetível, porém Intuitivo quando
A Alta Direção está consciente e comunica a necessidade de gestão de projeto de TI. A organização está em processo de desenvolvimento e utilização de algumas técnicas e métodos de gestão de projeto. Os projetos de TI têm definido informalmente os objetivos técnicos e de negócios. Há envolvimento limitado das partes interessadas no gerenciamento de projeto de TI. Foram desenvolvidas diretrizes iniciais contemplando muitos aspectos de gerenciamento de projeto. A aplicação das diretrizes de gerenciamento de projeto fica a cargo de cada gerente de projeto.

3 Processo Definido quando
O processo e a metodologia de gestão de projeto foram estabelecidos e comunicados. Os projetos de TI são definidos com objetivos técnicos e de negócio apropriados. Os gestores de TI e de negócio estão começando a se envolver e comprometer com a gestão dos projetos de TI. Uma estrutura de gestão de projetos está estabelecida dentro da TI, com papéis e responsabilidades iniciais definidos. Os projetos de TI são monitorados com marcos, cronograma, orçamento e medidas de desempenho definidos e atualizados. Há um treinamento em gestão de projetos disponível. Esse treinamento é principalmente o resultado de iniciativas individuais da equipe. Procedimentos de garantia da qualidade e atividades de pós-implementação foram definidos, mas não estão sendo amplamente aplicados pelos gerentes de TI. Os projetos estão começando a ser gerenciados como portfólios.

4 Gerenciado e Mensurável quando
A Direção requer a revisão de indicadores formais padronizados e lições aprendidas em cada projeto logo após sua conclusão. A gestão de projeto é medida e avaliada por toda a organização e não apenas dentro da TI. Melhorias na gestão de projeto são formalizadas e comunicadas, e os membros das equipes de projeto são treinados nessas melhorias. A área de TI implementou uma estrutura organizacional de projeto com papéis, responsabilidades e critérios de desempenho documentados. Foram estabelecidos critérios para avaliar o sucesso de cada marco. O valor e o risco são medidos e gerenciados antes, durante e depois da conclusão do projeto. Os projetos cada vez mais consideram os objetivos da empresa, não sendo apenas específicos de TI. Há um suporte sólido e ativo dos gestores e das partes interessadas. Há treinamento relevante de gestão de projeto planejado para a equipe do escritório de projetos e todas as áreas da TI.

5 Otimizado quando
Uma metodologia comprovada de ciclo de vida de projeto está implementada, imposta e integrada à cultura de toda a organização. Uma iniciativa constante para identificar e institucionalizar as melhores práticas de gestão de projetos foi implementada. Uma estratégia de TI para desenvolvimento de recursos e projetos operacionais está definida e implementada. Há uma coordenação de projetos integrada responsável pelos projetos e programas desde o início até a pós-implementação. Um planejamento corporativo de programas e projetos assegura que recursos de usuário e de TI sejam bem utilizados no apoio às iniciativas estratégicas.

Adquirir e Implementar

AI 1 Identificar Soluções Automatizadas

AI2 Adquirir e Manter *Software* Aplicativo

AI3 Adquirir e Manter Infraestrutura de Tecnologia

AI4 Habilitar Operação e Uso

AI5 Adquirir Recursos de TI

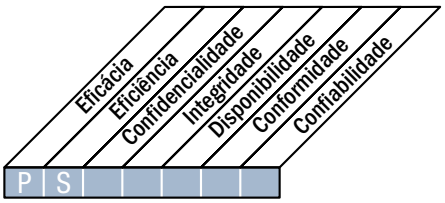
AI6 Gerenciar Mudanças

AI7 Instalar e Homologar Soluções e Mudanças

DESCRIÇÃO DE PROCESSO

AI1 Identificar Soluções Automatizadas

A necessidade de uma nova aplicação ou função requer uma análise prévia à aquisição ou ao desenvolvimento para assegurar que os requisitos de negócio sejam atendidos através de uma abordagem eficaz e eficiente. Este processo contempla a definição das necessidades, considera fontes alternativas, a revisão de viabilidade econômica e tecnológica, a execução das análises de risco e de custo-benefício e a obtenção de uma decisão final por "desenvolver" ou "comprar". Todos esses passos permitem às organizações minimizar os custos de aquisição e implementação de soluções e permitem ao negócio alcançar seus objetivos.



Controle sobre o seguinte processo de TI:

Identificar Soluções Automatizadas

que satisfaça aos seguintes requisitos do negócio para a TI:

traduzir os requisitos funcionais de negócio e de controle em um projeto eficiente e eficaz de soluções automatizadas

com foco em:

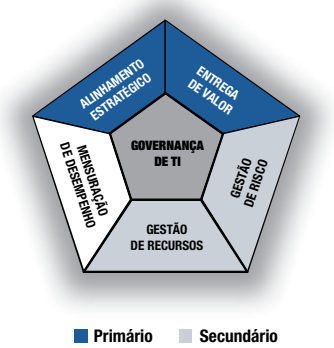
identificar soluções tecnicamente viáveis e com boa relação custo-benefício

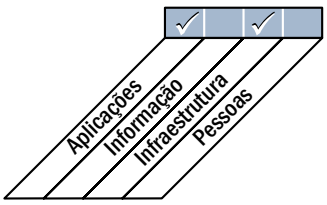
é alcançado por:

- Definição dos requisitos técnicos e de negócio
- Realização de estudos de viabilidade conforme definido nos padrões de desenvolvimento
- Aprovação (ou rejeição) de requisitos e resultados de estudos de viabilidade

e medido por:

- Quantidade de projetos nos quais os benefícios esperados não foram alcançados devido a premissas incorretas de viabilidade
- Percentual de estudos de viabilidade aceitos pelos respectivos proprietários de processos de negócios
- Percentual de usuários satisfeitos com as funcionalidades entregues





Objetivos de Controle Detalhados

AI1 Identificar Soluções Automatizadas

AI1 Definição e Manutenção de Requisitos Técnicos e Funcionais de Negócio
Identificar, priorizar, especificar e pactuar os requisitos técnicos e funcionais do negócio cobrindo todo escopo de todas as iniciativas necessárias para obter os resultados esperados do programa de investimentos em TI.

AI1.2 Relatório de Análise de Risco
Identificar, documentar e analisar os riscos associados aos requisitos de negócio e desenho de soluções como parte do processo de desenvolvimento dos requisitos da organização.

AI1.3 Estudo de Viabilidade e Formulação de Ações Alternativas
Desenvolver um estudo de viabilidade que examine a possibilidade de implementar os requisitos. O gerenciamento de negócios, suportado pela área de TI, deve avaliar a viabilidade e as ações alternativas e fazer recomendações ao patrocinador do negócio.

AI1.4 Decisão e Aprovação de Requisitos e Estudo de Viabilidade
O patrocinador do negócio aprova e sinaliza os requisitos técnicos e funcionais do negócio, bem como os relatórios de estudo de viabilidade em estágios-chave predeterminados. O patrocinador do negócio toma a decisão final quanto à escolha da solução e à forma de aquisição.

Diretrizes de Gerenciamento

AI1 Identificar Soluções Automatizadas

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI;
PO3	Atualizações periódicas do "estado da tecnologia"; Padrões tecnológicos;
PO8	Padrões para aquisição e desenvolvimento;
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
AI6	Descrição do processo de mudanças;
DS1	SLA´s;
DS3	Planejamento de desempenho e capacidade (requisitos)

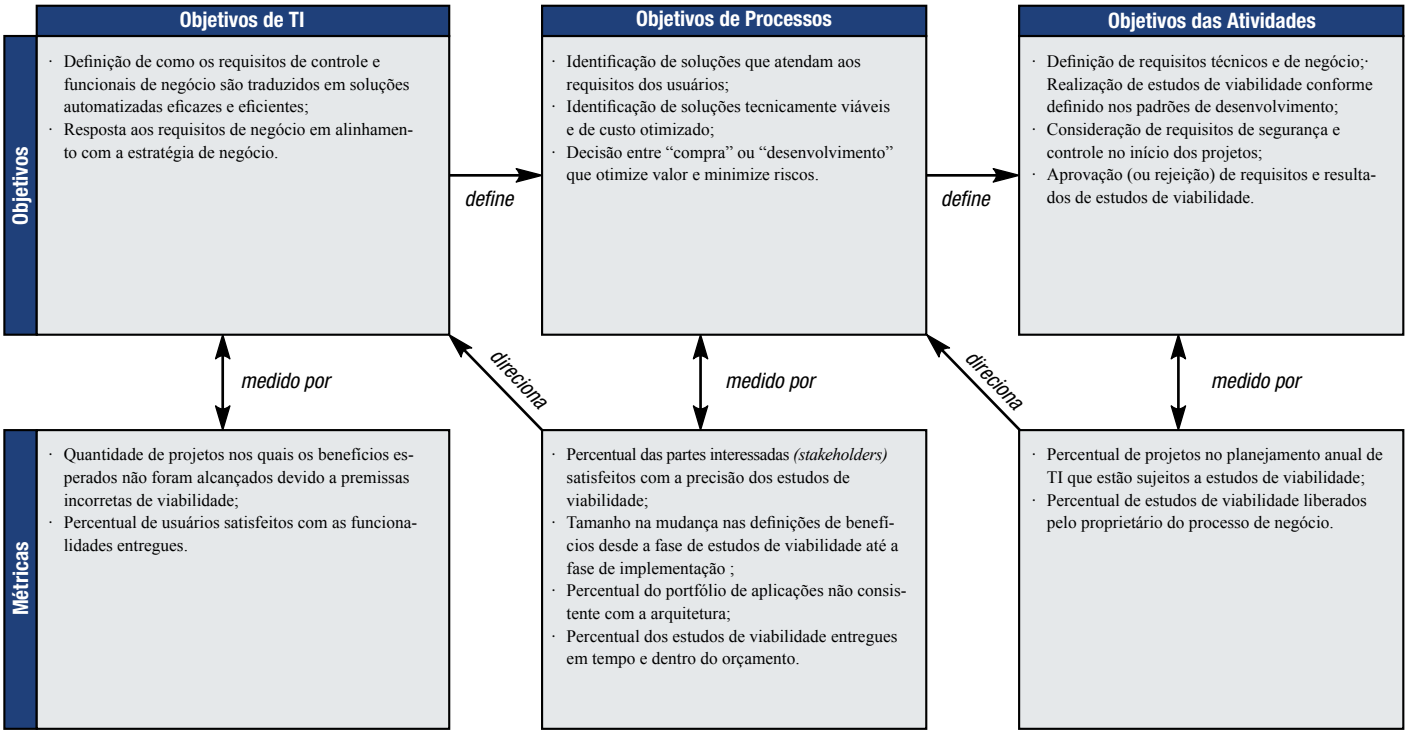
Saída	Destino						
Estudo de viabilidade dos requisitos de negócio	PO2	PO6	PO7	AI2	AI3	AI4	AI5

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir requisitos técnicos e funcionais de negócio;			C	C	R	C	R	R		A/R	I
Estabelecer processos para integridade/atualização de requisitos;				C		C		C		A/R	C
Identificar, documentar e analisar os riscos de processos de negócio;			A/R	R	R	R	C	R		R	C
Conduzir um estudo de viabilidade/avaliação de impacto para a implementação dos requisitos de negócio propostos;			A/R	R	R	C	C	C		R	C
Avaliar os benefícios das soluções propostas para a operação de TI;		I	R	A/R	R	I	I	I		R	
Avaliar os benefícios das soluções propostas para o negócio;			A/R	R		C	C	C	I	R	
Desenvolver um processo de aprovação de requisitos;			C	A		C	C	C		R	C
Aprovação e liberação das soluções propostas		C	A/R	R	R	C	C	C	I	R	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

AI1 Identificar Soluções Automatizadas

O gerenciamento do processo de ***"Identificar Soluções Automatizadas"*** que satisfaça ao requisito do negócio para a TI de ***"traduzir os requisitos funcionais de negócio e de controle em um projeto eficiente e eficaz de soluções automatizadas"*** é:

0 Inexistente quando
A organização não exige a identificação dos requisitos funcionais e operacionais para o desenvolvimento, implementação e modificação de soluções, tais como sistemas, serviços, infraestrutura, *software* e dados. A organização não tem consciência das soluções tecnológicas disponíveis potencialmente relevantes ao seu negócio.

1 Inicial/ *Ad hoc* quando
Há uma consciência da necessidade de definir os requisitos e identificar as soluções tecnológicas. Grupos de pessoas se reúnem para discutir informalmente as necessidades, e os requisitos nem sempre são documentados. As soluções são identificadas por indivíduos com base em conhecimento limitado do mercado ou em resposta a ofertas de fornecedores. Existe pesquisa ou análise minimamente estruturada da tecnologia disponível no mercado.

2 Repetível, porém Intuitivo quando
Existem alguns métodos intuitivos para identificar as soluções de TI, porém variam entre as diferentes áreas do negócio. As soluções são identificadas informalmente com base nas experiências e em conhecimentos internos da área de TI. O sucesso de cada projeto depende da experiência de poucas pessoas-chave. A qualidade da documentação e das tomadas de decisão varia consideravelmente. Métodos não estruturados são utilizados para definir os requisitos e identificar as soluções tecnológicas.

3 Processo Definido quando
Existem métodos claros e estruturados para determinar as soluções de TI. As abordagens para determinar as soluções de TI requerem que alternativas sejam avaliadas com base em requisitos de negócio e do usuário, oportunidades tecnológicas, viabilidade econômica, avaliação dos riscos e outros fatores. O processo para determinar as soluções de TI é aplicado a alguns projetos baseado em fatores como as decisões tomadas pelos indivíduos, o tempo de gerenciamento comprometido ou o tamanho e a prioridade dos requisitos de negócios originais. Métodos estruturados são utilizados para definir requisitos e identificar soluções de TI.

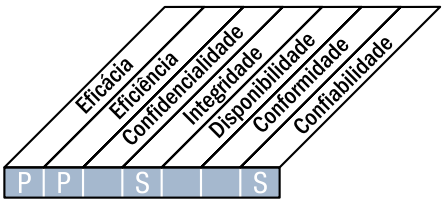
4 Gerenciado e Mensurável quando
Existe uma metodologia estabelecida para identificar e avaliar as soluções de TI que é utilizada pela maioria dos projetos. A documentação dos projetos é de boa qualidade, e cada estágio é aprovado de forma adequada. Os requisitos são bem articulados e harmonizados com as estruturas predefinidas. Soluções alternativas são consideradas, incluindo análises de custos e benefícios. A metodologia é clara, definida, entendida de forma geral e mensurável. Há uma interface claramente definida entre o gerenciamento de TI e o negócio para identificar e avaliar as soluções de TI.

5 Otimizado quando
A metodologia de identificação e avaliação das soluções de TI está sujeita a contínuo aperfeiçoamento. A metodologia de aquisição e implementação é flexível para se ajustar aos projetos de grande porte e de pequeno porte. A metodologia é suportada por um banco de dados de conhecimento interno e externo que contém material de referência de soluções tecnológicas. A metodologia por si só produz documentação em uma estrutura predefinida que torna eficiente a produção e a manutenção. Novas oportunidades de utilizar a tecnologia para ganhar vantagem competitiva, influenciar o processo de reengenharia dos negócios e proporcionar melhoria geral da eficiência são frequentemente identificadas. A Direção irá detectar e agir sempre que as soluções de TI forem aprovadas sem levar em consideração tecnologias alternativas e requisitos funcionais de negócio.

DESCRIÇÃO DE PROCESSO

AI2 Adquirir e Manter Software Aplicativo

As aplicações devem ser disponibilizadas em alinhamento com os requisitos do negócio. Este processo contempla o projeto das aplicações, a inclusão de controles e requisitos de segurança apropriados, o desenvolvimento e a configuração de acordo com padrões. Isso permite às organizações apoiarem de forma adequada as operações do negócio com as aplicações corretas.



Controle sobre o seguinte processo de TI:

Adquirir e Manter Software Aplicativo

que satisfaça aos seguintes requisitos do negócio para a TI:

tornar disponíveis as aplicações em alinhamento com os requisitos do negócio, no prazo desejado e com um custo razoável

com foco em:

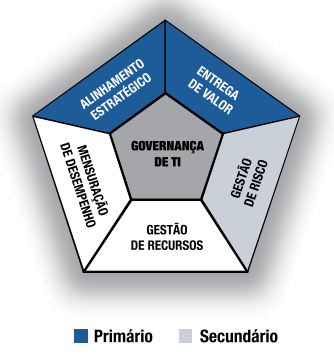
assegurar a existência de um processo de desenvolvimento que contemple o cumprimento de prazos e otimização de custos

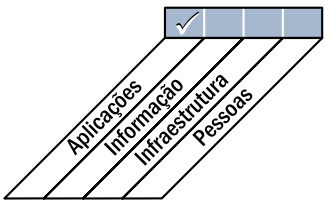
é alcançado por:

- Tradução dos requisitos de negócio nas especificações de projeto
- Adesão aos padrões de desenvolvimento em todas as modificações
- Segregação entre as atividades de desenvolvimento, teste e operação

e medido por:

- Quantidade de problemas em produção por aplicação que causem períodos perceptíveis de indisponibilidade
- Percentual de usuários satisfeitos com a funcionalidade oferecida





Objetivos de Controle Detalhados

AI2 Adquirir e Manter Software Aplicativo

A12.1 Projeto em Nível Macro
Traduzir os requisitos de negócio em especificações de projeto em nível macro para o desenvolvimento de software, levando em consideração o direcionamento tecnológico e a arquitetura de informação da organização. O gerenciamento deve aprovar as especificações de projeto para assegurar que o projeto de alto nível atenda aos requisitos. Reavaliar quando ocorrer discrepâncias técnicas ou lógicas significativas durante o desenvolvimento ou a manutenção.

AI2.2 Projeto Detalhado
Detalhar requisitos técnicos e de projeto dos softwares aplicativos. Definir os critérios de aceitação dos requisitos. Aprovar os requisitos para assegurar que eles correspondam ao projeto em nível macro. Reavaliar quando ocorrer discrepâncias técnicas ou lógicas significativas durante o desenvolvimento ou a manutenção.

AI2.3 Controle e Auditabilidade do Aplicativo
Assegurar que os controles de negócio sejam expressos adequadamente nos controles dos aplicativos de forma que o processamento ocorra no prazo correto e seja exato, completo, autorizado e auditável.

AI2.4 Segurança e Disponibilidade do Aplicativo
Considerar os requisitos de segurança e disponibilidade em resposta aos riscos identificados e em linha com a classificação de dados, a arquitetura de segurança da informação e o perfil de tolerância a riscos da organização.

AI2.5 Configuração e Implementação de Software Aplicativo Adquirido
Customizar e implementar as funcionalidades automatizadas adquiridas para alcançar os objetivos de negócios.

AI2.6 Principais Atualizações dos Sistemas Existentes
Seguir um processo de desenvolvimento similar ao de desenvolvimento de novos sistemas quando ocorrer grandes mudanças nos sistemas existentes que possam resultar em mudanças significativas nos projetos e/ou funcionalidades atuais.

AI2.7 Desenvolvimento de Software Aplicativo
Assegurar que as funcionalidades automatizadas sejam desenvolvidas em conformidade com as especificações de projeto, padrões de desenvolvimento e documentação e requisitos de qualidade e de autorização. Assegurar que todos os aspectos contratuais e legais sejam identificados e considerados nos softwares aplicativos desenvolvidos por terceiros.

AI2.8 Garantia de Qualidade de Software
Desenvolver e executar o plano de garantia de qualidade de software para obter a qualidade especificada na definição dos requisitos de projeto e nos procedimentos e políticas de qualidade da organização.

AI2.9 Gestão dos Requisitos das Aplicações
Acompanhar a situação individual dos requisitos (incluindo todos os requisitos rejeitados) durante o desenho, o desenvolvimento e a implementação e garantir que as mudanças nos requisitos sejam aprovadas através de um processo de gerenciamento de mudanças.

AI2.10 Manutenção de Software Aplicativo
Desenvolver a estratégia e o plano de manutenção de software aplicativo.

Diretrizes de Gerenciamento

AI2 Adquirir e Manter Software Aplicativo

Origem	Entrada
PO2	Dicionário de dados; Estrutura de classificação de dados, Plano otimizado de sistemas de negócio;
PO3	Atualizações periódicas do "estado da tecnologia";
PO5	Relatórios de Custo/Benefício;
PO8	Padrões para aquisição e desenvolvimento;
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
AI1	Estudo de viabilidade dos requisitos de negócio;
AI6	Descrição do processo de mudanças

Saída	Destino						
Especificações de controles para segurança de aplicações;	DS5						
Conhecimento de aplicações e pacotes de *software*;	AI4						
Decisões de aquisição;	AI5						
SLAs planejados inicialmente;	DS1						
Especificações de disponibilidade, continuidade e recuperação	DS3	DS4					

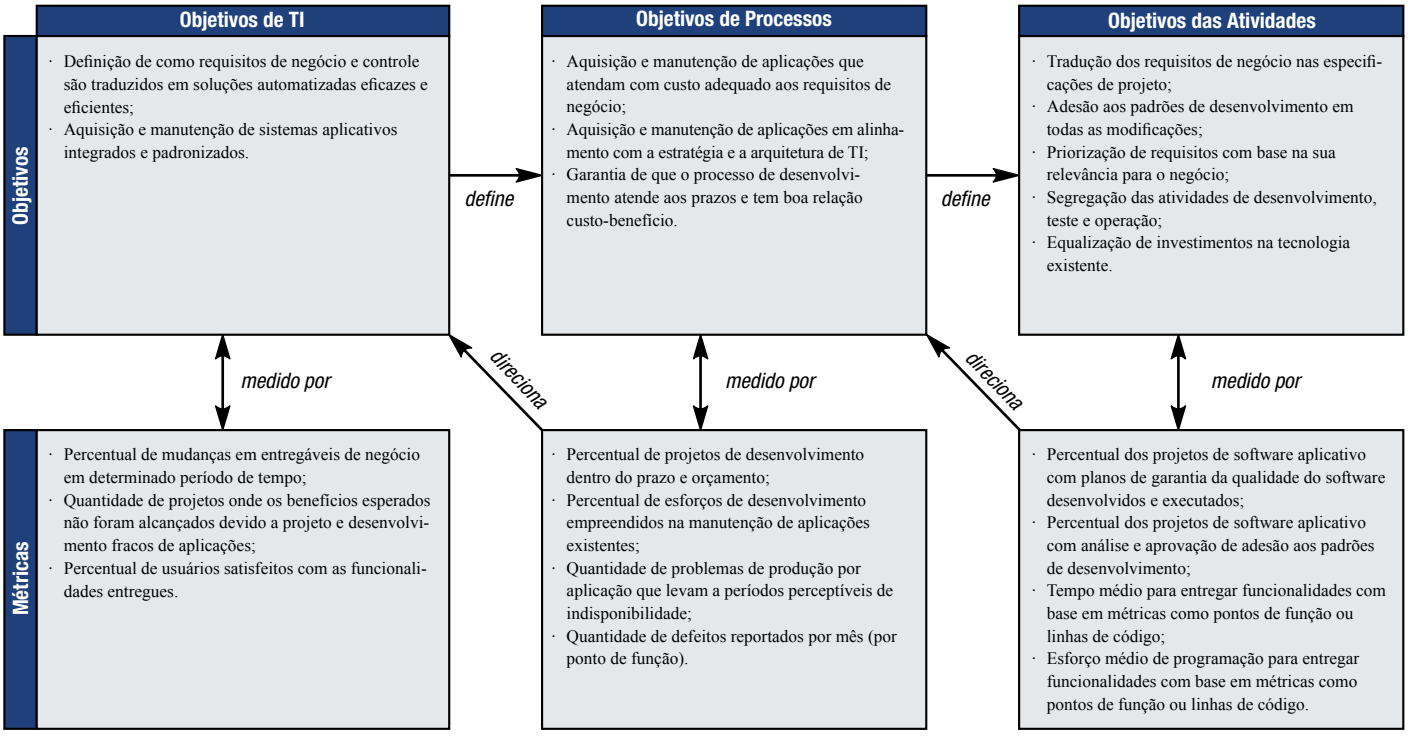
Tabela RACI

Funções

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Traduzir os requisitos de negócio em macro especificações de projeto;					C		C	A/R		R	C
Preparar projeto detalhado e requisitos técnicos dos *softwares* aplicativos;				I	C	C	C	A/R		R	C
Especificar no projeto os controles das aplicações;					R	C		A/R		R	R
Customizar e implementar as funcionalidades automatizadas adquiridas;					C	C		A/R		R	C
Desenvolver metodologias e processos formais para gerenciar o processo de desenvolvimento de aplicações;				C		C	C	A	C	R	C
Criar um plano de garantia da qualidade de *software* para os projetos;					I		C	R		A/R	C
Rastrear e gerenciar requisitos das aplicações;								R		A/R	
Desenvolver um plano para a manutenção dos *softwares* aplicativos				C		C		A/R		C	

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

AI2 Adquirir e Manter Software Aplicativo

O gerenciamento do processo de ***"Adquirir e Manter Software Aplicativo"*** que satisfaça ao requisito do negócio para a TI de ***"tornar disponíveis as aplicações em alinhamento com os requisitos do negócio, no prazo desejado e com um custo razoável"*** é:

0 Inexistente quando
Não há processo para especificação e o projeto de aplicações. Em geral as aplicações são obtidas com base nas ofertas de fornecedores, no reconhecimento de marca ou familiaridade do pessoal de TI com produtos específicos, com pouco ou nenhum reconhecimento dos requisitos reais do negócio.

1 Inicial/ *Ad hoc* quando
Há uma conscientização da necessidade de um processo de aquisição e manutenção. Formas de aquisição e manutenção do software aplicativo variam a cada projeto. Existe uma variedade de soluções isoladas para os requisitos específicos de negócios, provavelmente adquiridas de modo independente, o que resulta em ineficiências de manutenção e suporte. Aspectos de segurança e disponibilidade são pouco considerados no projeto ou na aquisição do software aplicativo.

2 Repetível, porém Intuitivo quando
Há vários processos paralelos similares de aquisição e manutenção de aplicativos com base nas habilidades funcionais dos profissionais da TI. A taxa de sucesso com as aplicações depende altamente das habilidades e do nível de experiência internas da TI. A manutenção normalmente é problemática e sofre forte impacto quando se perde o conhecimento interno devido à saída de pessoas da organização. Aspectos de segurança e disponibilidade foram pouco considerados no projeto ou na aquisição do software aplicativo.

3 Processo Definido quando
Existe um processo claro, definido e geralmente bem entendido de aquisição e manutenção de software aplicativo. Esse processo está em alinhamento com as estratégias de TI e negócio. Existem tentativas de aplicação de processos documentados de forma consistente em projetos e aplicações. As metodologias geralmente são inflexíveis e de difícil aplicação geral, por isso alguns passos provavelmente são pulados. Atividades de manutenção são planejadas, agendadas e coordenadas.

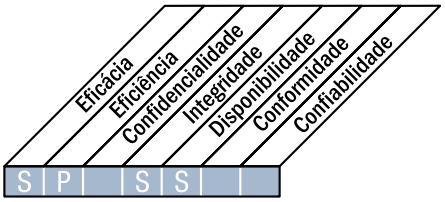
4 Gerenciado e Mensurável quando
Há uma metodologia formal e bem entendida que inclui um processo de especificação e projeto, critérios de aquisição, um processo de teste e requisitos para documentação. Existem mecanismos de aprovação acordados e documentados para assegurar que todos os passos sejam seguidos e as exceções sejam devidamente autorizadas. Práticas e procedimentos estão bem ajustados à organização, são utilizados por todo pessoal e aplicáveis à maioria dos requisitos de aplicação.

5 Otimizado quando
As práticas de aquisição e manutenção de software de aplicação estão alinhadas aos processos definidos. O enfoque baseia-se em componentes, com aplicações padronizadas e predefinidas ajustadas às necessidades do negócio. A abordagem é corporativa. A metodologia de aquisição e manutenção é bem avançada e permite rapidez na implementação, possibilitando agilidade e flexibilidade para reagir a mudanças dos requisitos do negócio. A metodologia de aquisição, implementação e manutenção de software é submetida a melhoria contínua e apoiada por banco de dados de conhecimento interno e externo contendo material de referência e melhores práticas. A metodologia cria documentação em uma estrutura predefinida que torna a produção e a manutenção eficientes.

Descrição de Processo

AI3 Adquirir e Manter Infraestrutura de Tecnologia

As organizações devem ter processos de aquisição, implementação e atualização da infraestrutura de tecnologia. Isso requer uma abordagem planejada de aquisição, manutenção e proteção da infraestrutura em alinhamento com as estratégias tecnológicas acordadas e o fornecimento de ambientes de desenvolvimento e teste. Isso assegura um apoio tecnológico contínuo às aplicações de negócio.



Controle sobre o seguinte processo de TI:

Adquirir e manter infraestrutura tecnológica

que satisfaça aos seguintes requisitos do negócio para a TI:

adquirir e manter uma infraestrutura de TI integrada e padronizada

com foco em:

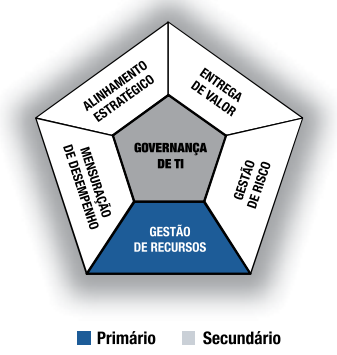
Disponibilizar plataformas apropriadas às aplicações de negócio em alinhamento com a arquitetura de TI definida e os padrões tecnológicos

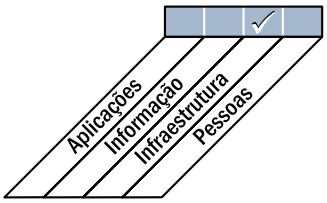
é alcançado por:

- Preparação de um plano de aquisição tecnológica alinhado com o plano de infraestrutura tecnológica
- Planejamento da manutenção da infraestrutura
- Implementação de controles internos, medidas de segurança e de auditoria

e medido por:

- Percentual das plataformas que não estejam alinhadas com os padrões definidos de tecnologia e arquitetura de TI
- Quantidade de processos críticos de negócio sustentados por infraestrutura obsoleta (ou próxima da obsolescência)
- Quantidade de componentes de infraestrutura que não contam mais com suporte (ou que tendem a não ter suporte num futuro próximo)





OBJETIVOS DE CONTROLE DETALHADOS

AI3 Adquirir e Manter Infraestrutura de Tecnologia

AI3.1 Plano de Aquisição de Infraestrutura Tecnológica
Preparar um plano para aquisição, implementação e manutenção da infraestrutura tecnológica que satisfaça aos requisitos técnicos e funcionais estabelecidos do negócio e esteja de acordo com a direção tecnológica da organização.

AI3.2 Infraestrutura de Recursos, Proteção e Disponibilidade
Implementar controles internos, medidas de segurança e auditabilidade durante a configuração, integração e manutenção de hardware e software da infraestrutura para proteger os recursos e assegurar disponibilidade e integridade. As responsabilidades pela utilização de componentes críticos devem ser claramente definidas e entendidas por aqueles que desenvolvem e integram os componentes da infraestrutura. Seu uso deve ser monitorado e avaliado.

AI3.3 Manutenção da Infraestrutura
Desenvolver uma estratégia e um plano para manutenção da infraestrutura e assegurar que as mudanças sejam controladas em alinhamento com os procedimentos de gerenciamento de mudança da organização. Incluir revisão periódica com base nas necessidades dos negócios, gerenciamento de correções e estratégias de atualização, análise de riscos, vulnerabilidades e requisitos de segurança.

AI3.4 Viabilidade do Ambiente de Teste
Estabelecer um ambiente de desenvolvimento e de teste para proporcionar eficiência e eficácia nos testes de viabilidade e integração dos componentes da infraestrutura.

Diretrizes de Gerenciamento

AI3 Adquirir e Manter Infraestrutura de Tecnologia

Origem	Entrada
PO3	Plano de infraestrutura tecnológica, padrões e oportunidades, atualizações periódicas do "estado da tecnologia";
PO8	Padrões para aquisição e desenvolvimento;
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
AI1	Estudo de viabilidade dos requisitos de negócio;
AI6	Descrição do processo de mudanças;
DS3	Planejamento de desempenho e capacidade (requisitos)

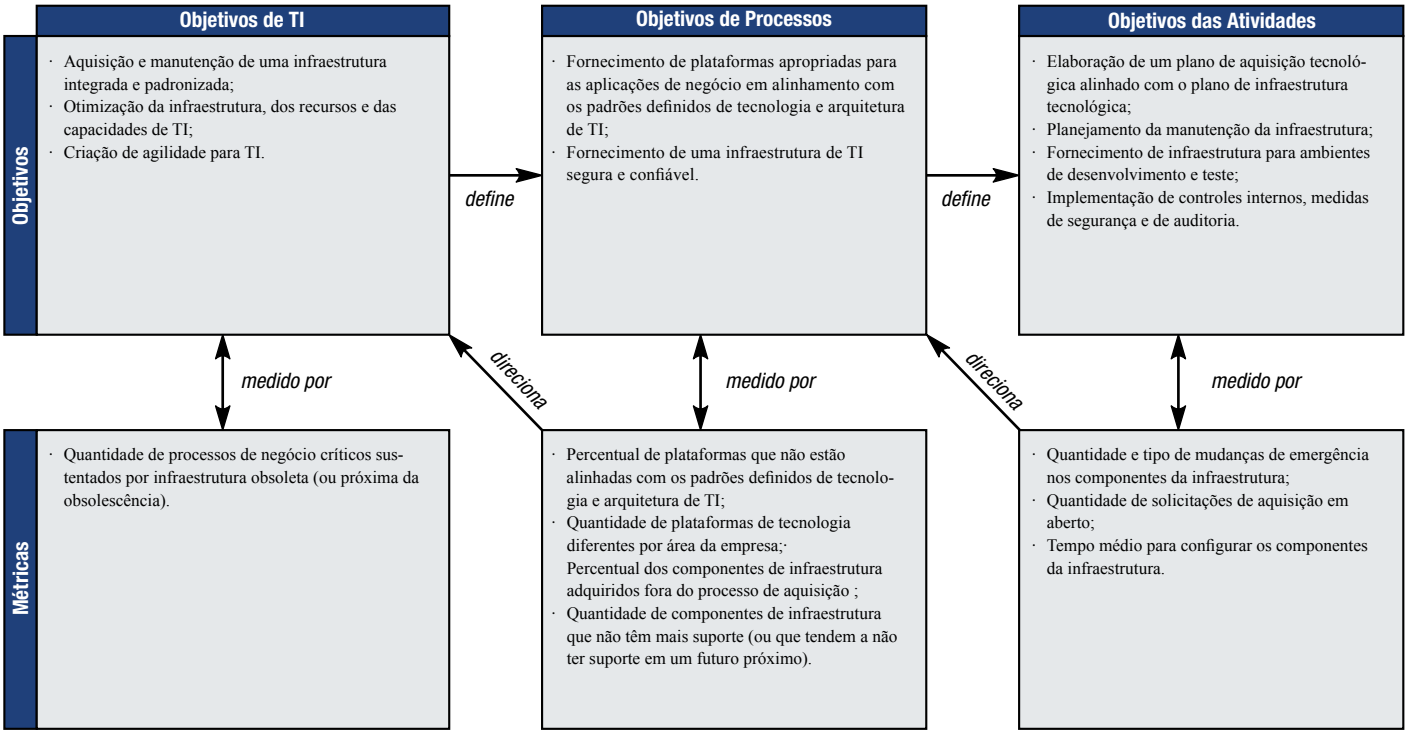
Saída	Destino
Decisões de aquisição;	AI5
Sistema configurado para ser testado/instalado;	AI7
Requisitos do ambiente físico;	DS12
Atualizações para padrões tecnológicos;	PO3
Requisitos de monitoramento de sistema;	DS3
Conhecimento da infraestrutura;	AI4
Acordos de nível operacional planejados inicialmente	DS1

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir processos/procedimentos de aquisição;		C		A		C	C	C	R		I
Negociar aquisição e adquirir a requerida infraestrutura com os fornecedores (aprovados);		C/I		A	I	R	C	C	R		I
Definir estratégia e plano de manutenção para a infraestrutura;				A		R	R	R	C		
Configurar componentes da infraestrutura				A		R	C				I

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

AI3 Adquirir e Manter Infraestrutura de Tecnologia

O gerenciamento do processo de ***"Adquirir e Manter Infraestrutura de Tecnologia"*** que satisfaça ao requisito do negócio para a TI de ***"adquirir e manter uma infraestrutura de TI integrada e padronizada"*** é:

0 Inexistente quando
O gerenciamento da infraestrutura tecnológica não é reconhecido como um tópico suficientemente importante para ser considerado.

1 Inicial/ *Ad hoc* quando
Existem alterações feitas na infraestrutura de qualquer aplicação nova, sem qualquer planejamento geral. Embora exista a consciência de que a infraestrutura de TI é importante, não há nenhuma abordagem consistente e abrangente. A atividade de manutenção reage às necessidades de curto prazo. O ambiente de teste é o próprio ambiente de produção.

2 Repetível, porém Intuitivo quando
Há consistência entre as abordagens táticas de aquisição e manutenção da infraestrutura de TI. A aquisição e a manutenção da infraestrutura de TI não estão baseadas em nenhuma estratégia definida, tampouco consideram as necessidades das aplicações de negócios que devem ser suportadas. Há um entendimento de que a infraestrutura de TI seja importante, apoiada por algumas práticas formais. Algumas manutenções são programadas, porém não são programadas e coordenadas por completo. Para alguns ambientes, há um ambiente de teste separado.

3 Processo Definido quando
Existe um processo claro, definido e geralmente entendido para aquisição e manutenção da infraestrutura de TI. O processo atende às necessidades das aplicações de negócios críticas, está alinhado às estratégias de TI e de negócio, porém não é aplicado de maneira consistente. A manutenção é planejada, agendada e coordenada. Existem ambientes distintos para produção e teste.

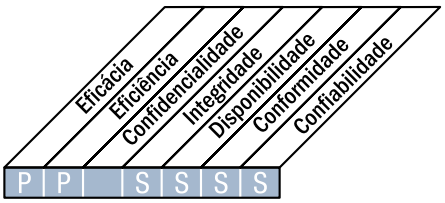
4 Gerenciado e Mensurável quando
O processo de aquisição e manutenção da infraestrutura tecnológica se desenvolveu ao ponto de funcionar bem na maioria das situações, é seguido de forma consistente e está focado na reutilização. A infraestrutura de TI suporta adequadamente as aplicações de negócio. O processo é bem organizado e proativo. O custo e a expectativa de tempo para atingir os níveis esperados de escalabilidade, flexibilidade e integração estão parcialmente otimizados.

5 Otimizado quando
O processo de aquisição e manutenção de infraestrutura tecnológica é proativo e bem alinhado com as aplicações de negócio críticas e a arquitetura tecnológica. Boas práticas referentes às soluções tecnológicas são seguidas, e a organização está consciente dos mais recentes desenvolvimentos de plataformas e ferramentas de gerenciamento. Os custos são reduzidos através de racionalização e padronização dos componentes da infraestrutura e pelo uso de automação. Um alto nível de consciência técnica pode identificar os caminhos ideais de melhoria proativa de desempenho, incluindo avaliação de opções de terceirização. A infraestrutura de TI é vista como fator-chave para alavancar a utilização da TI.

DESCRIÇÃO DE PROCESSO

AI4 Habilitar Operação e Uso

Conhecimento sobre novos sistemas deve estar disponível. Este processo requer a elaboração de documentação e manuais para usuários e para TI e a promoção de treinamentos para assegurar a operação e uso apropriado das aplicações e infraestrutura.



Controle sobre o seguinte processo de TI:

Habilitar operação e uso

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar a satisfação de usuários finais com ofertas de serviços e níveis de serviços e a completa integração das aplicações e soluções tecnológicas aos processos de negócio

com foco em:

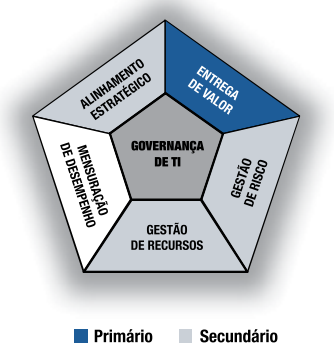
fornecer manuais de usuário, manuais operacionais e materiais de treinamento eficazes para transferir o conhecimento necessário a operação e uso bem-sucedido do sistema.

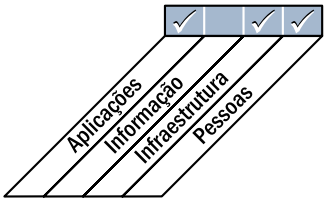
é alcançado por:

- Desenvolvimento e disponibilização de documentação de transferência de conhecimento
- Comunicação e treinamento de usuários, gestores de negócio, equipes de suporte e equipes de operação
- Produção de materiais de treinamento

e medido por:

- Quantidade de aplicações nas quais os procedimentos de TI estão completamente integrados aos processos de negócio
- Percentual de proprietários de negócio satisfeitos com os treinamentos e material de suporte das aplicações
- Quantidade de aplicações que dispõem de treinamento adequado de suporte operacional e de usuário





Objetivos de Controle Detalhados

AI4 Habilitar Operação e Uso

AI4.1 Planejamento para Soluções Operacionais
Desenvolver um plano para identificar e documentar todos os aspectos técnicos, a capacidade operacional e os níveis de serviços necessários para que todos que irão operar, utilizar e manter as soluções automatizadas possam exercer suas responsabilidades.

AI4.2 Transferência de Conhecimento ao Gerenciamento do Negócio
Transferir o conhecimento ao gerenciamento do negócio para permitir que este assuma a propriedade do sistema e dados, bem como exerça suas responsabilidades nos processos de entrega, qualidade de serviço, controles internos e administração da aplicação.

AI4.3 Transferência de Conhecimento aos Usuários Finais
Transferir conhecimento e habilidades para permitir aos usuários o uso efetivo e eficiente dos sistemas aplicativos que sustentam processos de negócio.

AI4.4 Transferência de Conhecimento às Equipes de Operações e Suporte
Transferir conhecimento e habilidades para permitir que as equipes de operações e suporte técnico entreguem, suportem e mantenham os sistemas e a infraestrutura associada de forma eficaz e eficiente

Diretrizes de Gerenciamento

AI4 Habilitar Operação e Uso

Origem	Entrada
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
AI1	Estudo de viabilidade dos requisitos de negócio;
AI2	Conhecimento de aplicações e pacotes de *software*;
AI3	Conhecimento da infraestrutura;
AI7	Erros conhecidos e aceitos;
DS7	Atualizações necessárias de documentações

Saída	Destino						
Manuais de usuário, operação, suporte, técnico e administração;	AI7	DS4	DS8	DS9	DS11	DS13	
Requisitos de transferência de conhecimento para implementação de soluções;	DS7						
Materiais de treinamento	DS7						

Tabela RACI

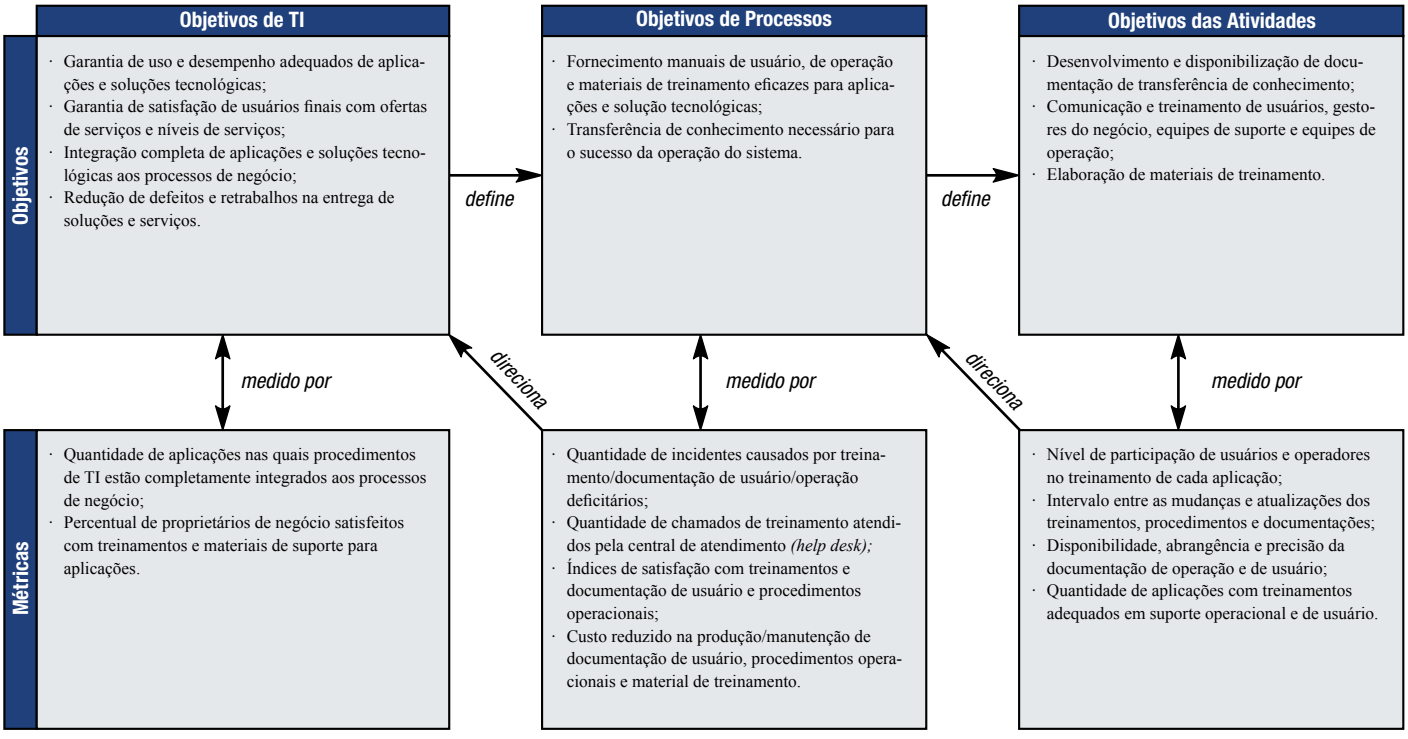
Funções

Atividades

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Time de Implantação	Departamento de Treinamento
Desenvolver estratégia para operacionalizar a solução;				A	A			R			I	R	C
Desenvolver metodologia de transferência de conhecimento;				C	A							C	R
Desenvolver manuais de procedimentos para usuários finais;					A/R			R			C	C	
Desenvolver documentação de suporte técnico para equipes de operação e suporte;						A/R		C			C		
Desenvolver e realizar treinamento;					A	A		R					R
Avaliar os resultados dos treinamentos e melhorar a documentação quando necessário					A	A						R	R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

AI4 Habilitar Operação e Uso

O gerenciamento do processo de ***"Habilitar Operação e Uso"*** que satisfaça ao requisito do negócio para a TI de ***"assegurar a satisfação de usuários finais com ofertas de serviços e níveis de serviços, e integrar completamente as aplicações e soluções tecnológicas aos processos de negócio"*** é:

0 Inexistente quando
Não há nenhum processo estabelecido no que diz respeito à elaboração de documentação de usuário, manuais de operações e material de treinamento. Os únicos materiais existentes são aqueles fornecidos na compra dos produtos.

1 Inicial/ *Ad hoc* quando
Há consciência de que a documentação de processos é necessária. A documentação é ocasionalmente produzida e é inconsistentemente distribuída a grupos limitados. A maioria da documentação e muitos procedimentos estão desatualizados. Os materiais de treinamento tendem a ser esquemas exclusivos com qualidade variável. Praticamente não existe integração dos procedimentos nos diferentes sistemas e unidades de negócios. Não há informações vindas das unidades de negócios sobre planejamento dos programas de treinamento.

2 Repetível, porém Intuitivo quando
Métodos similares são utilizados para gerar procedimentos e documentação, porém não são baseados em uma abordagem estruturada. Não há abordagem uniforme para o desenvolvimento de procedimentos operacionais e de usuários. Os materiais de treinamento são elaborados pelas pessoas ou equipes de projeto, e a qualidade depende tão somente das pessoas envolvidas. Os procedimentos e a qualidade do suporte de usuário variam de ineficiente a muito bom, com pouquíssimas consistência e integração na organização. Programas de treinamento de negócio e de usuários são providenciados ou facilitados, mas não há um plano abrangente de cronograma e recursos para a realização de treinamentos.

3 Processo Definido quando
Há uma estrutura claramente definida, aceita e entendida para tratar da documentação de usuários, manuais de operações e material de treinamento. Os procedimentos são armazenados e mantidos em uma biblioteca formal e podem ser acessados por qualquer pessoa que precise conhecê-los. As correções dos procedimentos e documentações são feitas de forma reativa. Os procedimentos estão disponíveis *offline* e podem ser acessados e mantidos em caso de desastre. Existe um processo que especifica atualizações de procedimentos e material de treinamento como resultado de um projeto de mudança. Apesar da existência de abordagens definidas, o conteúdo real é variável porque não há controle que obrigue a conformidade com padrões. Os usuários estão informalmente envolvidos no processo. Ferramentas automatizadas são gradativamente utilizadas na geração e na distribuição dos procedimentos. Treinamentos para unidades de negócios e usuários são planejados e agendados.

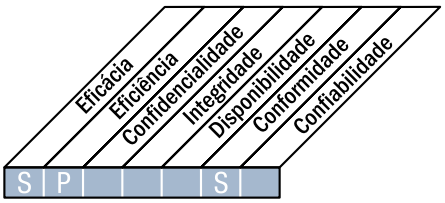
4 Gerenciado e Mensurável quando
Há uma estrutura definida para manter os procedimentos e materiais de treinamento suportados pelo gerenciamento de TI. A abordagem adotada para manter os procedimentos e manuais de treinamento contempla todos os sistemas e unidades de negócios; dessa forma, os processos podem ser revisados a partir de uma perspectiva de negócio. Procedimentos e materiais de treinamento são integrados para incluir interdependências e interfaces. Existem controles que asseguram a adoção de padrões, e são desenvolvidos e mantidos procedimentos referentes a todos os processos. *Feedbacks* das unidades de negócio e usuários sobre documentação e treinamento são coletados e avaliados como parte de um processo de melhoria contínua. Normalmente a documentação e o material de treinamento apresentam bom nível de confiabilidade e disponibilidade. Recentemente foi implementado um processo de documentação e gerenciamento de procedimentos automatizados. O desenvolvimento de procedimentos automatizados está cada vez mais integrado ao desenvolvimento de sistemas de aplicação, facilitando consistência e o acesso pelo usuário. O treinamento das unidades de negócio e dos usuários atende às necessidades do negócio. O gerenciamento de TI desenvolve métricas para a elaboração e a disponibilização de documentação, material de treinamento e programas de treinamento.

5 Otimizado quando
O processo da documentação operacional e de usuário é aprimorado constantemente através da adoção de novas ferramentas e métodos. Os materiais de procedimentos e de treinamento são considerados uma base de conhecimento em constante evolução que é mantida eletronicamente usando gerenciamento de atualização de conhecimento, fluxos de trabalho *(workflow)* e tecnologias de distribuição, tornando-a acessível e fácil de manter. A documentação e o material de treinamento são atualizados para refletir mudanças operacionais, organizacionais e de software. O desenvolvimento da documentação e do material de treinamento e a distribuição de programas de treinamento estão plenamente integrados ao negócio e às definições de processo de negócio, portanto apoiando os requisitos corporativos em vez de apenas apoiar os procedimentos orientados à TI.

Descrição do Processo

AI5 Adquirir Recursos de TI

Recursos de TI, incluindo pessoas, hardware, software e serviços precisam ser adquiridos. Isso requer a definição e a aplicação de procedimentos de aquisição, a seleção de fornecedores, o estabelecimento de arranjos contratuais e a aquisição propriamente dita. Assim assegura-se que a organização tenha todos os recursos de TI necessários a tempo e com boa relação custo-benefício.



Controle sobre o seguinte processo de TI:

Adquirir recursos de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

melhorar o custo-eficiência de TI e sua contribuição para a lucratividade do negócio

com foco em:

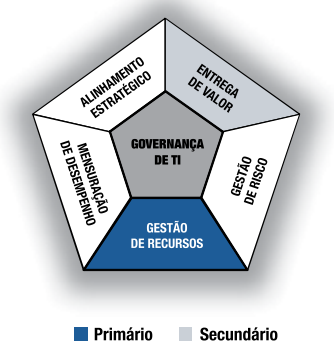
adquirir e manter habilidades de TI que respondam à estratégia de entrega e a uma infraestrutura de TI padronizada e integrada, e reduzir o risco de aquisição de recursos de TI

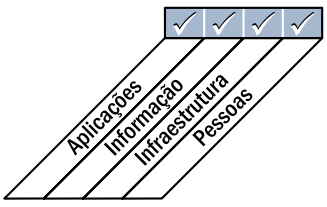
é alcançado por:

- Obtenção de parecer profissional para aspectos legais e contratuais
- Definição de procedimentos e padrões de aquisição
- Aquisição de hardware, software e serviços requeridos em alinhamento com os procedimentos definidos

e medido por:

- Quantidade de discordâncias relacionadas aos contratos de aquisição
- Custo reduzido de compra
- Percentual das principais partes interessadas satisfeitas com os fornecedores





Objetivos de Controle Detalhados

AI5 Adquirir Recursos de TI

AI5.1 Controle de Aquisição
Desenvolver e acompanhar um conjunto de procedimentos e padrões consistentes com o processo e a estratégia corporativa de aquisição para assegurar que a aquisição de infraestrutura, instalações, hardware, software e serviços satisfaça aos requisitos de negócio.

AI5.2 Gerenciamento de Contratos de Fornecedores
Instituir um procedimento para estabelecer, modificar e rescindir contratos com todos os fornecedores. O procedimento deve contemplar no mínimo as formalidades legais, financeiras, organizacionais, documentais, de desempenho, de segurança e de propriedade intelectual e as responsabilidades e obrigações legais em casos de cancelamento (incluindo cláusulas de penalidades). Todos os contratos e as respectivas alterações devem ser revisados por consultores legais.

AI5.3 Seleção de Fornecedores
Selecionar fornecedores de acordo com a prática formal e justa que assegure a melhor opção viável com base nos requisitos definidos a partir de informações dadas por fornecedores em potencial e acordadas entre fornecedores e clientes.

AI5.4 Aquisição de Recursos de TI
Garantir que os interesses da organização sejam protegidos em todos os contratos de aquisição. Incluir e impor os direitos e as obrigações de todas as partes nos termos contratuais de aquisição de software, desenvolvimento de recursos, infraestrutura e serviços.

Diretrizes de Gerenciamento

AI5 Adquirir Recursos de TI

Origem	Entrada
PO1	Estratégia de aquisição de TI;
PO8	Padrões para aquisição;
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
AI1	Estudo de viabilidade dos requisitos de negócio;
AI2-3	Decisões de aquisição;
DS2	Catálogo de fornecedores

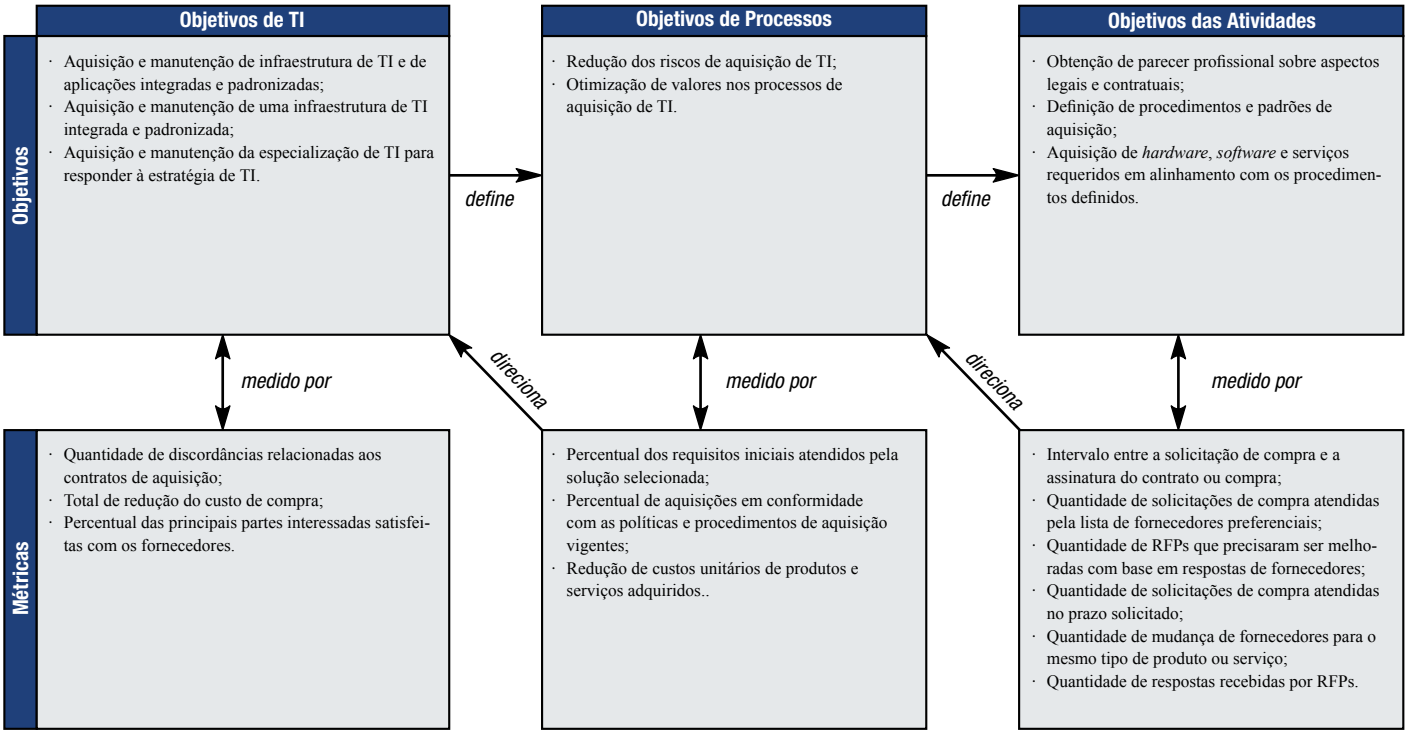
Saída	Destino
Requisitos de gerenciamento de relacionamento com terceiros;	DS2
Itens adquiridos;	AI7
Tratativas contratuais	DS2

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Desenvolver políticas e procedimentos de aquisição de TI alinhadas com as políticas de aquisição corporativas;	I	C		A		I	I	I	R		C
Estabelecer/manter uma listagem de fornecedores homologados;									A/R		
Avaliar e selecionar fornecedores através de processos de requisição de propostas *(RFP - Request For Proposal);*	C	C		A		R		R	R	R	C
Desenvolver contratos que protejam os interesses corporativos;	R	C		A		R		R	R		C
Adquirir de acordo com os procedimentos estabelecidos				A		R		R	R		C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

AI5 Adquirir Recursos de TI

O gerenciamento do processo de ***"Adquirir Recursos de TI"*** que satisfaça ao requisito do negócio para a TI de ***"melhorar a eficiência de custo de TI e sua contribuição para a lucratividade do negócio"*** é:

0 Inexistente quando
Não há nenhum processo estabelecido de aquisição de recursos de TI. A organização não reconhece a necessidade de políticas e procedimentos claros para assegurar que todos os recursos de TI sejam disponibilizados a tempo e com relação custo-benefício aceitável.

1 Inicial/ *Ad hoc* quando
A organização reconhece a necessidade de políticas e procedimentos documentados que vinculem a aquisição de TI ao processo de aquisição corporativo. Os contratos de aquisição de recursos de TI são elaborados e gerenciados por gerentes de projeto e outras pessoas no exercício de seus julgamentos profissionais, e não como resultado de políticas e procedimentos formais. Existe apenas um relacionamento *ad hoc* entre os processos de aquisição corporativa e TI. Os contratos de aquisição são gerenciados na conclusão do projeto, e não durante o projeto.

2 Repetível, porém Intuitivo quando
Há consciência na organização da necessidade de políticas e procedimentos básicos de aquisição de TI. As políticas e os procedimentos estão parcialmente integrados ao processo corporativo de aquisição. Os processos de aquisição são mais utilizados nos projetos grandes e de maior visibilidade. O nível de responsabilização pela aquisição de TI e o gerenciamento de contrato é determinado pela experiência individual de cada gerente de contrato. A importância do gerenciamento de fornecedores e de relacionamento é reconhecida, porém tratada por iniciativas individuais. Os processos de contratação são mais utilizados para os projetos grandes e de maior visibilidade.

3 Processo Definido quando
Há políticas e procedimentos para aquisição de TI instituídos pela Direção de TI. Essas políticas e procedimentos são guiados pelo processo geral de aquisição da organização. O processo de aquisição de TI está totalmente integrado aos sistemas corporativos de aquisição. Existem padrões definidos para a aquisição de recursos de TI. Os fornecedores de recursos de TI estão integrados aos mecanismos de gerenciamento de projetos da organização, de uma perspectiva de gerenciamento de contratos. A Direção de TI comunica a necessidade do gerenciamento adequado de aquisições e contratos em toda a área de TI.

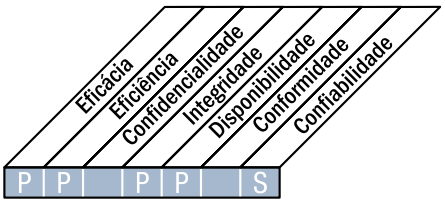
4 Gerenciado e Mensurável quando
A aquisição de TI está totalmente integrada com os sistemas corporativos de aquisição. Os padrões estabelecidos para a aquisição de recursos de TI são seguidos em todas as aquisições. As métricas utilizadas no gerenciamento de contratos e de aquisições são consideradas relevantes nos estudos de caso dos processos de aquisição de TI. Relatórios que sustentam os objetivos de negócio estão disponíveis. Os responsáveis pelo gerenciamento estão cientes das exceções nas políticas e nos procedimentos de aquisição de TI. O gerenciamento de relacionamentos estratégicos está evoluindo. Os responsáveis pelo gerenciamento de TI impõem o uso de processos de aquisição e gerenciamento de contratos em todas as aquisições através da revisão de medidas de desempenho.

5 Otimizado quando
A Direção de TI institui e viabiliza processos de aquisição de TI e impõe a conformidade com as políticas e os procedimentos para a aquisição de TI. As métricas utilizadas no gerenciamento de aquisição e de contratos são levadas em conta nos estudos de caso para aquisições de TI. Bons e longos relacionamentos são estabelecidos com a maioria dos fornecedores e parceiros, e a qualidade desses relacionamentos é avaliada e monitorada. Os relacionamentos são tratados de forma estratégica. Padrões, políticas e procedimentos de TI para aquisição de recursos de TI são estrategicamente gerenciados e respondem pelo acompanhamento de métricas do processo. A Direção de TI comunica a importância estratégica do adequado gerenciamento de aquisição e do gerenciamento de contratos em toda área de TI.

DESCRIÇÃO DO PROCESSO

AI6 Gerenciar Mudanças

Todas as mudanças, incluindo manutenções e correções de emergência, relacionadas com a infraestrutura e as aplicações no ambiente de produção são formalmente gerenciadas de maneira controlada. As mudanças (incluindo procedimentos, processos, parâmetros de sistemas e de serviço) devem ser registradas, avaliadas e autorizadas antes da implementação e revisadas em seguida, tendo como base os resultados efetivos e planejados. Isso assegura a mitigação de riscos de impactos negativos na estabilidade ou na integridade do ambiente de produção.



Controle sobre o seguinte processo de TI:

Gerenciar Mudanças

que satisfaça aos seguintes requisitos do negócio para a TI:

atender aos requisitos de negócio em alinhamento com a estratégia da organização, reduzindo retrabalho e defeitos na entrega de soluções e serviços

com foco em:

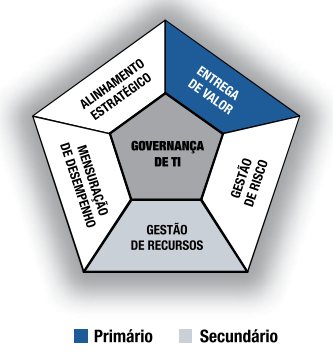
controlar a avaliação de impacto, autorização e implementação de todas as mudanças na infraestrutura, nas aplicações e nas soluções técnicas de TI, minimizar erros devido a especificações de requisitos incompletas e interromper a implementação de mudanças não autorizadas

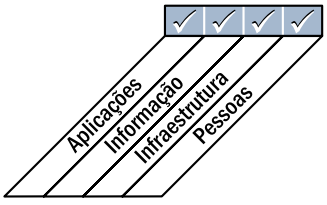
é alcançado por:

· Definição e comunicação de procedimentos de mudanças, incluindo mudanças emergenciais.
· Avaliação, priorização e autorização de mudanças.
· Acompanhamento de status e apresentação de relatório de mudanças.

e medido por:

· Quantidade de paradas ou erros em dados devido a especificações inadequadas ou avaliações de impacto críticas incompletas
· Retrabalho de infraestrutura ou aplicação causado por especificações de mudança inadequadas
· Percentual de mudanças que seguem o processo formal de controle de mudanças.





Objetivos de Controle Detalhados

AI6 Gerenciar Mudanças

AI6.1 Padrões e Procedimentos de Mudança
Estabelecer procedimentos formais de gerenciamento de mudanças para lidar de modo padronizado com todas as solicitações de mudança em aplicações, procedimentos, processos, parâmetros de sistema, parâmetros de serviço e plataformas subjacentes (inclusive solicitações de manutenção e reparo).

AI6.2 Avaliação de Impacto, Priorização e Autorização
Avaliar todas as solicitações de mudança de modo estruturado com relação a impactos no sistema operacional e na respectiva funcionalidade. Assegurar que todas as mudanças sejam categorizadas, priorizadas e autorizadas.

AI6.3 Mudanças de Emergência
Estabelecer um processo para definição, solicitação, testes, documentação, avaliação e autorização de mudanças de emergência que não sigam o processo de mudança estabelecido.

AI6.4 Acompanhamento de Status e Relatórios de Mudanças
Estabelecer um sistema de acompanhamento e relatórios de mudanças para documentar mudanças rejeitadas, comunicar o status de mudanças aprovadas e em andamento e executar mudanças. Garantir que as mudanças autorizadas sejam implementadas conforme planejado.

AI6.5 Finalização da Mudança e Documentação
Atualizar a documentação os procedimentos do sistema e de usuários sempre que forem implementadas mudanças no sistema.

Diretrizes de Gerenciamento

AI6 Gerenciar Mudanças

Origem	Entrada
PO1	Portfólio de projetos de TI;
PO8	Ações de melhoria de qualidade;
PO9	Planos de ação para remediação de riscos de TI;
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
DS3	Mudanças necessárias;
DS5	Mudanças de segurança necessárias;
DS8	Solicitações de serviço/solicitações de mudança;
DS9-10	Solicitações de mudança (como e onde aplicar a correção);
DS10	Registros de problemas

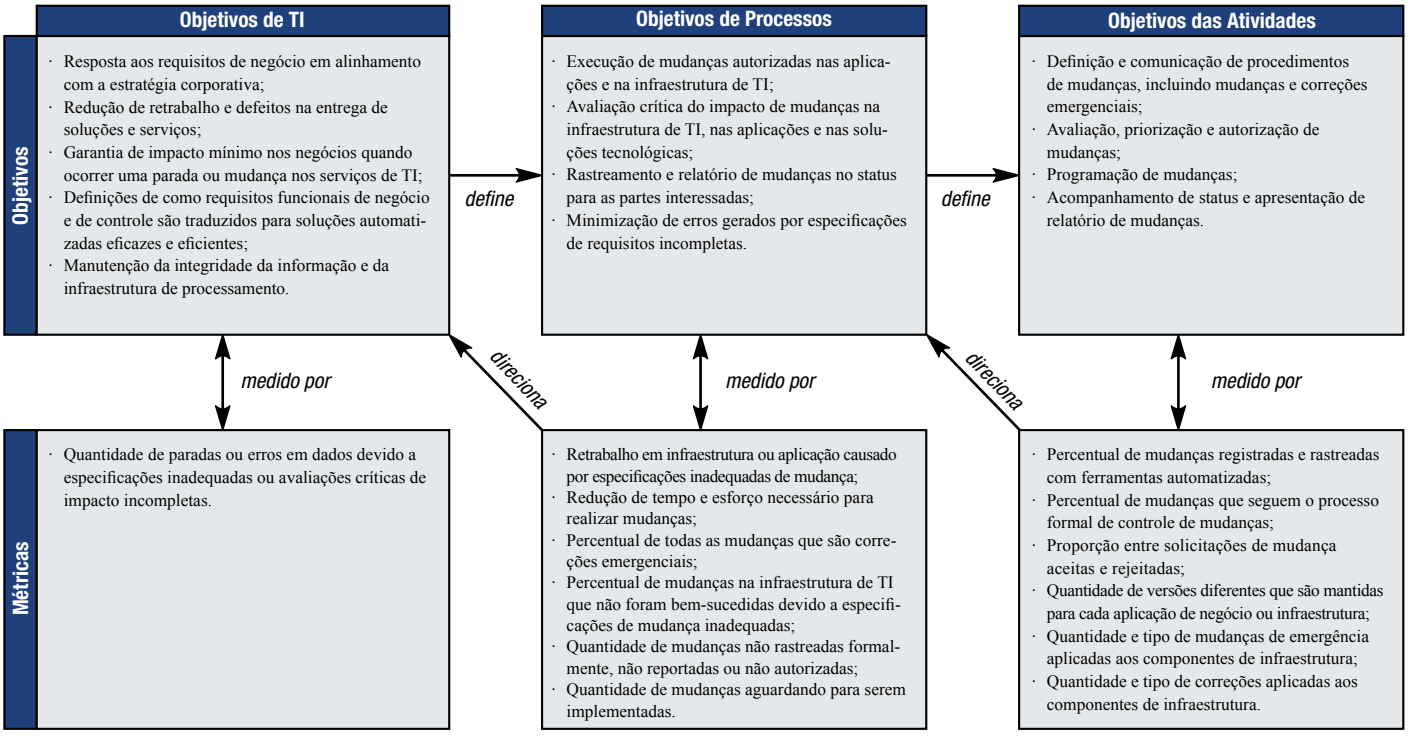
Saída	Destino						
Descrição do processo de mudanças;	AI1...AI3						
Relatórios de status das mudanças;	ME1						
Autorização de mudanças	AI7	DS8	DS10				

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Desenvolver e implementar um processo para registrar, avaliar e priorizar de forma consistente as solicitações de mudança;				A	I	R	C	R	C	C	C
Avaliar criticamente o impacto e priorizar mudanças baseadas em necessidades do negócio;				I	R	A/R	C	R	C	R	C
Assegurar que qualquer mudança crítica e emergencial siga o processo aprovado;				I	I	A/R	I	R			C
Autorizar mudanças;				I	C	A/R		R			
Gerenciar e disseminar informações relevantes relacionadas a mudanças				A	I	R	C	R	I	R	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

AI6 Gerenciar Mudanças

O gerenciamento do processo de ***"Gerenciar Mudanças"*** que satisfaça ao requisito do negócio para a TI de ***"atender aos requisitos de negócio em alinhamento com a estratégia da organização, reduzindo retrabalho e defeitos na entrega de soluções e serviços"*** é:

0 Inexistente quando
Não há um processo de gerenciamento de mudanças formalmente estabelecido, e as mudanças podem ser feitas praticamente sem nenhum controle. Não há consciência de que as mudanças podem interromper as operações de TI de negócio, tampouco há consciência dos benefícios de um bom gerenciamento de mudanças.

1 Inicial/ *Ad hoc* quando
É reconhecido que as mudanças devem ser gerenciadas e controladas. As práticas variam, e existe a probabilidade de execução de mudanças não autorizadas. A documentação de mudança é insuficiente ou inexistente e a de configuração é incompleta e não confiável. Provavelmente os erros ocorrem junto com interrupções no ambiente de produção devido a um gerenciamento de mudanças ineficiente.

2 Repetível, porém Intuitivo quando
Há um processo informal de gerenciamento de mudanças seguido na maioria das mudanças ocorridas, porém esse processo é desestruturado, rudimentar e propenso a erros. A precisão da documentação de configuração é inconsistente, e antes da mudança apenas são realizados um planejamento e uma avaliação limitados dos impactos.

3 Processo Definido quando
Há um processo formal de gerenciamento de mudanças, que inclui categorização, priorização, procedimentos de emergência, autorização de mudança e controle de versão, porém a conformidade com o processo ainda é emergente. São aplicadas soluções alternativas, e com frequência os processos são ignorados. Podem ocorrer erros, e mudanças não autorizadas acontecem ocasionalmente. A análise de impacto das mudanças de TI sobre as operações de negócios começa a ser formalizada para apoiar a implementação planejada de novas tecnologias e aplicações.

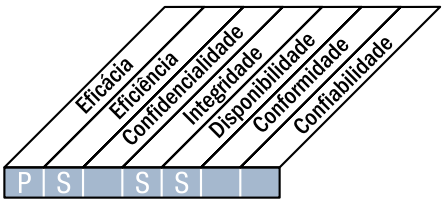
4 Gerenciado e Mensurável quando
O processo de gerenciamento de mudanças é bem desenvolvido, acompanha consistentemente todas as mudanças e os responsáveis pelo gerenciamento podem afirmar que as exceções são mínimas. Os processos são eficazes e eficientes, porém se apóiam em vários procedimentos e controles manuais para assegurar que a qualidade seja obtida. Todas as mudanças estão sujeitas ao planejamento e à avaliação de impacto para minimizar a probabilidade de problemas após a produção. Há um processo de aprovação de mudanças estabelecido. A documentação de gerenciamento de mudanças está atualizada e correta, e as mudanças são controladas formalmente. A documentação de configuração é precisa. O planejamento e a implementação do gerenciamento de mudanças estão ficando mais integrados com as mudanças nos processos de negócio, para assegurar que o treinamento, as mudanças organizacionais e as questões de continuidade de negócio sejam tratados. Há maior coordenação entre o gerenciamento de mudanças de TI e a redefinição de processos de negócio. Há um processo consistente para monitorar a qualidade e o desempenho do processo de gerenciamento de mudanças.

5 Otimizado quando
O processo de gerenciamento de mudanças é revisado e atualizado regularmente para permanecer em alinhamento com as boas práticas. O processo de revisão reflete o resultado do monitoramento. As informações de configuração são automatizadas por software e propiciam o controle de versão. O rastreamento de mudanças é sofisticado e inclui ferramentas que detectam software sem licença e não autorizado. O gerenciamento de mudanças de TI é integrado ao gerenciamento de mudanças de negócio para assegurar que a TI viabilize o crescimento da produtividade e crie novas oportunidades de negócios para a organização.

Descrição do Processo

AI7 Instalar e Homologar Soluções e Mudanças

Novos sistemas precisam ser colocados em operação uma vez concluído seu desenvolvimento. É necessária a realização de testes apropriados em um ambiente dedicado, com dados de teste relevantes, definição de instruções de implantação e migração, planejamento de liberação e mudanças no ambiente de produção e uma revisão pós-implementação. Isso assegura que os siste¬mas operacionais estejam alinhados com as expectativas e os resultados acordados.



Controle sobre o seguinte processo de TI:

Instalar e homologar soluções e mudanças

que satisfaça aos seguintes requisitos do negócio para a TI:

sistemas novos ou alterados funcionem sem maiores problemas após a instalação

com foco em:

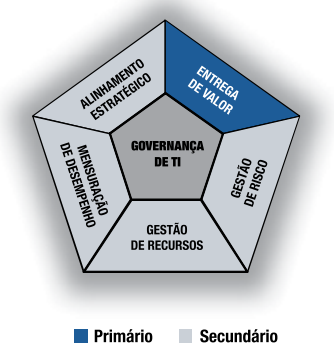
Testar se as aplicações e as soluções de infraestrutura atendem ao propósito pretendido e estão livres de erros e planejar a implementação e a migração para produção

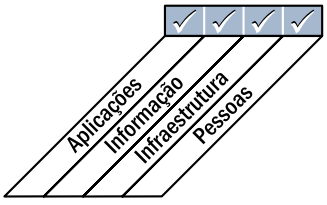
é alcançado por:

- Estabelecimento de metodologia de teste
- Realização de planejamento de liberação para produção
- Avaliação e aprovação dos resultados de testes pelos responsáveis pelo gerenciamento de negócio
- Realização de revisões após a implementação

e medido por:

- Tempo de indisponibilidade da aplicação ou quantidade de correções de dados devido a testes inadequados
- Percentual de sistemas que na avaliação pós-implementação alcança os benefícios planejados originalmente
- Percentual de projetos que tenham plano de testes documentado e aprovado





Objetivos de Controle Detalhados

AI7 Instalar e Homologar Soluções e Mudanças

AI7.1 Treinamento
Treinar a equipe dos departamentos usuários envolvidos e as equipes de operações de TI de acordo com o plano de implementação e treinamento definido e os materiais associados, como parte de todos os projetos de desenvolvimento, implementação ou modificação de sistemas de informação.

AI7.2 Plano de Teste
Estabelecer um plano de teste baseado nos padrões organizacionais que definem papéis, responsabilidades e critérios de sucesso de entrada e saída. Assegurar que o plano seja aprovado pelas partes relevantes.

AI7.3 Plano de Implementação
Estabelecer um plano de implementação e de retorno à configuração anterior. Obter aprovação de todas as partes relevantes.

AI7.4 Ambiente de Testes
Estabelecer um ambiente de testes seguro que reflita o ambiente de operações planejado no que diz respeito a segurança, controles internos, práticas operacionais, exigências de qualidade e confidencialidade e cargas de trabalho.

AI7.5 Conversão de Dados e Sistemas
Planejar a conversão de dados e a migração da infraestrutura como parte dos métodos de desenvolvimento da organização, incluindo trilhas de auditoria, procedimentos de retorno à situação anterior e de recuperação de falhas.

AI7.6 Teste de Mudanças
Assegurar que as mudanças sejam testadas de maneira independente e de acordo com o plano de testes definido antes da migração para o ambiente de produção.

AI7.7 Teste de Aceitação Final
Assegurar que o gerenciamento do departamento usuário e da área de TI avalie o resultado do processo de testes como determinado no plano de testes. Corrigir erros significativos identificados no processo de testes, executar todos os testes listados no plano de testes, bem como qualquer teste de regressão necessário. Após a avaliação, aprovar a promoção para a produção.

AI7.8 Promoção para a Produção
Após a conclusão dos testes, controlar a transferência dos sistemas alterados para operação, de acordo com o plano de implementação. Obter a aprovação das partes interessadas, como usuários, proprietário do sistema e gerência operacional. Quando apropriado, executar o sistema em paralelo com o sistema antigo durante um período e comparar comportamento/resultados.

AI7.9 Revisão pós-implementação
Estabelecer procedimentos em linha com o gerenciamento de mudanças organizacionais para garantir a realização da revisão pós-implementação, conforme definido no plano de implementação.

Diretrizes de Gerenciamento

AI7 Instalar e Homologar Soluções e Mudanças

Origem	Entrada
PO3	Padrões tecnológicos;
PO4	Proprietários formais dos sistemas;
PO8	Padrões para desenvolvimento;
PO10	Diretrizes de gerenciamento de projetos e planejamento detalhado de projetos;
AI3	Sistema configurado para ser testado/instalado;
AI4	Manuais de usuário, operação, suporte, técnico e administração;
AI5	Itens adquiridos;
AI6	Autorização de mudanças

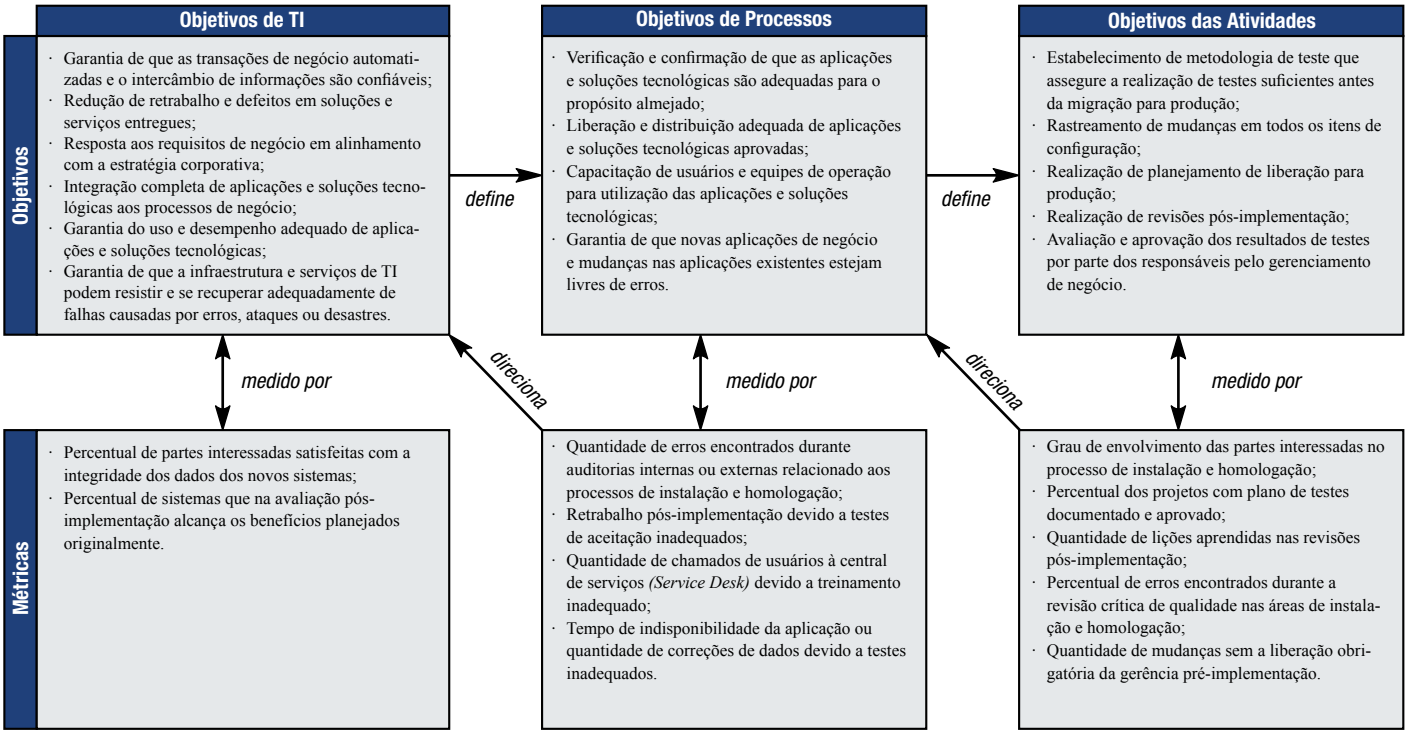
Saída	Destino						
Itens de configuração liberados;	DS8	DS9					
Erros conhecidos e aceitos;	AI4						
Migração para produção;	DS13						
Liberação de *software* e planejamento de distribuição;	DS13						
Revisão pós-implementação;	PO2	PO5	PO10				
Monitoramento de controles internos	ME2						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Confeccionar e revisar o planejamento de implantação;			C	A	I	C	C	R		C	C
Definir e revisar a estratégia de testes (critérios de entrada e saída) e a metodologia de planejamento de testes operacionais;			C	A	C	C	C	R		C	C
Confeccionar e manter um repositório de requisitos de negócio e técnicos e testes realizados em sistemas homologados;				A				R			
Realizar os testes de conversão e integração no ambiente de testes;			I	I	R	C	C	A/R		I	C
Fornecer o ambiente de testes e conduzir os testes finais de aceitação;			I	I	R	A	C	A/R		I	C
Recomendar migração para produção baseado nos critérios de homologação acordados			I	R	A	R	C	R		I	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

AI7 Instalar e Homologar Soluções e Mudanças

O gerenciamento do processo de ***"Instalar e homologar soluções e mudanças"*** que satisfaça ao requisito do negócio para a TI de ***"sistemas novos ou alterados funcionam sem maiores problemas após a instalação"*** é:

0 Inexistente quando
Há uma completa falta de processos formais de instalação e verificação, e tanto a alta gerência quanto a equipe de TI não reconhecem a necessidade de verificar se as soluções atendem ao propósito pretendido.

1 Inicial/ *Ad hoc* quando
Existe a consciência da necessidade de verificar e confirmar se as soluções implementadas servem ao propósito pretendido. Testes são executados em alguns projetos, mas a iniciativa para teste fica a cargo de cada equipe de projeto e as abordagens adotadas variam. A verificação e a comunicação formais são raras ou inexistentes.

2 Repetível, porém Intuitivo quando
Existe alguma consistência entre as abordagens de teste e verificação, mas tipicamente elas não estão baseadas em nenhuma tecnologia. Os grupos de desenvolvimento costumam decidir sobre a abordagem de teste, e normalmente não existem testes de integração. Existe um processo informal de aprovação.

3 Processo Definido quando
Existe uma metodologia formal relacionada a instalação, migração, conversão e aceitação. Os processos de instalação e verificação estão integrados em um ciclo de vida do sistema e automatizados até certo ponto. Treinamento, teste, migração para produção e verificação provavelmente estão sujeitos a desvio do processo definido, com base em decisões individuais. A qualidade dos sistemas que entram em produção é inconsistente, com novos sistemas frequentemente gerando um nível considerável de problemas pós-implementação.

4 Gerenciado e Mensurável quando
Os procedimentos são formalizados e desenvolvidos para serem bem organizados e práticos, com ambientes de teste e procedimento de validação definidos. Na prática, todas as principais mudanças feitas nos sistemas seguem esta abordagem formalizada. A avaliação de atendimento aos requisitos do usuário é padronizada e mensurável, produzindo métricas que podem ser efetivamente revisadas e analisadas pelo gerenciamento. A qualidade dos sistemas que entram no ambiente de produção é satisfatória ao gerenciamento, mesmo com níveis razoáveis de problemas pós-implementação. A automatização do processo é *ad hoc* e dependente do projeto. A gerência pode estar satisfeita com o nível atual de eficiência, apesar da falta de avaliação pós-implementação. O sistema de teste reflete adequadamente o ambiente operacional. Teste de fadiga para os novos sistemas e teste de regressão para os sistemas existentes são aplicados em grandes projetos.

5 Otimizado quando
Os processos de instalação e validação foram refinados a um nível de boa prática, com base nos resultados de refinamento e melhoria contínua. Os processos de instalação e validação estão completamente integrados ao ciclo de vida do sistema e automatizados quando apropriado, facilitando o treinamento, o teste e a migração para produção mais eficiente dos novos sistemas. Ambientes de testes bem desenvolvidos, registros de problemas e processos de resolução de erros asseguram uma migração eficiente e eficaz para o ambiente de produção. A verificação normalmente ocorre sem retrabalho, e os problemas de pós-implementação normalmente são limitados a correções menores. As revisões pós-implementação são padronizadas, e as lições aprendidas são canalizadas de volta aos processos para assegurar melhoria contínua da qualidade. Teste de fadiga para os novos sistemas e teste de regressão para os sistemas modificados são consistentemente aplicados.

Entregar e Suportar

DS1 Definir e Gerenciar Níveis de Serviços

DS2 Gerenciar Serviços Terceirizados

DS3 Gerenciar o Desempenho e a Capacidade

DS4 Assegurar a Continuidade dos Serviços

DS5 Garantir a Segurança dos Sistemas

DS6 Identificar e Alocar Custos

DS7 Educar e Treinar os Usuários

DS8 Gerenciar a Central de Serviço e os Incidentes

DS9 Gerenciar a Configuração

DS10 Gerenciar Problemas

DS11 Gerenciar os Dados

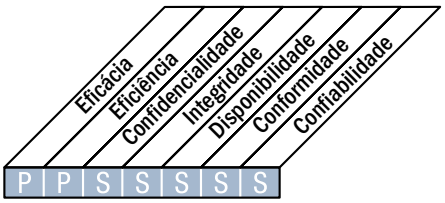
DS12 Gerenciar o Ambiente Físico

DS13 Gerenciar as Operações

DESCRIÇÃO DE PROCESSO

DS1 Definir e Gerenciar Níveis de Serviço

A comunicação eficaz entre a Direção de TI e os clientes de negócio sobre os serviços necessários é possibilitada por um acordo definido e documentado que aborda os serviços de TI e os níveis de serviço esperados. Este processo também inclui monitoramento e relatório oportuno às partes interessadas quanto ao atendimento dos níveis de serviço. Este processo permite o alinhamento entre os serviços de TI e os respectivos requisitos do negócio.



Controle sobre o seguinte processo de TI:

Definir e gerenciar níveis de serviço

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar o alinhamento dos principais serviços de TI com a estratégia de negócio

com foco em:

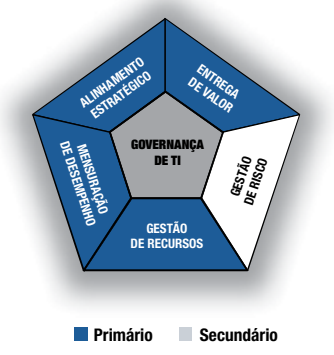
identificar os requisitos de serviço, acordar os níveis de serviço e monitorar o atendimento desses níveis de serviço

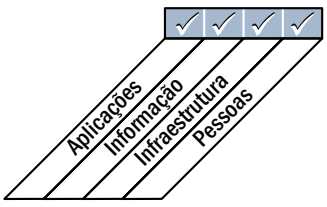
é alcançado por:

- Formalização de acordos de níveis de serviços internos e externos alinhados com os requisitos e com a capacidade de entrega.
- Reporte do atendimento aos níveis de serviços acordados (reuniões e relatórios)
- Identificação e comunicação de requisitos de serviços novos e atualizados para o planejamento estratégico

e medido por:

- Percentual das partes interessadas que entendem que os níveis de entrega de serviço estão de acordo com os níveis acordados
- Quantidade de serviços prestados inexistentes no catálogo
- Quantidade anual de reuniões formais de análise crítica de acordo de nível de serviço (SLA) com os representantes do negócio.





Objetivos de Controle Detalhados

DS1 Definir e Gerenciar Níveis de Serviço

DS1.1 Estrutura de Gestão de Níveis de Serviço
Definir um modelo que fornece um processo formalizado de gerenciamento de níveis de serviço entre o cliente e o provedor de serviço. Esse modelo mantém um contínuo alinhamento com os requisitos de negócio e suas prioridades e facilita um entendimento comum entre o cliente e o(s) provedor(es). A estrutura inclui processos para criar requisitos de serviço, definições de serviços, acordos de nível de serviço (SLAs), acordos de nível de operação (OLAs) e recursos financeiros. Esses atributos são organizados em um catálogo de serviços. A estrutura define a estrutura organizacional de gerenciamento do nível de serviço, contemplando os cargos, as tarefas e as responsabilidades dos clientes e dos provedores de serviços internos e externos.

DS1.2 Definição de Serviços
Basear as definições de serviços de TI nas características de serviços e requisitos do negócio, organizados e armazenados centralmente por meio da implementação de uma abordagem de catálogo/portfólio de serviços.

DS1.3 Acordos de Nível de Serviço
Definir e acordar os acordos de nível de serviço para todos os serviços críticos de TI com base nos requisitos do cliente e na capacidade de entrega por parte da TI. Isso abrange o comprometimento com o cliente, requisitos de suporte para atendimento aos serviços, métricas quantitativas e qualitativas de serviços aprovados pelas partes interessadas, garantia de recursos financeiros e acordos comerciais (caso aplicável), cargos e responsabilidades, inclusive a supervisão do SLA. Os itens a considerar são: disponibilidade, confiabilidade, desempenho, capacidade de crescimento, níveis de suporte, planejamento da continuidade, segurança e restrições quanto a demandas.

DS1.4 Acordos de Nível Operacional
Assegurar que os acordos de nível operacional (OLAs) expliquem como os serviços serão realizados tecnicamente de modo a apoiar o(s) SLA(s) adequadamente. Os acordos de nível operacional especificam os processos técnicos em termos compreensíveis para o provedor e podem apoiar diversos SLAs.

DS1.5 Monitoramento e Relatório de Realizações de Nível de Serviço
Monitorar continuamente os critérios de desempenho dos níveis de serviço especificados. Os relatórios devem ser disponibilizados em um formato compreensível às partes interessadas em termos de realização de níveis de serviço. As estatísticas de monitoramento são analisadas, e são tomadas medidas gerenciais para revelar as tendências negativas e positivas de cada serviço e dos serviços como um todo.

DS1.6 Revisão dos Acordos de Nível de Serviço e dos Contratos
Regularmente realizar análise crítica dos acordos de nível de serviço e dos contratos com provedores de serviço internos e externos para assegurar que sejam eficazes e atualizados e que as mudanças em requisitos tenham sido consideradas.

Diretrizes de Gerenciamento

DS1 Definir e Gerenciar Níveis de Serviço

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI; Portfólio de serviços de TI;
PO2	Classificações atribuídas a dados;
PO5	Portfólio de serviços de TI atualizado;
AI2	SLAs planejados inicialmente;
AI3	OLAs planejados inicialmente;
DS4	Requisitos de serviço para desastres, incluindo papéis e responsabilidades;
ME1	Informações de desempenho para planejamento de TI

Saída	Destino						
Relatório de revisão de contratos;	DS2						
Relatórios de desempenho de processos;	ME1						
Requisitos novos ou atualizados de serviços;	PO1						
SLAs;	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs;	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Portfólio de serviços de TI atualizado	PO1						

Tabela RACI

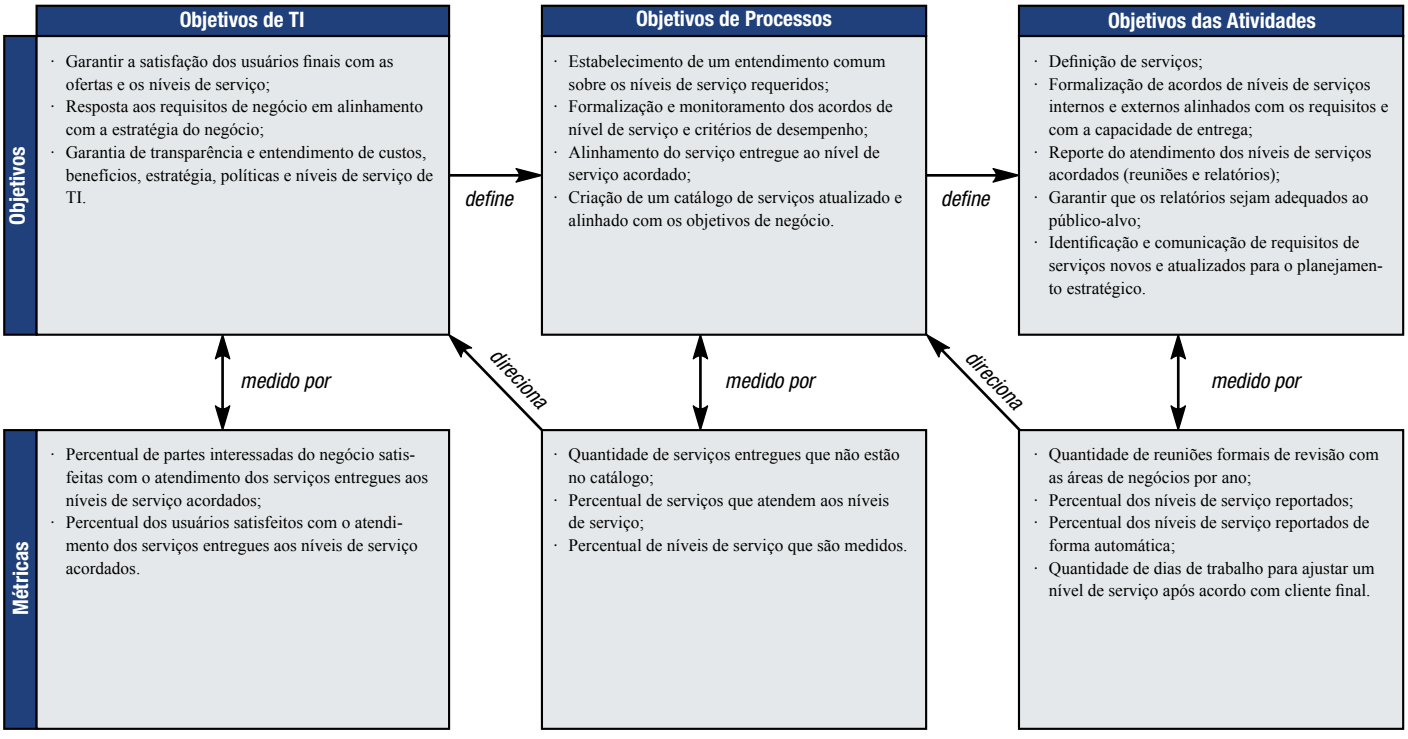
Funções

Atividades

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Gerência de Serviços
Criar uma estrutura para a definição de serviços de TI;			C	A	C	C	I	C	C	I	C	R
Produzir um catálogo de serviços de TI;			I	A	C	C	I	C	C	I	I	R
Definir acordos de níveis de serviços (SLAs) para serviços críticos de TI;		I	I	C	C	R	I	R	R	C	C	A/R
Definir acordos de níveis de operação (OLAs) para atendimento de SLAs;				I	C	R	I	R	R	C	C	A/R
Monitorar e reportar o desempenho do nível de serviço fim-a-fim;				I	I	R		I	I		I	A/R
Revisar contratos de SLA e de fornecedores de serviços;		I		I	C	R		R	R		C	A/R
Revisar e atualizar o catálogo de serviços de TI;			I	A	C	C	I	C	C	I	I	R
Criar plano de melhoria de serviços			I	A	I	R	I	R	C	C	I	R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS1 Definir e Gerenciar Níveis de Serviço

O gerenciamento do processo de ***"definir e gerenciar níveis de serviço"*** que satisfaça ao requisito do negócio para a TI de ***"assegurar o alinhamento dos principais serviços de TI com a estratégia de negócio"*** é:

0 Inexistente quando
A Direção não reconhece a necessidade de um processo para definir os níveis de serviço. Não são atribuídas responsabilidades para monitorá-los.

1 Inicial/ *Ad hoc* quando
Há consciência da necessidade de gerenciar os níveis de serviço, mas o processo é informal e reativo. As responsabilidades de definição e gerenciamento dos serviços não estão definidas. Se as medições de desempenho existem, elas são apenas qualitativas e com metas definidas de modo impreciso. Os relatórios são informais, inconsistentes e sem frequência definida.

2 Repetível, porém Intuitivo quando
Existem níveis de serviço acordados, porém são informais e não analisados criticamente. O relatório de nível de serviço é incompleto, pode ser irrelevante ou enganoso aos clientes e depende das habilidades e da iniciativa individual dos gerentes. Um coordenador de nível de serviço é indicado e tem responsabilidades definidas, porém com autoridade limitada. Se existe um processo de conformidade com os acordos de nível de serviço, ele é voluntário e não obrigatório.

3 Processo Definido quando
As responsabilidades são bem definidas, porém com autoridade baseada em julgamento individual. O processo de desenvolvimento de acordos de nível de serviço é estabelecido com pontos de verificação para reavaliação dos níveis de serviço e satisfação do cliente. Serviços e níveis de serviço são definidos, documentados e acordados seguindo um processo padrão. Níveis de serviço incompletos são identificados, contudo os procedimentos para resolver essas deficiências são informais. Existe uma clara ligação entre o alcance dos níveis de serviço esperados e o capital alocado. Os níveis de serviço são acordados, mas podem não atender às necessidades do negócio.

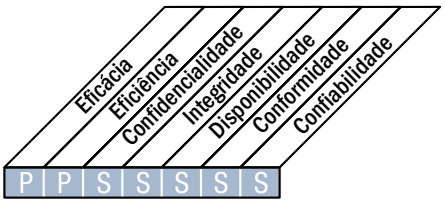
4 Gerenciado e Mensurável quando
Os níveis de serviço são cada vez mais estabelecidos na fase de definição dos requisitos de sistema e incorporados ao projeto da aplicação e dos ambientes operacionais. A satisfação dos clientes é rotineiramente medida e avaliada. As métricas de desempenho refletem as necessidades dos clientes e não as metas de TI. As métricas de avaliação dos níveis de serviço estão se tornando padronizadas e representam padrões da indústria. Os critérios para definir os níveis de serviço baseiam-se na importância dos negócios e incluem disponibilidade, confiabilidade, desempenho, capacidade de crescimento, suporte ao usuário, planejamento de continuidade e considerações de segurança. Uma análise de causa-raiz é feita rotineiramente quando os níveis de serviço não são atingidos. O processo de relato de monitoramento dos níveis de serviço está se tornando cada vez mais automatizado. Os riscos financeiros e operacionais associados à inobservância dos níveis de serviço são definidos e claramente entendidos. Um sistema formal de medição é instituído e mantido.

5 Otimizado quando
Os níveis de serviço são continuamente reavaliados para assegurar o alinhamento entre os objetivos de TI e de negócio, considerando o custo/benefício da tecnologia. Todos os processos de gerenciamento de níveis de serviço estão sujeitos a melhoria contínua. Os níveis de satisfação dos clientes são constantemente monitorados e gerenciados. Os níveis de serviço esperados refletem as metas estratégicas das unidades de negócio e são avaliados com base em padrões da indústria. A direção de TI possui os recursos e responsabilidade necessários para atingir as metas de níveis de serviço, e o esquema de remuneração é estruturado para incentivar o alcance dessas metas. A alta direção monitora as métricas de performance como parte de um processo de melhoria contínua.

Descrição de Processo

DS2 Gerenciar Serviços Terceirizados

A necessidade de assegurar que os serviços prestados por fornecedores satisfaçam aos requisitos do negócio requer um processo efetivo de gestão da terceirização. Esse processo é realizado definindo-se claramente os papéis, responsabilidades e expectativas nos acordos de terceirização bem como revisando e monitorando tais acordos quanto à efetividade e à conformidade. A gestão eficaz dos serviços terceirizados minimiza os riscos de negócio associados aos fornecedores que não cumprem seu papel.



Controle sobre o seguinte processo de TI:

Gerenciar os serviços terceirizados

que satisfaça aos seguintes requisitos do negócio para a TI:

fornecer serviços terceirizados satisfatórios e transparentes do ponto de vista de benefícios, custos e riscos

com foco em:

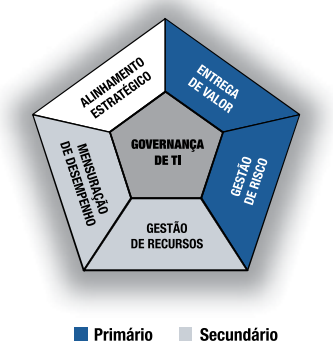
estabelecer relacionamentos e responsabilidades bilaterais com prestadores de serviço terceirizados qualificados e monitorar a entrega dos serviços para verificar e assegurar o cumprimento dos acordos

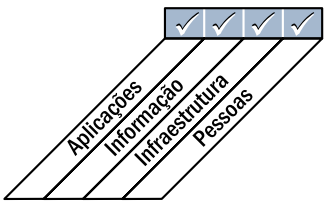
é alcançado por:

- Identificação e categorização dos prestadores de serviços
- Identificação e redução dos riscos associados ao fornecedor
- Monitoração e medição do desempenho do fornecedor

e medido por:

- Quantidade de reclamações de usuários devido aos serviços contratados
- Percentual de grandes fornecedores que atendam claramente aos requisitos e níveis de serviço definidos
- Percentual de grandes fornecedores sujeitos a monitoramento





Objetivos de Controle Detalhados

DS2 Gerenciar Serviços Terceirizados

DS2.1 Identificação do Relacionamento com Todos os Fornecedores
Identificar todos os serviços terceirizados e categorizá-los de acordo com o tipo, a importância e a criticidade. Manter documentação formal dos relacionamentos técnicos e organizacionais contemplando papéis e responsabilidades, metas, produtos esperados e as credenciais dos representantes desses fornecedores.

DS2.2 Gestão do Relacionamento com Fornecedores
Formalizar o processo de gestão do relacionamento com cada fornecedor. Os proprietários dos relacionamentos devem estabelecer ligação entre os clientes e os negócios dos fornecedores e garantir a qualidade do relacionamento com base na confiança e na transparência (por exemplo, através dos acordos de nível de serviço).

DS2.3 Gerenciamento de Riscos do Fornecedor
Identificar e minimizar os riscos relacionados à capacidade dos fornecedores de prestação efetiva de serviços de maneira contínua, segura e eficiente. Garantir que os contratos estejam em conformidade com os padrões universais de negócios de acordo com as exigências legais e regulamentares. O gerenciamento de riscos deve considerar acordos de confidencialidade (NDA), condições gerais e garantias dos contratos, viabilidade continuada do fornecedor, conformidade com requisitos de segurança, fornecedores alternativos, penalidades e gratificações etc.

DS2.4 Monitoramento de Desempenho do Fornecedor
Estabelecer um processo para monitorar a prestação do serviço de modo a assegurar que o fornecedor atenda aos requisitos atuais do negócio, obedecendo os contratos e acordos de nível de serviço firmados, e que seu desempenho seja competitivo com outros prestadores e condições do mercado.

Diretrizes de Gerenciamento

DS2 Gerenciar Serviços Terceirizados

Origem	Entrada
PO1	Estratégia de fornecimento de TI;
PO8	Padrões para aquisição;
AI5	Tratativas contratuais; Requisitos de gerenciamento de relacionamento com terceiros;
DS1	SLAs; Relatório de revisão de contratos;
DS4	Requisitos de serviço para desastres, incluindo papéis e responsabilidades

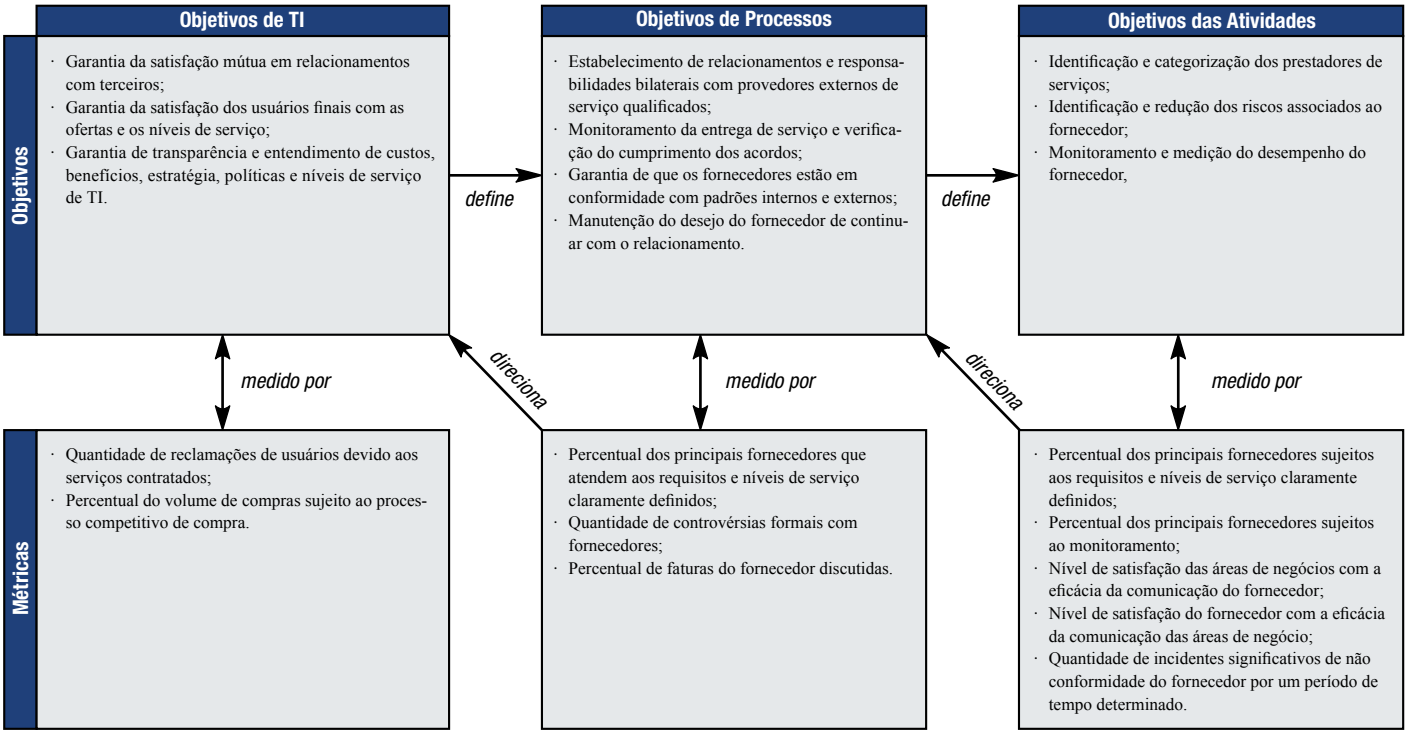
Saída	Destino
Relatórios de desempenho de processos;	ME1
Catálogo de fornecedores;	AI5
Riscos de fornecedores	PO9

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Identificar e categorizar relacionamentos com prestadores de serviços terceirizados;				I	C	R	C	R	A/R	C	C
Definir e documentar o processo de gestão de fornecedores;		C		A	I	R	I	R	R	C	C
Estabelecer políticas e procedimentos de seleção e avaliação de fornecedores;		C		A	C	C		C	R	C	C
Identificar, avaliar criticamente e mitigar riscos de fornecimento;		I		A		R		R	R	C	C
Monitorar a entrega de serviços de fornecedores;				R	A	R		R	R	C	C
Avaliar os objetivos de longo prazo do relacionamento com fornecedores de serviços para todas as partes interessadas	C	C	C	A/R	C	C	C	C	R	C	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS2 Gerenciar os Serviços Terceirizados

O gerenciamento do processo de ***"gerenciar os serviços terceirizados"*** que satisfaça ao requisito do negócio para a TI de ***"fornecer serviços terceirizados satisfatórios e transparentes do ponto de vista de benefícios, custos e riscos"*** é:

0 Inexistente quando
As responsabilidades não estão definidas. Não há políticas e procedimentos formais referentes à contratação de serviços terceirizados. Os serviços terceirizados não são aprovados nem analisados criticamente pela Direção. Não existem avaliações e informes por parte dos terceiros. Com a ausência de obrigação contratual de reportar, a alta direção não está informada sobre a qualidade dos serviços prestados.

1 Inicial/ *Ad hoc* quando
A Direção está consciente da necessidade de haver políticas e procedimentos documentados para a gestão da terceirização, incluindo contratos assinados. Não há termos padronizados para acordos com prestadores de serviço. A avaliação dos serviços prestados é informal e reativa. As práticas dependem da experiência individual e dos fornecedores (por exemplo, sob demanda).

2 Repetível, porém Intuitivo quando
O processo para supervisionar os fornecedores de serviços terceirizados, riscos associados e entrega dos serviços é informal. É utilizado um contrato *pro forma* assinado, contendo termos e condições padronizados pelos distribuidores/vendedores (por exemplo, a descrição dos serviços a serem prestados). Relatórios dos serviços prestados são disponibilizados, mas não satisfazem aos objetivos do negócio.

3 Processo Definido quando
Procedimentos bem documentados são implantados para governar os serviços terceirizados, com processos claros para examinar cuidadosamente e negociar com os prestadores. Quando um acordo de prestação de serviços é realizado, o relacionamento com o terceiro é puramente contratual. A natureza dos serviços a serem prestados é detalhada no contrato e contempla as exigências operacionais, legais e de controle. A responsabilidade pela supervisão dos serviços terceirizados é definida. Os termos contratuais são baseados em modelos padronizados. O risco para o negócio associado aos serviços terceirizados é avaliado e relatado.

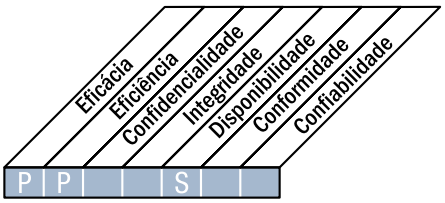
4 Gerenciado e Mensurável quando
São estabelecidos critérios formais e padronizados para definir os termos de compromisso, inclusive o escopo do serviço, produtos/serviços a serem fornecidos, premissas, programação, custos, modelos de cobrança e responsabilidades. As responsabilidades pela gestão dos fornecedores e contratos são atribuídas. As qualificações, os riscos e as capacidades associados ao fornecedor são continuamente verificados. Os requisitos de serviço são definidos e vinculados aos objetivos do negócio. Existe um processo de análise crítica do desempenho do serviço frente aos termos contratuais, dando condições para uma avaliação atual e futura dos serviços terceirizados. Modelos de repasses de custos são utilizados nos processos de compras. Todas as partes envolvidas estão cientes do serviço, do custo e dos marcos de tempo esperados. Existem objetivos e métricas acordados para a supervisão dos fornecedores de serviços.

5 Otimizado quando
Os contratos assinados com terceiros são criticamente analisados em intervalos predefinidos. A responsabilidade pela gestão dos fornecedores e da qualidade dos serviços prestados é atribuída. Evidências de adesão contratual das medidas de controle, legais e operacionais são monitoradas e ações corretivas são impostas. O terceirizado está sujeito a auditorias periódicas independentes, e o feedback do desempenho é realizado e utilizado para melhorar a prestação dos serviços. As avaliações variam conforme as mudanças nas condições do negócio. As métricas suportam a prévia detecção de problemas em potencial nos serviços terceirizados. A remuneração de terceiros está ligada ao alcance de níveis de serviço amplos acordados. A Direção ajusta o processo de aquisição e monitoramento do serviço terceirizado com base nas métricas.

DESCRIÇÃO DE PROCESSO

DS3 Gerenciar o Desempenho e a Capacidade

A necessidade de gerenciar o desempenho e a capacidade dos recursos de TI requer um processo que realize análises críticas periódicas do desempenho e da capacidade atuais dos recursos de TI. Esse processo inclui a previsão de necessidades futuras com base em requisitos de carga de trabalho, armazenamento e contingência. Esse processo assegura que os recursos de informação que suportam os requisitos do negócio estejam sempre disponíveis.



Controle sobre o seguinte processo de TI:

Gerenciar o desempenho e a capacidade

que satisfaça aos seguintes requisitos do negócio para a TI:

otimizar o desempenho da infraestrutura, dos recursos e das capacidades de TI em resposta às necessidades do negócio

com foco em:

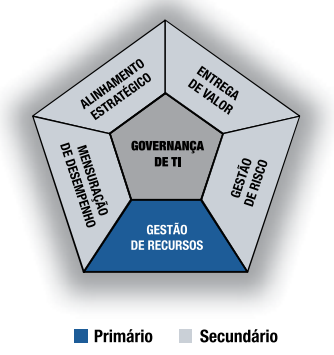
atender aos requisitos de tempo de resposta dos diversos acordos de nível de serviço, minimizar o período de indisponibilidade e proporcionar melhorias contínuas no desempenho e na capacidade de TI através de monitoramento e medição

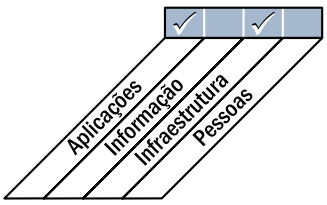
é alcançado por:

- Planejamento e fornecimento de capacidade e disponibilidade dos sistemas
- Monitoração e informe do desempenho dos sistemas
- Modelagem e previsão do desempenho dos sistemas

e medido por:

- Quantidade de horas perdidas pelo usuário por mês devido ao planejamento insuficiente da capacidade
- Percentual de picos onde a utilização desejada é excedida
- Percentual de tempo de resposta em que os SLAs não são alcançados





OBJETIVOS DE CONTROLE DETALHADOS

DS3 Gerenciar o Desempenho e a Capacidade

DS3.1 Desempenho e Planejamento de Capacidade
Estabelecer um processo de planejamento para a realização de análise crítica do desempenho e da capacidade dos recursos de TI, de forma a assegurar que com custos justificáveis o desempenho e a capacidade estejam disponíveis para processar a carga de serviço acordada conforme determinam os acordos de nível de serviço. Os planos de capacidade e desempenho devem considerar técnicas de modelagem apropriadas para produzir modelos de capacidade e desempenho atuais e futuros de recursos de TI.

DS3.2 Capacidade e Desempenho Atuais
Realizar a análise crítica do desempenho e a capacidade atual dos recursos de TI de forma a determinar se existe capacidade e desempenho suficientes para atendimento conforme os níveis de serviço acordados.

DS3.3 Capacidade e Desempenho Futuros
Conduzir regularmente a previsão de desempenho e capacidade dos recursos de TI para minimizar o risco de interrupção de serviços devido a capacidade insuficiente ou degradação do desempenho. Identificar também o excesso de capacidade para possível remanejamento. Identificar as tendências de carga de trabalho e realizar previsões para orientar o plano de capacidade e desempenho.

DS3.4 Disponibilidade de Recursos de TI
Fornecer a capacidade e o desempenho necessários, levando em consideração aspectos como cargas normais de trabalho, contingências, requisitos de armazenamento e ciclos de vida de recurso de TI. Medidas devem ser tomadas quando o desempenho e a capacidade não estão alinhados com o nível necessário (por exemplo, priorizar tarefas, mecanismos de tolerância a falhas e práticas de alocação de recurso). A Direção deve assegurar que os planos de contingência viabilizem apropriadamente a disponibilidade, a capacidade e o desempenho de cada recurso de TI.

DS3.5 Monitoramento e Relatórios
Monitorar constantemente o desempenho e a capacidade dos recursos de TI. Os dados acumulados atendem a dois propósitos:
- Manter e sintonizar o desempenho atual no ambiente de TI e tratar questões como capacidade de recuperação, contingência, cargas de trabalho atuais e previstas, planejamento de armazenamento e aquisição de recursos.
- Relatar a disponibilidade de serviços prestados ao negócio conforme determinado pelos SLAs. Acompanhar todos os relatórios de exceções com recomendações de ações corretivas.

Diretrizes de Gerenciamento

DS3 Gerenciar o Desempenho e a Capacidade

Origem	Entrada
AI2	Especificações de disponibilidade, continuidade e recuperação;
AI3	Requisitos de monitoramento de sistema;
DS1	SLAs

Saída	Destino						
Informação de desempenho e capacidade;	PO2	PO3					
Planejamento de desempenho e capacidade (requisitos);	PO5	AI1	AI3	ME1			
Mudanças necessárias;	AI6						
Relatórios de desempenho de processos	ME1						

Tabela RACI

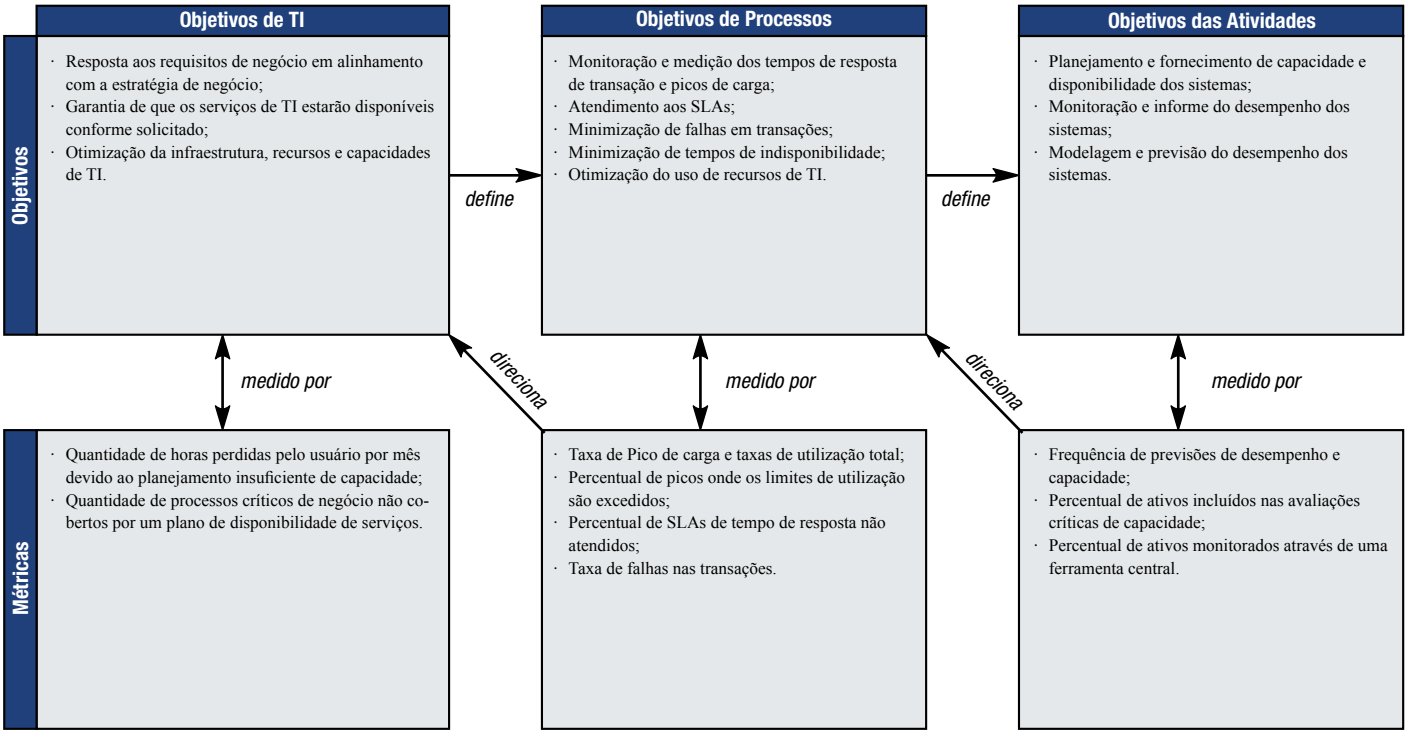
Funções

Atividades

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Estabelecer um processo de planejamento para revisar o desempenho e capacidade de recursos de TI;				A		R	C	C	C	C	
Revisar o desempenho e capacidade atuais de recursos de TI;				C	I	A/R		C	C	C	
Conduzir previsão de desempenho e capacidade de recursos de TI;				C	C	A/R	C	C	C	C	
Conduzir análises de desvios para identificar erros de dimensionamento de recursos de TI;				C	I	A/R		R	C	C	I
Conduzir um plano de contingência para potenciais indisponibilidades de recursos de TI;				C	I	A/R		C	C	I	C
Monitorar constantemente e reportar a disponibilidade, desempenho e capacidade de recursos de TI				I	I	A/R		I	I	I	I

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS3 Gerenciar o Desempenho e a Capacidade

O gerenciamento do processo de ***"gerenciar o desempenho e a capacidade"*** que satisfaça ao requisito do negócio para a TI de ***"otimizar o desempenho da infraestrutura, recursos e capacidades de TI em resposta às necessidades do negócio"*** é:

0 Inexistente quando
A Direção não reconhece que os principais processos de negócio podem exigir altos níveis de desempenho de TI ou que a necessidade total do negócio por serviços de TI possa exceder a capacidade atual. Não está implementado um processo de planejamento de capacidade.

1 Inicial/ *Ad hoc* quando
Com frequência os usuários precisam contornar limitações de desempenho e capacidade. Os proprietários dos processos de negócio não entendem a necessidade do planejamento de desempenho e capacidade. A medida tomada no sentido do gerenciamento de desempenho e de capacidade é tipicamente reativa. O processo de planejamento de capacidade e desempenho é informal. O entendimento do desempenho e da capacidade atuais e futuros dos recursos de TI é limitado.

2 Repetível, porém Intuitivo quando
As Direções do negócio e de TI têm consciência do impacto do não-gerenciamento de desempenho e capacidade. As necessidades de desempenho são geralmente satisfeitas com base nas avaliações de sistemas individuais e no conhecimento das equipes de suporte e de projeto. Algumas ferramentas individuais até podem ser utilizadas para diagnosticar os problemas de capacidade e desempenho, porém a consistência dos resultados depende da perícia de pessoas-chave. Não há uma avaliação abrangente da capacidade de desempenho de TI ou considerações sobre os picos de demanda e cenários de pior caso. Problemas de disponibilidade possivelmente ocorrem de modo aleatório, e há uma demora considerável para diagnosticá-los e corrigi-los. Qualquer medição de desempenho é fundamentada primeiramente nas necessidades da TI e não nas necessidades do cliente.

3 Processo Definido quando
Os requisitos de desempenho e capacidade são definidos ao longo do ciclo de vida do sistema. Existem requisitos e métricas de nível de serviço definidos que podem ser utilizados para medir o desempenho operacional. Requisitos futuros de desempenho e capacidade são modelados seguindo um processo definido. Os relatórios são elaborados fornecendo estatísticas de desempenho. Problemas relativos a desempenho e capacidade ainda podem ocorrer e demandarão tempo para serem corrigidos. Apesar dos níveis de serviço divulgados, os usuários e clientes podem se sentir céticos no tocante à capacidade de serviço.

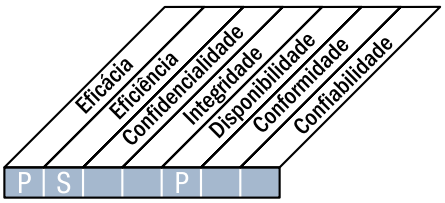
4 Gerenciado e Mensurável quando
Processos e ferramentas estão disponíveis para medir o uso, o desempenho e a capacidade do sistema, e os resultados são comparados aos objetivos definidos. Há informação atualizada, com estatísticas de desempenho padronizadas e alertas de incidentes causados por capacidade e desempenho insuficientes. Questões de capacidade e desempenho insuficientes são negociadas de acordo com os procedimentos padronizados e definidos. Ferramentas automatizadas são utilizadas para monitorar recursos específicos, tais como espaço em disco, redes lógicas, servidores e ativos de rede. As estatísticas de capacidade e desempenho são relatadas com base nos processos de negócio, por isso os usuários e clientes entendem os níveis de serviço de TI. Os usuários geralmente se sentem satisfeitos com a capacidade de serviço atual e podem demandar níveis de disponibilidade novos e aperfeiçoados. As métricas para medição de desempenho e capacidade foram acordadas, mas aplicadas apenas de forma esporádica e inconsistente.

5 Otimizado quando
Os planos de desempenho e capacidade são completamente sincronizados com as previsões de demanda de negócio. A demanda de negócio e a infraestrutura de TI estão sujeitas a análises críticas regulares para assegurar que uma ótima capacidade seja alcançada no mais baixo custo possível. As ferramentas para monitorar os recursos críticos de TI têm sido padronizadas e utilizadas nas plataformas e relacionadas ao sistema de gerenciamento de incidentes corporativos. As ferramentas de monitoramento detectam e podem corrigir automaticamente problemas relacionados ao desempenho e à capacidade. Análise de tendências é executada para revelar problemas de desempenho iminentes causados pelo crescente volume de negócios, o que permite planejar e evitar problemas inesperados. As métricas para mensuração de desempenho e capacidade de TI têm sido bem sintonizadas com as medidas de resultados esperados e os indicadores de performance em todos os processos críticos de negócio e são avaliadas consistentemente. A Direção ajusta o planejamento de desempenho e capacidade seguindo a análise dessas métricas.

DESCRIÇÃO DE PROCESSO

DS4 Assegurar a Continuidade dos Serviços

Prover a continuidade dos serviços de TI requer o desenvolvimento, manutenção e teste de um plano de continuidade de TI, armazenamento de cópias de segurança *(backup)* em instalações remotas *(offsite)* e realizar treinamentos periódicos do plano de continuidade. Um processo eficaz de continuidade de serviços minimiza a probabilidade e o impacto de uma interrupção de um serviço chave de TI nas funções e processos críticos de negócio.



Controle sobre o seguinte processo de TI:

Assegurar a continuidade dos serviços

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar um impacto mínimo nos negócios no caso de uma interrupção dos serviços de TI

com foco em:

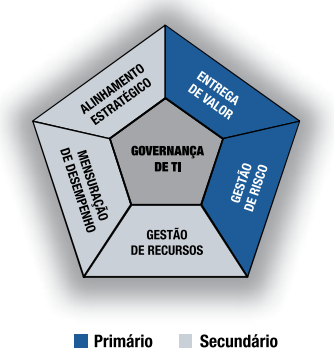
incorporar a capacidade de recuperação em soluções automatizadas e desenvolver, manter e testar os planos de continuidade

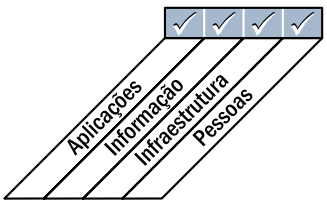
é alcançado por:

- Desenvolvimento, manutenção e melhoria da contingência de TI
- Treinamento e teste de planos de contingência de TI
- Armazenamento em locais remotos *(offsite)* de cópias dos dados e dos planos de contingência

e medido por:

- Quantidade de horas perdidas por usuários por mês devido inoperância de sistema não planejada
- Quantidade de processos críticos de negócio dependentes da TI e não contemplados no plano de continuidade de TI





Objetivos de Controle Detalhados

DS4 Assegurar a Continuidade dos Serviços

DS4.1 Estrutura de Continuidade
Desenvolver um modelo para continuidade de TI a fim de apoiar o gerenciamento da continuidade do negócio de toda a empresa através de um processo consistente. O objetivo do modelo é apoiar na determinação das necessidades de capacitação em recuperação da infraestrutura e conduzir o desenvolvimento dos planos de contingência de TI e recuperação de desastres. O modelo deve orientar a estrutura organizacional quanto ao gerenciamento da continuidade, contemplando papéis, tarefas e responsabilidades dos provedores de serviço internos e externos, seus gerenciamentos, clientes e as regras e estruturas para documentar, testar e executar planos de recuperação de desastres e continuidade de TI. O plano também deve tratar fatores como identificação de recursos críticos, monitoramento e informe de disponibilidade de recursos críticos, processamento alternativo e princípios de cópia de segurança *(backup)* e recuperação.

DS4.2 Planos de Continuidade de TI
Desenvolver planos de continuidade de TI com base na estrutura e projetados para reduzir o impacto de uma grande interrupção de funções e processos de negócio fundamentais. Os planos devem ser baseados no entendimento do risco de possíveis impactos no negócio, contemplar os requisitos de capacidade de restabelecimento, processamento alternativo e capacidade de recuperação de todos os serviços críticos de TI. Também devem abranger manuais de uso, papéis, responsabilidades, procedimentos, processos de comunicação e abordagens de teste.

DS4.3 Recursos Críticos de TI
Dar atenção especial aos itens mais críticos no plano de continuidade de TI para assegurar a capacidade de restabelecimento e definir prioridades em situações de recuperação. Prevenir o desvio de atenção para os itens de recuperação menos críticos e assegurar resposta e recuperação em alinhamento com as necessidades de negócio de maior importância; ao mesmo tempo, assegurar que os custos sejam mantidos em um nível aceitável e em conformidade com os requisitos contratuais e regulamentares. Considerar a capacidade de restauração e os requisitos de resposta e recuperação em diferentes níveis (por exemplo, de 1 a 4 horas, de 4 horas a 24 horas, mais de 24 horas e os períodos operacionais de negócios críticos).

DS4.4 Manutenção do Plano de Continuidade de TI
Encorajar o gerenciamento de TI a definir e executar procedimentos de controle de mudança para assegurar que o plano de continuidade de TI seja mantido atualizado e reflita sempre os requisitos de negócios atuais. É essencial que as mudanças nos procedimentos e responsabilidades sejam comunicadas claramente e de forma oportuna.

DS4.5 Teste do Plano de Continuidade de TI
Testar o plano de continuidade de TI regularmente para assegurar que os sistemas de TI possam ser efetivamente recuperados, que desvios sejam tratados e que o plano se mantenha relevante. Para tanto, são necessários preparação cuidadosa, documentação, registro dos resultados dos testes e implementação de planos de ação de acordo com os resultados. Deve-se considerar estender o teste de recuperação apenas de aplicações isoladas a cenários de testes fim a fim integrados com fornecedores.

DS4.6 Treinamento do Plano de Continuidade de TI
Assegurar que todas as partes envolvidas recebam treinamento regular sobre os procedimentos, papéis e respectivas responsabilidades no caso de um incidente ou desastre. Verificar e intensificar o treinamento de acordo com os resultados dos teste de continuidade.

DS4.7 Distribuição do Plano de Continuidade
Definir e gerenciar uma estratégia de distribuição para assegurar que os planos sejam seguramente distribuídos e que estejam apropriadamente disponíveis às partes interessadas e autorizados quando e onde necessário. Toda atenção deve ser dispensada para tornar o plano acessível em todos os cenários de desastre.

DS4.8 Recuperação e Retomada dos Serviços de TI
Planejar as ações a serem executadas nos momentos de recuperação e retomada dos serviços de TI. Isto pode incluir ativação de *backup sites*, iniciação de processamento alternativo, comunicação para as partes interessadas e os clientes, procedimentos de retorno à produção etc. Assegurar que o negócio entenda o tempo de recuperação de TI e os investimentos tecnológicos necessários para sustentar as necessidades de recuperação e retorno à produção.

DS4.9 Armazenamento de Cópias de Segurança em Locais Remotos
Armazenar remotamente todas as mídias de cópias de segurança críticas, documentação e outros recursos de TI necessários para a recuperação da TI e os planos de continuidade de negócio. O conteúdo armazenado nas cópias de segurança precisa ser determinado em colaboração entre os proprietários dos processos de negócio e o pessoal de TI. O gerenciamento das instalações de armazenamento remotas deve atentar para a política de classificação de dados e as práticas de armazenamento de mídias da empresa. O gerenciamento de TI deve assegurar que as condições dos locais de armazenamento remotos sejam periodicamente avaliadas, pelo menos anualmente, nos quesitos conteúdo, proteção ambiental e segurança. Assegurar a compatibilidade de *hardware* e *software* para restaurar os dados arquivados e testar e atualizar periodicamente os dados arquivados.

DS4.10 Revisão Pós-Retomada dos Serviços
Após a retomada bem-sucedida da função de TI depois de um desastre, determinar se o gerenciamento de TI tem procedimentos para avaliar a adequação do plano atual e realizar sua atualização, se necessário.

Diretrizes de Gerenciamento

DS4 Assegurar a Continuidade dos Serviços

Origem	Entrada
PO2	Classificações atribuídas a dados;
PO9	Avaliação de riscos;
AI2	Especificações de disponibilidade, continuidade e recuperação;
AI4	Manuais de usuário, operação, suporte, técnico e administração;
DS1	SLAs e OLAs

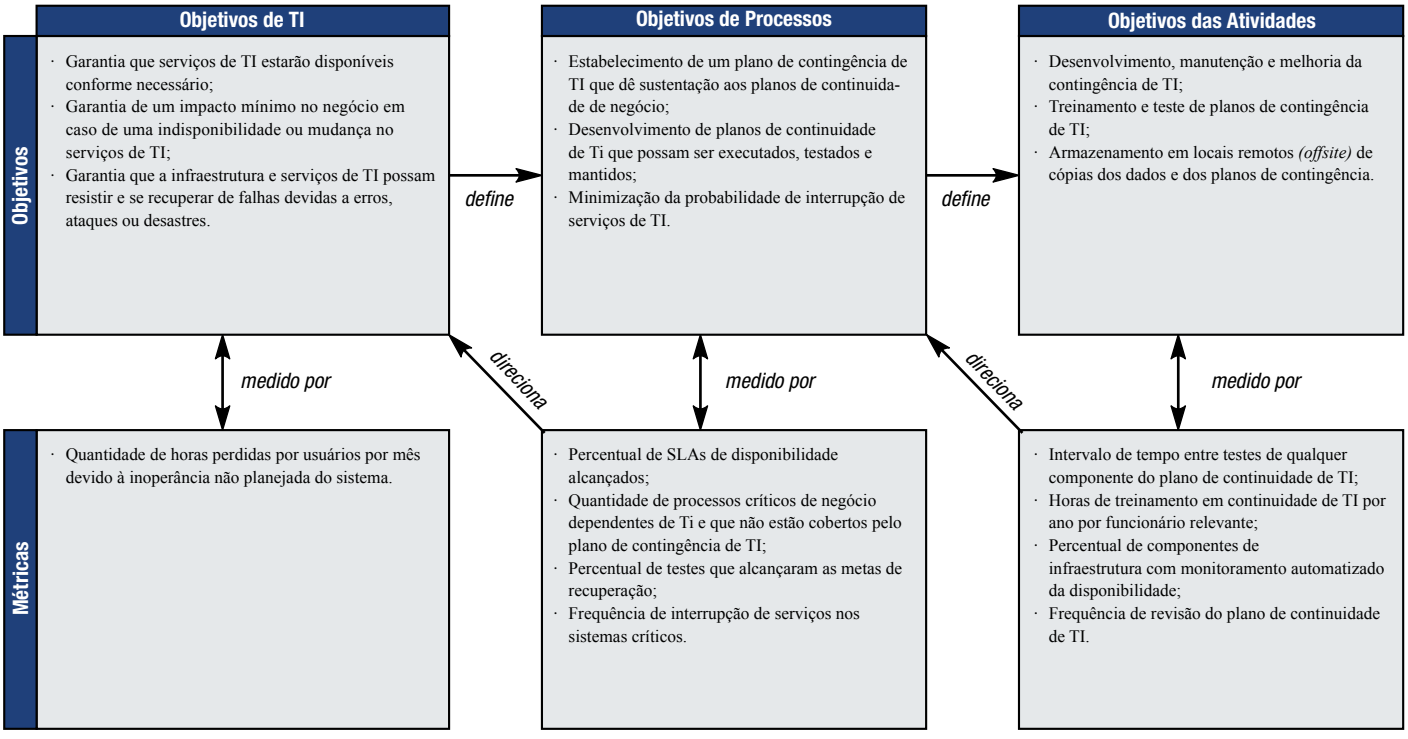
Saída	Destino						
Resultados dos testes de contingência;	PO9						
Criticidade dos itens de configuração de TI;	DS9						
Plano de guarda e proteção de cópias de segurança *(backups)*;	DS11	DS13					
Níveis de incidentes/desastres;	DS8						
Requisitos de serviço para desastres, incluindo papéis e responsabilidades;	DS1	DS2					
Relatórios de desempenho de processos	ME1						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Desenvolver uma estrutura de continuidade de TI;		C	C	A	C	R	R	R	C	C	R
Realizar uma análise de impacto no negócio (BIA) e avaliação de riscos;		C	C	C	C	A/R	C	C	C	C	C
Desenvolver e manter planos de continuidade de TI;	I	C	C	C	I	A/R		C	C	C	C
Identificar e categorizar recursos de TI baseado em objetivos de recuperação;				C		A/R		C	I	C	I
Definir e executar procedimentos de controle de mudanças para assegurar a atualização do plano de continuidade de TI;				I		A/R		R	R	R	I
Testar frequentemente o plano de continuidade de TI;				I	I	A/R		C	C	I	I
Desenvolver um plano de ações com base nos resultados dos testes;				C	I	A/R	C	R	R	R	I
Planejar e conduzir treinamento de continuidade de TI;				I	R	A/R		C	R	I	I
Planejar a recuperação dos serviços de TI;		I	I	C	C	A/R	C	R	R	R	C
Planejar e implementar a guarda e proteção das cópias de segurança *(backup)*;				I		A/R		C	C	I	I
Estabelecer procedimentos para condução de revisões pós-restabelecimento dos serviços				C	I	A/R		C	C		C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS4 Assegurar a Continuidade dos Serviços

O gerenciamento do processo de ***"assegurar a continuidade dos serviços"*** que satisfaça ao requisito do negócio para a TI de ***"assegurar um impacto mínimo nos negócios no caso de uma interrupção nos serviços de TI"*** é:

0 Inexistente quando
Não há entendimento dos riscos, vulnerabilidades e ameaças às operações de TI ou do impacto da perda dos serviços de TI nos negócios. Não é considerado que a continuidade dos serviços deve ter atenção da Direção.

1 Inicial /*Ad hoc* quando
As responsabilidades pela continuidade dos serviços são informais e a autoridade para exercer essas responsabilidades é limitada. O gerenciamento está se tornando consciente dos riscos relacionados e da necessidade da continuidade dos serviços. O foco da Direção quanto à continuidade dos serviços está relacionado aos recursos de infraestrutura e não aos serviços de TI. Os usuários implementam paliativos em resposta a interrupções nos serviços. A resposta da TI para a maioria das interrupções é reativa e despreparada. Paralisações dos sistemas são agendadas para atender às necessidades da TI, porém não consideram os requisitos do negócio.

2 Repetível, porém Intuitivo quando
A responsabilidade de assegurar a continuidade do serviço é estabelecida. As abordagens para assegurar a continuidade do serviço são fragmentadas. Relatórios de disponibilidade de sistema são esporádicos, podem ser incompletos e não levam em consideração o impacto nos negócios. Não existe um plano de continuidade de TI documentado, embora haja comprometimento da continuidade da disponibilidade de serviços e seus maiores princípios sejam conhecidos. Existe um inventário de sistemas e componentes críticos, mas ele pode não ser confiável. Práticas de serviços contínuos estão surgindo, contudo o sucesso depende das pessoas.

3 Processo Definido quando
A responsabilidade solidária pelo gerenciamento da continuidade dos serviços está clara. A responsabilidade pelo planejamento e pelos testes da continuidade dos serviços é claramente definida e atribuída. O plano de continuidade de TI é documentado e baseia-se na importância do sistema e no impacto nos negócios. Há relatos periódicos dos testes de continuidade de serviços. As pessoas tomam a iniciativa de seguir padrões e recebem treinamento para lidar com a maioria dos incidentes ou desastres. A Direção comunica consistentemente a necessidade do plano de assegurar a continuidade de serviço. Componentes de alta disponibilidade e redundância de sistema estão sendo aplicados. É mantido um inventário sobre os componentes e sistemas críticos.

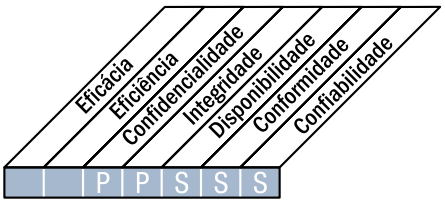
4 Gerenciado e Mensurável quando
As responsabilidades e os padrões para a continuidade dos serviços são impostos. A responsabilidade por manter o plano de continuidade de serviço é atribuída. As atividades de manutenção são baseadas nos testes de continuidade de serviço, em boas práticas internas, e na mudança do ambiente de negócio e de TI. Dados estruturados sobre a continuidade dos serviços estão sendo coletados, analisados, relatados e gerando ações. É dado treinamento obrigatório e formal sobre os processos de continuidade de serviço. Boas práticas de disponibilidade de sistemas estão sendo consistentemente implementadas. As práticas de disponibilidade e planejamento de continuidade de serviços influenciam um ao outro. Os incidentes de descontinuidade são classificados e os procedimentos de encaminhamento de cada incidente é bem conhecido por todos os envolvidos. Objetivos e métricas de continuidade dos serviços foram desenvolvidos e acordados, mas podem ser inconsistentemente medidos.

5 Otimizado quando
Processos integrados de continuidade de serviços consideram a comparação com o mercado *(benchmarking)* e as melhores práticas externas. O plano de continuidade de TI é integrado ao plano de continuidade de negócio e é rotineiramente mantido. A necessidade de assegurar a continuidade de serviços é garantida pelos fornecedores e principais prestadores de serviço. Ocorrem testes formais do plano de continuidade de TI, e seus resultados são a base da atualização do plano. Coleta e análise dos dados são utilizados para melhoria contínua do processo. O planejamento de continuidade de serviço e as práticas de disponibilidade estão completamente alinhados. A Direção assegura que um desastre ou incidente importante não ocorrerá devido a um único ponto de falha. Práticas de encaminhamento são entendidas e rigorosamente impostas. Os objetivos e métricas sobre o alcance da continuidade de serviços são mensurados de forma sistemática. A Direção ajusta o planejamento à continuidade do serviço em resposta às medições.

Descrição do Processo

DS5 Garantir a Segurança dos Sistemas

Para manter a integridade da informação e proteger os ativos de TI, é necessário implementar um processo de gestão de segurança. Esse processo inclui o estabelecimento e a manutenção de papéis, responsabilidades, políticas, padrões e procedimentos de segurança de TI. A gestão de segurança inclui o monitoramento, o teste periódico e a implementação de ações corretivas das deficiências ou dos incidentes de segurança. A gestão eficaz de segurança protege todos os ativos de TI e minimiza o impacto sobre os negócios de vulnerabilidades e incidentes de segurança.



Controle sobre o seguinte processo de TI:

Garantir a segurança dos sistemas

que satisfaça aos seguintes requisitos do negócio para a TI:

manter a integridade da infraestrutura de informação e de processamento e minimizar o impacto de vulnerabilidades e incidentes de segurança

com foco em:

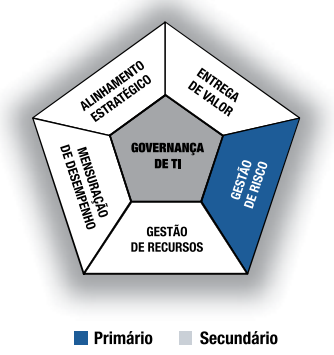
definir políticas, procedimentos e padrões de segurança de TI e monitorar, detectar, reportar e solucionar vulnerabilidades e incidentes de segurança

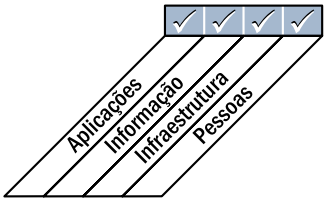
é alcançado por:

· Entendimento dos requisitos, vulnerabilidades e ameaças de segurança
· Gerenciamento padronizado das identidades e autorizações de usuários
· Testes periódicos de segurança

e medido por:

· Quantidade de incidentes que prejudicam a reputação pública da corporação
· Quantidade de sistemas em que os requisitos de segurança não são atendidos
· Quantidade de violações na segregação de funções





Objetivos de Controle Detalhados

DS5 Garantir a Segurança dos Sistemas

DS5.1 Gestão da Segurança de TI
Gerenciar a segurança de TI no mais alto nível organizacional da empresa de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio.

DS5.2 Plano de Segurança de TI
Traduzir os requisitos de negócio, de risco e conformidade, em um plano abrangente de segurança de TI, que leve em consideração a infraestrutura de TI e a cultura de segurança. O plano deve ser implementado em políticas e procedimentos de segurança, juntamente com investimentos adequados em serviços, pessoal, software e hardware. Políticas e procedimentos de segurança devem ser comunicados aos usuários e partes interessadas.

DS5.3 Gestão de Identidade
Todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, desenvolvimento, operação e manutenção de sistemas) devem ser identificáveis de modo exclusivo. Os direitos de acesso dos usuários aos sistemas e dados devem estar em conformidade com as necessidades dos negócios e com os requisitos da função definidos e documentados. Os direitos de acesso devem ser solicitados pela gestão de usuários, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança. As identidades e os direitos de acesso dos usuários devem ser mantidos em um repositório central. É necessário implementar e manter atualizadas medidas técnicas e de procedimentos com boa relação custo-benefício para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso.

DS5.4 Gestão de Contas de Usuário
Assegurar que a solicitação, a emissão, a suspensão, a modificação e o bloqueio de contas de usuário e dos respectivos privilégios sejam tratados por procedimentos de gestão de contas de usuário. Incluir um procedimento de aprovação de concessão de direitos de acesso pelos proprietários dos dados ou sistemas. Esse procedimento deve ser aplicado a todos os usuários, inclusive aos administradores (usuários com privilégios), usuários internos e externos, para os casos normais ou emergenciais. Os direitos e obrigações relativos ao acesso a sistemas e informações corporativos devem ser definidos em contrato para todos os tipos de usuários. Devem ser feitas revisões frequentes de todas as contas e os respectivos privilégios.

DS5.5 Teste de Segurança, Vigilância e Monitoramento
Garantir que a implementação de segurança de TI seja testada e monitorada proativamente. A segurança de TI deve ser revalidada periodicamente para garantir que o nível de segurança aprovado seja mantido. A função de monitoramento e registro de eventos *(logging)* deve possibilitar a prevenção e/ou detecção prematura de atividades anormais e incomuns que precisem ser tratadas, bem como a subsequente geração de relatórios no tempo apropriado.

DS5.6 Definição de Incidente de Segurança
Definir e comunicar claramente as características de incidentes de segurança em potencial para que possam ser tratados adequadamente pelos processos de gestão de incidentes ou gestão de problemas.

DS5.7 Proteção da Tecnologia de Segurança
Garantir que as tecnologias de segurança importantes sejam invioláveis e que as documentações de segurança não sejam reveladas desnecessariamente.

DS5.8 Gestão de Chave Criptográfica
Assegurar que sejam estabelecidos políticas e procedimentos de geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada.

DS5.9 Prevenção, Detecção e Correção de Software Malicioso
Assegurar que medidas preventivas, de detecção e corretivas sejam estabelecidas corporativamente, em especial correções de segurança *(patches)* e controles de vírus, para proteger os sistemas de informação e tecnologias contra malwares (vírus, *worms, spyware, spam.)*.

DS5.10 Segurança de Rede
Garantir que técnicas de segurança e procedimentos de gestão relacionados (como *firewalls*, aplicativos de segurança, segmentação de rede e detecção de intrusão) sejam utilizados para autorizar o acesso e controlar os fluxos de informação entre redes.

DS5.11 Comunicação de Dados Confidenciais
Assegurar que as transações de comunicação de dados confidenciais ocorram somente por um caminho confiável ou controlado de modo a fornecer autenticação de conteúdo, comprovante de envio, comprovante de recebimento e não-rejeição de origem.

Diretrizes de Gerenciamento

DS5 Garantir a Segurança dos Sistemas

Origem	Entrada
PO2	Arquitetura da informação; Classificações atribuídas a dados;
PO3	Padrões tecnológicos;
PO9	Avaliação de riscos;
AI2	Especificações de controles para segurança de aplicações;
DS1	OLAs

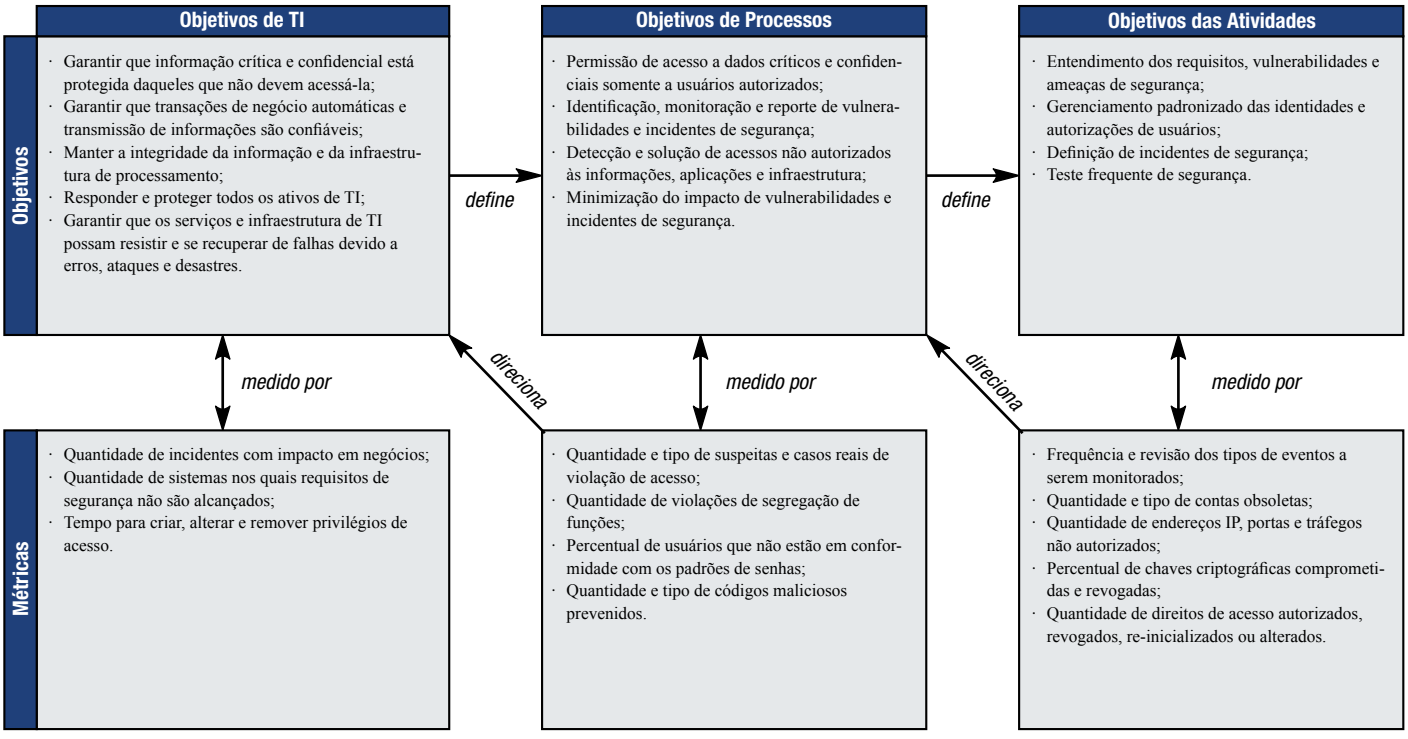
Saída	Destino
Definição de Incidente de Segurança;	DS8
Requisitos específicos de treinamento em conscientização de segurança;	DS7
Relatórios de desempenho de processos;	ME1
Mudanças de segurança necessárias;	AI6
Vulnerabilidades e ameaças de segurança;	PO9
Políticas e Plano de Segurança de TI	DS11

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir e manter um plano de segurança de TI;	I	C	C	A	C	C	C	C	I	I	R
Definir, implementar e operar um processo de gestão de identidades (contas);			I	A	C	R	R	I			C
Monitorar incidentes de segurança reais e potenciais;				A	I	R	C	C			R
Revisar e validar periodicamente os privilégios e direitos de acesso de usuários;				I	A	C					R
Implementar e manter procedimentos para manter e proteger chaves criptográficas;				A		R			I		C
Implementar e manter controles técnicos e procedimentais para proteger a comunicação de dados através das redes;				A	C	C	R	R			C
Conduzir frequentemente análise de vulnerabilidades		I		A	I	C	C	C			R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS5 Garantir a Segurança dos Sistemas

O gerenciamento do processo de ***"Garantir a segurança dos sistemas"*** que satisfaça ao requisito do negócio para a TI de ***"manter a integridade da infraestrutura de informação e de processamento e minimizar o impacto de vulnerabilidades e incidentes de segurança"*** é:

0 Inexistente quando

A organização não reconhece a necessidade de segurança da informação. Responsabilidades não estão estabelecidas para garantir a segurança. Medidas de apoio à gestão de segurança de TI não estão implementas. Não há relatórios de segurança de TI, e não existe nenhum processo de resposta às falhas de segurança de TI. Não há um processo reconhecível de administração de segurança.

1 Inicial /*Ad hoc* quando

A organização reconhece a necessidade de segurança de TI. A consciência da necessidade de segurança depende principalmente das pessoas. A segurança de TI é tratada de forma reativa e não é mensurada. As falhas de segurança de TI detectadas geram acusações internas, pois a atribuição de responsabilidades é obscura. As respostas às falhas de segurança de TI são imprevisíveis.

2 Repetível, porém Intuitivo quando

As responsabilidades pela segurança de TI são atribuídas por um coordenador de segurança de TI, apesar da autoridade do gestor do coordenador ser limitada. A consciência da necessidade de segurança é fragmentada e limitada. Embora informações relevantes de segurança sejam produzidas pelos sistemas, elas não são analisadas. Serviços terceirizados podem não tratar das necessidades específicas de segurança da organização. Políticas de segurança estão sendo desenvolvidas, mas as habilidades e ferramentas são inadequadas. Os relatórios de segurança de TI são inconsistentes, mal elaborados ou impertinentes. Treinamento em segurança está disponível, mas depende da decisão de cada funcionário. A segurança de TI é considerada principalmente como sendo de responsabilidade e domínio de TI, e a empresa não percebe a segurança da TI como parte do seu domínio.

3 Processo Definido quando

A conscientização de segurança existe e é promovida pela Direção. Os procedimentos de segurança de TI são definidos e alinhados com a política de segurança de TI. As responsabilidades pela segurança de TI são atribuídas e entendidas, mas não são consistentemente impostas. Um plano de segurança de TI e soluções de segurança são resultado de análises de risco. O relatório de segurança não tem foco em negócio. Testes de segurança são realizados de forma *ad hoc* (por exemplo, teste de intrusão). O treinamento em segurança é disponibilizado para a TI e para o Negócio, mas é agendado e controlado informalmente.

4 Gerenciado e Mensurável quando

AAs responsabilidades pela segurança de TI são claramente atribuídas, gerenciadas e impostas. Avaliações críticas de riscos e impactos de segurança são executadas consistentemente. As práticas e políticas de segurança são complementadas com perfis básicos específicos. É mandatória a submissão aos métodos de promoção de conscientização da segurança. A identificação, a autenticação e a autorização do usuário são padronizadas. Certificações de segurança são buscadas por equipes responsáveis pela auditoria e o gerenciamento de segurança. Os testes de segurança são realizados utilizando padrões e processos formalizados visando melhorar os níveis de segurança. Os processos de segurança de TI são coordenados com a área corporativa de segurança da informação. Os relatórios de segurança estão alinhados aos objetivos de negócio. O treinamento em segurança de TI é ministrado às equipes de negócios e de TI. O treinamento em segurança da TI é planejado e gerenciado para atender às necessidades do negócio e aos perfis de riscos de segurança definidos. Os objetivos e métricas da gestão de segurança foram definidos, porém ainda não são mensurados.

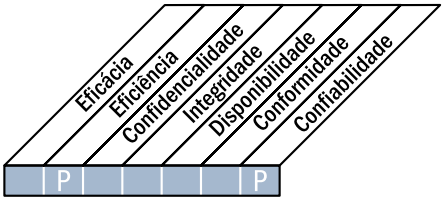
5 Otimizado quando

A segurança de TI é de responsabilidade conjunta das Direções de Negócio e de TI e está integrada aos objetivos corporativos de segurança. Os requisitos de segurança de TI são claramente definidos, otimizados e incluídos em um plano de segurança aprovado. Os usuários e clientes são gradativamente responsáveis pela definição dos requisitos de segurança, e as funções de segurança são integradas às aplicações no estágio de planejamento. Os incidentes de segurança são prontamente tratados com procedimentos formalizados de resposta a incidentes apoiados por ferramentas automatizadas. São realizadas avaliações de segurança críticas periódicas para verificar a efetividade da implementação do plano de segurança. As informações sobre ameaças e vulnerabilidades são sistematicamente coletadas e analisadas. Os controles adequados para minimizar riscos são prontamente comunicados e implementados. Testes de segurança, análise de causa-raiz dos incidentes de segurança e identificação proativa de riscos são utilizados em processos de melhoria contínua. Os processos de segurança e tecnologia estão integrados em toda organização. Métricas de gerenciamento de segurança são coletadas e comunicadas. A Direção utiliza essas métricas para ajustar o plano de segurança como parte do processo de melhoria contínua.

Descrição do Processo

DS6 Identificar e Alocar Custos

A necessidade de um sistema justo e equitativo de alocação de custo de TI para o negócio requer avaliação precisa dos custos de TI e acordo com os usuários do negócio sobre uma alocação razoável. Este processo contempla a construção e a operação de um sistema para capturar, alocar e reportar os custos de TI aos usuários dos serviços. Um sistema de alocação justo permite à empresa tomar decisões mais embasadas sobre o uso dos serviços.



Controle sobre o seguinte processo de TI:

Identificar e alocar custos

que satisfaça aos seguintes requisitos do negócio para a TI:

prover transparência e entendimento dos custos de TI e melhoria da relação custo-benefício através do uso bem informado dos serviços de TI

com foco em:

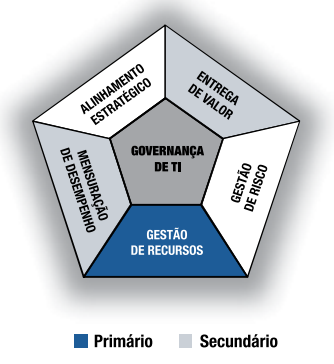
coleta completa e precisa dos custos de TI, um sistema de alocação justo aceito pelos usuários do negócio e um sistema de reporte oportuno do uso da TI e dos custos alocados

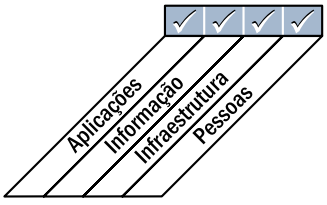
é alcançado por:

- Alinhamento dos valores cobrados à qualidade e quantidade dos serviços fornecidos
- Construção e concordância de um modelo de custo completo
- Implementação de um sistema de cobrança de valores conforme a política acordada com antecedência

e medido por:

- Percentual de faturas de serviços de TI aceitas/pagas pelo gestor de negócio
- Percentual de variação entre orçamentos, previsões e custos reais
- Percentual dos custos gerais de TI que são alocados de acordo com os modelos de custo combinados





Objetivos de Controle Detalhados

DS6 Identificar e Alocar Custos

DS6.1 Definição de Serviços
Identificar todos os custos de TI e associá-los aos serviços de TI, sustentando um modelo transparente de custeio. Os serviços de TI devem ser associados aos processos de negócio de forma que permita identificar os níveis de faturamento de serviço correspondentes.

DS6.2 Contabilidade de TI
Coletar e alocar os custos vigentes de acordo com o modelo de custo definido. Variações entre as previsões e os custos reais devem ser analisadas e relatadas em conformidade com os sistemas de medição financeira corporativos.

DS6.3 Modelagem de Custo e Cobrança
Com base na definição de serviço, definir um modelo de custo que considere os custos diretos, indiretos e gerais dos serviços e suporte o cálculo das taxas de cobrança por serviço. O modelo de custo deve estar alinhado aos procedimentos de contabilidade de custo corporativos. O modelo de custo de TI deve assegurar que a cobrança pelos serviços seja identificável, mensurável e previsível pelos usuários para incentivar o uso adequado dos recursos. O gestor de negócios deve ser capaz de verificar o uso real e a cobrança dos serviços.

DS6.4 Manutenção do Modelo de Custo
Realizar periodicamente análise crítica e comparação com referências do mercado *(benchmarking)* da adequação do modelo de custo/cobrança visando manter a relevância e a adequação aos negócios e às atividades de TI envolvidas.

Diretrizes de Gerenciamento

DS6 Identificar e Alocar Custos

Origem	Entrada
PO4	Proprietários formais dos sistemas;
PO5	Relatórios de custo/benefício; Orçamentos de TI;
PO10	Planejamento detalhado de projetos;
DS1	SLAs e OLAs

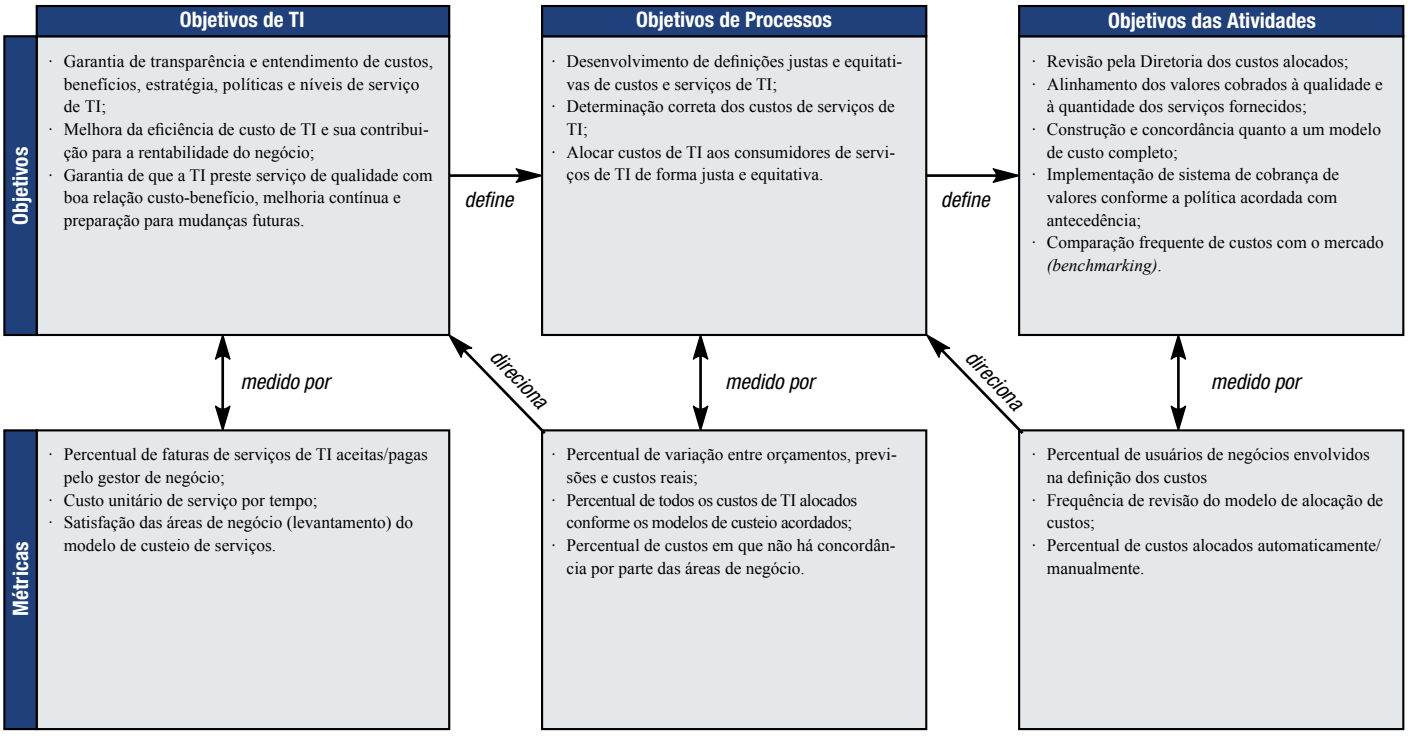
Saída	Destino
Aspectos financeiros de TI;	PO5
Relatórios de desempenho de processos	ME1

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Mapear a infraestrutura de TI em serviços fornecidos / processos de negócio suportados;		C	C	A	C	C	C	C	R	C	
Identificar todos custos de TI (pessoas, tecnologia, etc) e mapeá-los aos serviços de TI de forma unitária;		C		A		C	C	C	R	C	
Estabelecer e manter processos de contabilidade e controle de custos de TI;		C	C	A	C	C	C	C	R	C	
Estabelecer e manter políticas e procedimentos de custeio		C	C	A	C	C	C	C	R	C	

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS6 Identificar e Alocar Custos

O gerenciamento do processo de ***"identificar e alocar custos"*** que satisfaça ao requisito do negócio para a TI de ***"prover transparência e entendimento dos custos de TI e melhoria da relação custo-benefício através do uso bem informado dos serviços de TI"*** é:

0 Inexistente quando

Há uma ausência completa de qualquer processo reconhecível para identificação e alocação de custos dos serviços de informação fornecidos. A organização nem mesmo tem reconhecido que há uma questão a ser tratada no que diz respeito à contabilização dos custos e não há posicionamento comunicado a cerca do assunto.

1 Inicial/ *Ad hoc* quando

Há um entendimento geral de todos os custos dos serviços de informação, porém não existe detalhamento de custos por usuário, cliente, departamento, grupo de usuários, projeto ou serviço entregue. Não existe absolutamente nenhum tipo de monitoramento de custo, apenas relatórios de custos consolidados. Os custos de TI são alocados como custo operacional geral. Não são informados custos ou benefícios às áreas de negócio pelos serviços prestados.

2 Repetível, porém Intuitivo quando

Há uma consciência geral da necessidade de identificar e alocar custos. A alocação de custo é fundamentada em presunções informais ou rudimentares (por exemplo: custos de *hardware*), e não existe absolutamente nenhuma conexão com o que realmente levou aos valores. Os processos de alocação de custos são reproduzíveis. Não há treinamento ou comunicação formal de procedimentos padronizados de identificação e alocação de custos. A responsabilidade pela coleta ou alocação dos custos não está atribuída.

3 Processo Definido quando

Existe um modelo de custo de serviços de informação definido e documentado. Existe um processo definido para relacionar os custos de TI aos serviços prestados aos usuários. Há um nível adequado de ciência dos custos atribuíveis aos serviços de informação. A empresa recebe informações rudimentares sobre custos.

4 Gerenciado e Mensurável quando

A reponsabilidade pela gestão de custos dos serviços de informação está definida, é totalmente entendida em todos os níveis corporativos e apoiada por treinamento formal. Os custos diretos e indiretos são identificados e relatados de forma automatizada e oportuna aos gestores, usuários e proprietários do processo de negócio. Existem monitoramento e avaliação de custo de modo geral e medidas são tomadas quando detectados desvios de custo. O relatório de custo dos serviços de informação é associado aos objetivos de negócio e acordos de nível de serviço e monitorado pelos proprietários dos processos de negócio. Existe uma análise crítica financeira sobre a razoabilidade do processo de alocação de custo. Há um sistema de contabilização de custo automatizado, porém é focalizado na função de serviços de informação mais do que nos processos de negócio. Os objetivos e métricas de custo foram acordados, porém são medidos de forma inconsistente.

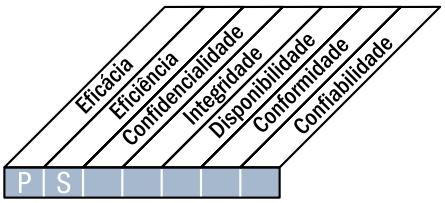
5 Otimizado quando

Os custos dos serviços prestados são identificados, coletados, consolidados e relatados aos gestores, usuários e proprietários de processos. Os custos são identificados e repassados aos usuários de serviços prestados com base na utilização. Os detalhes de custos sustentam os acordos de nível de serviço. Monitoramento e avaliação dos custos de serviços são utilizados para aperfeiçoar o custo dos recursos de TI. Cálculos de custos obtidos são utilizados para verificar a realização do benefício e utilizados no processo de previsão orçamentária da organização. O relatório de custo dos serviços de informação provê alertas de mudança nos requisitos de negócio através de sistemas de relatório inteligentes. Um modelo de custo variável é utilizado, derivado dos volumes processados por cada serviço prestado. O gerenciamento de custo tem sido refinado em um nível de prática industrial, embasado no resultado de melhoria contínua e comparação com outras organizações. A otimização dos custos é um processo contínuo. O gestor revê os objetivos e métricas como parte de um processo de melhoria contínua na reformulação dos sistemas de medição de custo.

Descrição do Processo

DS7 Educar e Treinar os Usuários

A educação efetiva de todos os usuários de sistemas de TI, inclusive daqueles dentro da própria TI, requer a identificação das necessidades de treinamento de cada grupo de usuário. Como complemento à identificação dessas necessidades, esse processo compreende a definição e a execução de uma estratégia eficaz de treinamento e medição dos resultados. Um programa de treinamento eficaz aumenta o uso efetivo da tecnologia através da redução dos erros de usuário, aumento da produtividade e aumento da conformidade com os controles principais (como as medidas de segurança do usuário).



Controle sobre o seguinte processo de TI:

Educar e treinar os usuários

que satisfaça aos seguintes requisitos do negócio para a TI:

uso efetivo e eficiente das aplicações e soluções tecnológicas, e conformidade do usuário com as políticas e os procedimentos

com foco em:

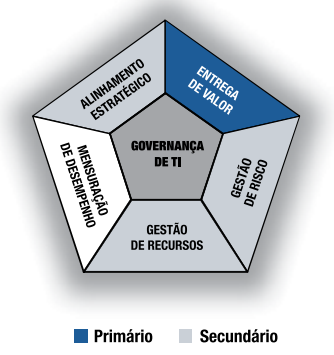
entender claramente as necessidades do usuário em termos de treinamento em TI e executar uma estratégia eficaz de treinamento e medição dos resultados

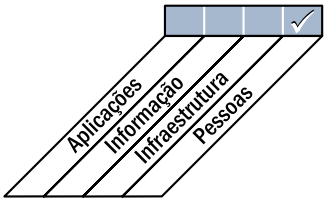
é alcançado por:

- Estabelecimento de uma grade de treinamento
- Organização de treinamento
- Disponibilização de treinamento
- Monitoramento e relatório da eficácia do treinamento

e medido por:

- Quantidade de chamadas ao centro de atendimento devido à falta de treinamento dos usuários
- Percentual de partes interessadas satisfeitas com o treinamento recebido
- Tempo entre a identificação da necessidade de treinamento e a respectiva realização





Objetivos de Controle Detalhados

DS7 Educar e Treinar os Usuários

DS7.1 Identificação das Necessidades de Ensino e Treinamento
Estabelecer e atualizar regularmente um currículo para cada grupo-alvo de empregados, considerando:
· As estratégias e necessidades atuais e futuras do negócio
· Valor da informação como um bem
· Os valores corporativos (valores éticos, cultura de segurança e controle etc.)
· A implementação de nova infraestrutura de TI e *softwares* (pacotes e aplicações)
· As habilidades, competências, certificação e atualizações necessárias
· Os métodos de ministrar aulas (em sala de aula, via *web*), o tamanho do grupo-alvo, acessibilidade e tempo

DS7.2 Entrega de Treinamento e Ensino
Com base nas necessidades de ensino e treinamento identificadas, definir os grupos-alvo e seus membros, mecanismos adequados de ministrar os treinamentos, professores, instrutores e monitores. Indicar os instrutores e organizar as sessões de treinamento de forma oportuna. Registrar inscrições (incluindo pré-requisitos), frequência de participação e avaliações de desempenho.

DS7.3 Avaliação do Treinamento Recebido
Avaliar o conteúdo do ensino e do treinamento recebidos no que diz respeito a relevância, qualidade, efetividade, absorção e retenção do conhecimento, custo e valor. Os resultados dessa avaliação devem servir de base para a definição dos futuros currículos e sessões de treinamento.

Diretrizes de Gerenciamento

DS7 Educar e Treinar os Usuários

Origem	Entrada
PO7	Habilidades e competências de usuários, incluindo treinamento individual; Requisitos de treinamentos específicos;
AI4	Materiais de treinamento; Requisitos de transferência e conhecimento para implementação de soluções;
DS1	OLAs;
DS5	Requisitos específicos de treinamento em conscientização de segurança;
DS8	Relatórios sobre satisfação de usuários

Saída	Destino
Relatórios de desempenho de processos;	ME1
Atualizações necessárias de documentações	AI4

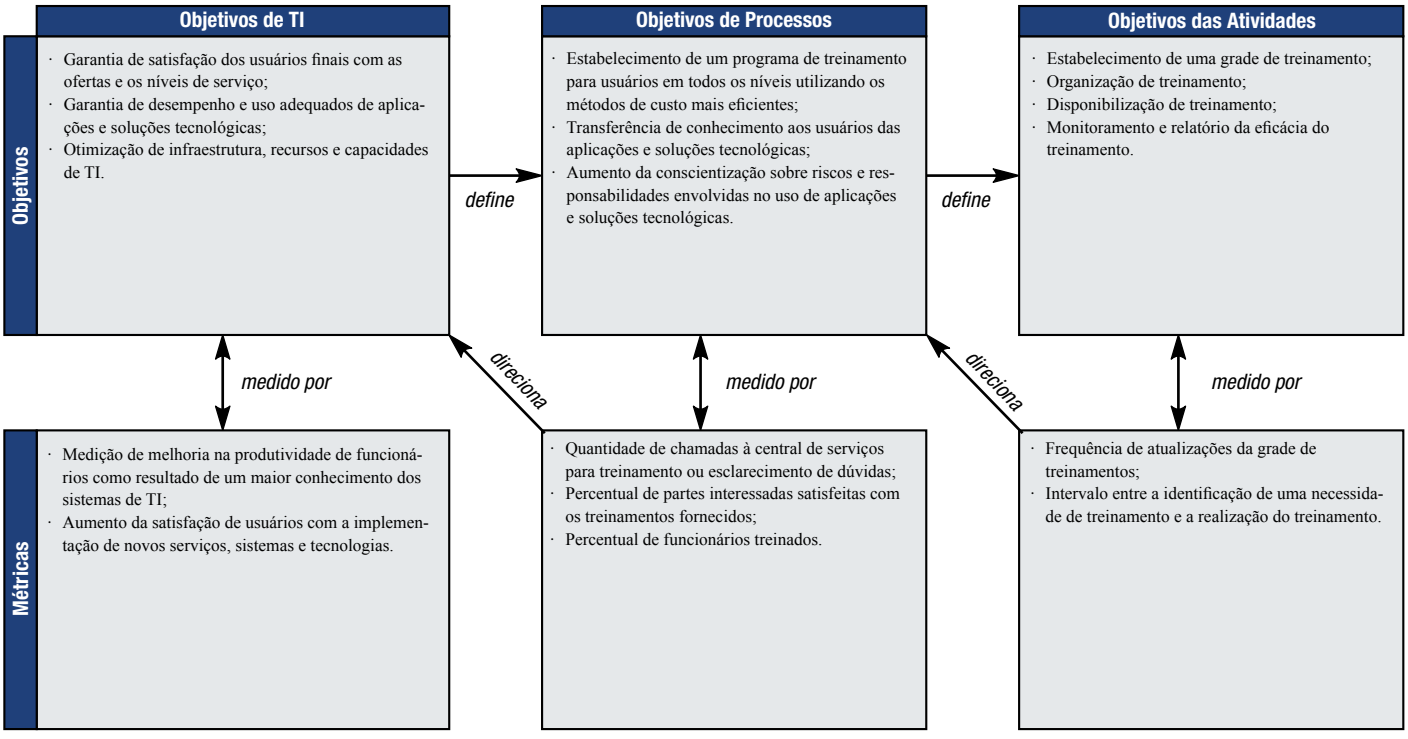
Tabela RACI

Funções

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Departamento de Treinamento
Identificar e caracterizar as necessidades de treinamento de usuários;			C	A	R	C	C	C	C	C	C	R
Criar um programa de treinamento;			C	A	R	C	I	C	C	C	I	R
Conduzir atividades de conscientização, educação e treinamento;			I	A	C	C	I	C	C	C	I	R
Realizar avaliação dos treinamentos;			I	A	R	C	I	C	C	C	I	R
Identificar e avaliar os melhores métodos e ferramentas de treinamento			I	A/R	R	C	C	C	C	C	C	R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS7 Educar e Treinar os Usuários

O gerenciamento do processo de ***"educar e treinar os usuários"*** que satisfaça ao requisito do negócio para a TI de ***"uso efetivo e eficiente das aplicações e soluções tecnológicas, e conformidade do usuário com as políticas e os procedimentos"*** é:

0 Inexistente quando
Há uma ausência completa de qualquer programa de ensino e treinamento. A organização nem mesmo reconhece que há uma questão a ser tratada com relação ao treinamento, e não há sequer posicionamento comunicado sobre essa questão.

1 Inicial/ *Ad hoc* quando
Há evidência de que a organização reconhece a necessidade de um programa de ensino e treinamento, porém não existem processos padronizados. Na ausência de um programa organizado, os empregados têm identificado e participado de cursos de treinamento por conta própria. Alguns dos cursos de treinamento têm abordado questões como conduta ética, conscientização da segurança do sistema e técnicas de segurança. A abordagem corporativa não é coesa, e são feitas apenas comunicações esporádicas e inconsistentes sobre as questões de ensino e treinamento.

2 Repetível, porém Intuitivo quando
Há consciência na organização da necessidade de um programa de ensino e treinamento e de processos associados. O treinamento está começando a ser identificado nos planos de desempenho individual dos funcionários. Os processos se desenvolveram ao ponto de treinamento e aulas informais serem ministrados por instrutores diferentes e abordar as mesmas matérias de maneiras diferentes. Algumas aulas tratam questões de conduta ética, conscientização e práticas de segurança de sistemas. Há extrema dependência do conhecimento de pessoas. Contudo, existe comunicação consistente nas questões relevantes e na necessidade de tratá-las.

3 Processo Definido quando
O programa de ensino e treinamento foi institucionalizado e comunicado, os gerentes e funcionários identificam e documentam as necessidades de treinamento. Os processos de ensino e treinamento são padronizados e documentados. Os orçamentos, recursos, instalações e instrutores são bem coordenados para suportar o programa de ensino e treinamento. São ministradas aulas formais aos funcionários sobre conduta ética, conscientização e práticas de segurança de sistema. A maioria dos processos de ensino e treinamento é monitorada, porém nem todas as divergências são detectadas pelo gerenciamento. Análises dos problemas de ensino e treinamento são feitas apenas ocasionalmente.

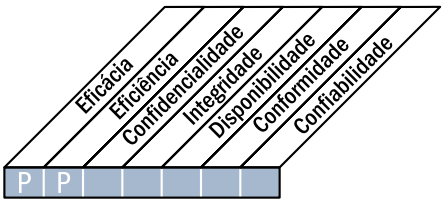
4 Gerenciado e Mensurável quando
Há um programa de ensino e treinamento amplo que permite resultados mensuráveis. As responsabilidades são claras, e a propriedade do processo é definida. O ensino e treinamento é um componente dos planos de carreira dos funcionários. O gestor apoia e participa de treinamentos e sessões educacionais. Todos os funcionários recebem treinamento em conduta ética e conscientização de segurança. Todos os funcionários recebem treinamento em práticas de segurança no nível adequado para evitar prejuízos causados por falhas que afetam a disponibilidade, a confidencialidade e a integridade. O gestor monitora a conformidade com diretrizes, normas, regras, metas corporativas através de análises criticas e constantes atualizações do programa e dos processos de ensino e treinamento. Os processos estão sujeitos a melhorias, e são aplicadas as melhores práticas internas.

5 Otimizado quando
Ensino e treinamento resultam na melhoria no desempenho individual. O ensino e o treinamento são fatores determinantes no plano de carreira do funcionário. Orçamentos, recursos, facilidades e instrutores são suficientemente disponibilizados para os programas de ensino e treinamento. Os processos são refinados e estão sob constante evolução, tendo como vantagem as melhores práticas externas e a modelagem de maturidade comparada com outras organizações. Todos os problemas e divergências são analisados em suas causas-raíz e ações eficientes são convenientemente executadas. Há uma atitude positiva a respeito dos princípios de conduta ética e segurança de sistema. TI é utilizada de forma otimizada, integrada e extensiva para automatizar e fornecer ferramentas ao programa de ensino e treinamento. São realizados treinamentos especializados externos, e análises comparativas com o mercado *(benchmarks)* são utilizadas como orientação.

Descrição do Processo

DS8 Gerenciar a Central de Serviço e os Incidentes

A resposta efetiva e em tempo adequado a dúvidas e problemas dos usuários de TI requer uma central de serviço *(service desk)* e processos de gerenciamento de incidentes bem projetados e implementados. Esse processo inclui a implementação de uma central de serviços capacitada para o tratamento de incidentes, incluindo registro, encaminhamento, análise de tendências, análise de causa-raiz e resolução. Os benefícios ao negócio incluem aumento de produtividade por meio de resolução rápida dos chamados dos usuários. Complementarmente, as áreas de negócio podem tratar as causas-raiz (como treinamento deficiente de usuário), através de relatórios efetivos.



Controle sobre o seguinte processo de TI:

Gerenciar a central de serviço e os incidentes

que satisfaça aos seguintes requisitos do negócio para a TI:

permitir o uso eficaz dos sistemas de TI através de análise e resolução de consultas, solicitações e incidentes

com foco em:

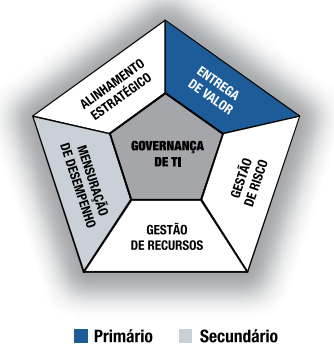
prover uma central de serviços profissional com respostas rápidas, procedimentos claros de escalonamento, análise de tendências e resolução

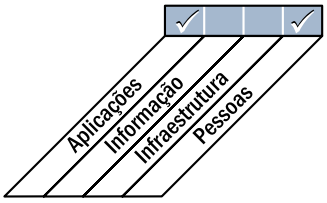
é alcançado por:

· Instalação e operação de uma central de serviços
· Monitoração e registro das tendências
· Definição clara de critérios e procedimentos de escalonamento

e medido por:

· Satisfação do usuário com o primeiro nível de atendimento
· Percentual de incidentes resolvidos no tempo estipulado/aceitável
· Índice de desistência dos chamados





Objetivos de Controle Detalhados

DS8 Gerenciar a Central de Serviço e os Incidentes

DS8 Central de Serviço
Estabelecer uma central de serviço, que é a interface entre o usuário e a TI, para registrar, comunicar, despachar e analisar todos os chamados, incidentes reportados, solicitações de serviços e demanda de informações. Devem existir procedimentos de monitoramento e encaminhamento com base em níveis de serviço acordados relativos ao SLA adequado que permita a classificação e a priorização de qualquer dúvida reportada como incidente, solicitação de serviço ou solicitação de informação. Medir a satisfação dos usuários finais com a qualidade da central de serviço e os serviços de TI.

DS8.2 Registro dos Chamados dos Clientes
Estabelecer uma função e um sistema que permitam o registro e o rastreamento de ligações, incidentes, solicitações de serviços e necessidade de informações. Deve trabalhar de perto com os processos de gerenciamento de incidentes, problemas, mudanças, capacidade e disponibilidade. Os incidentes devem ser classificados de acordo com as prioridades de negócio e serviço e direcionados à equipe adequada de gerenciamento de problemas. Os clientes devem ser mantidos informados sobre o status de seus chamados.

DS8.3 Escalonamento de Incidentes
Estabelecer os procedimentos da central de serviço para que os incidentes que não podem ser resolvidos imediatamente sejam adequadamente encaminhados, conforme os limites definidos no SLA, e soluções temporárias sejam implementadas, se aplicável. Assegurar que a propriedade e o monitoramento do ciclo de vida do incidente permaneçam com a central de serviço, independentemente do grupo de TI que esteja trabalhando nas atividades de resolução.

DS8.4 Encerramento de Incidente
Estabelecer procedimentos para o monitoramento periódico do encerramento de chamados de clientes. Quando o incidente foi resolvido, assegurar que a central de serviço registre os passos adotados para sua resolução e confirmar se as ações adotadas foram aceitas pelo cliente. Também registrar e relatar incidentes não solucionados (erros já conhecidos e alternativas existentes) para prover informações visando o adequado gerenciamento de problemas.

DS8.5 Relatórios e Análises de Tendências
Gerar relatórios de atividades da central de serviço, permitindo aos gestores medir o desempenho e o tempo de resposta dos serviços e identificar tendências ou problemas recorrentes, para que o serviço possa ser melhorado sempre.

Diretrizes de Gerenciamento

DS8 Gerenciar a Central de Serviço e os Incidentes

Origem	Entrada
AI4	Manuais de usuário, operação, suporte, técnico e administração;
AI6	Autorização de mudanças;
AI7	Itens de configuração liberados;
DS1	SLAs e OLAs;
DS4	Níveis de incidentes/desastres;
DS5	Definição de Incidente de Segurança;
DS9	Detalhes de Ativos / Configuração de TI;
DS10	Problemas e erros conhecidos e soluções alternativas;
DS13	Chamados de incidentes

Saída	Destino						
Solicitações de serviço/solicitações de mudança;	AI6						
Relatórios de incidentes;	DS10						
Relatórios de desempenho de processos;	ME1						
Relatórios sobre satisfação de usuários	DS7	ME1					

Tabela RACI

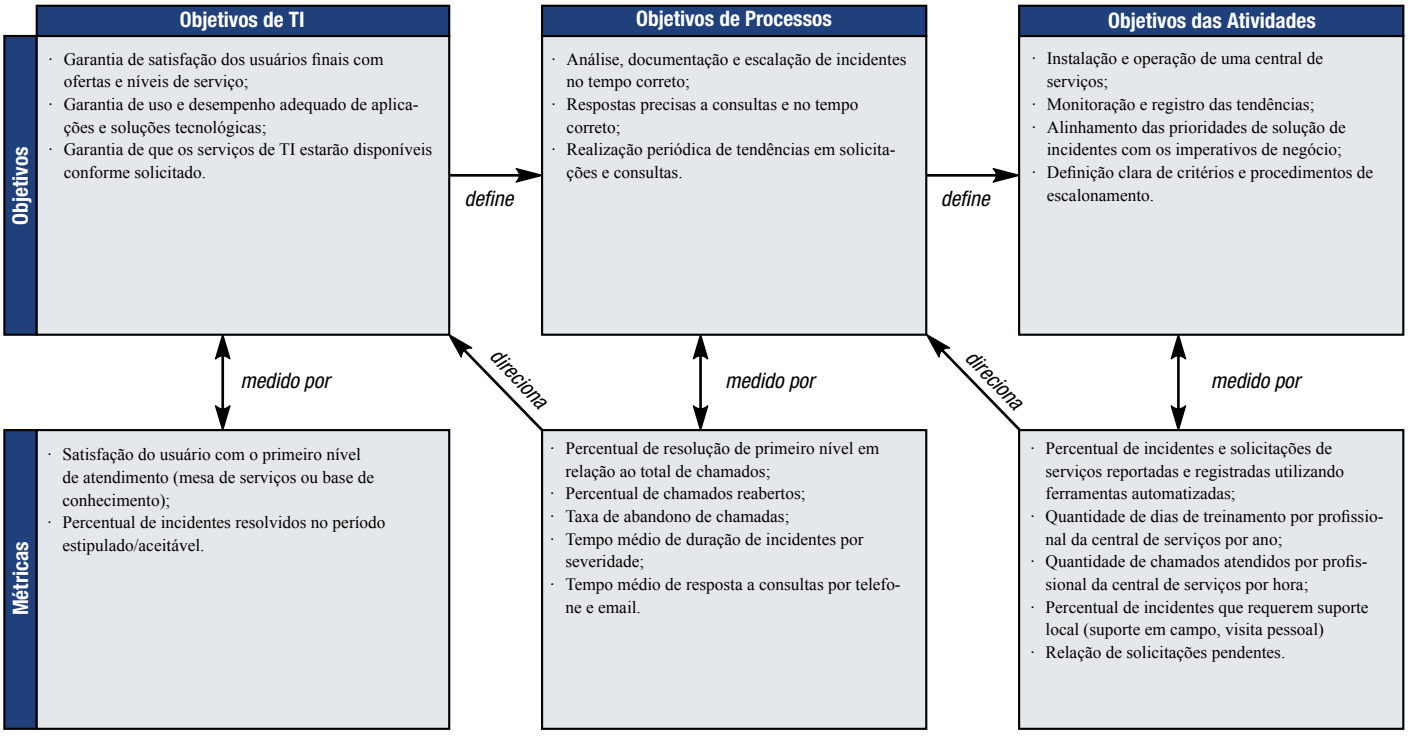
Funções

Atividades

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Gerência de Incidentes / Service Desk
Criar processos de classificação (severidade e impacto) e escalação (funcional e hierárquica);				C	C	C	C	C	C		C	A/R
Detectar e registrar incidentes, solicitações de serviço e solicitações de informações;												
Classificar, investigar e diagnosticar consultas;				I		C	C	C			I	
Resolver, recuperar e fechar incidentes;					I	R	R	R			C	
Informar usuários (por exemplo atualizações de status);				I	I							
Produzir relatórios gerenciais	I			I	I	I			I		I	

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS8 Gerenciar a Central de Serviço e os Incidentes

O gerenciamento do processo de ***"gerenciar a central de serviço e os incidentes"*** que satisfaça ao requisito do negócio para a TI de ***"permitir o uso eficaz dos sistemas de TI através da análise e resolução de consultas, solicitações e incidentes"*** é:

0 Inexistente quando
Não há suporte para resolver temas e questões de usuários. Há uma completa falta de processo de gerenciamento de incidente. A organização não reconhece que há uma questão a ser tratada.

1 Inicial/ *Ad hoc* quando
A gerência reconhece a necessidade de um processo sustentado por ferramentas e pessoas para responder aos chamados de usuários e gerenciar a resolução de incidentes. Entretanto, não existe um processo padronizado e só é oferecido suporte reativo. A gerência não monitora chamados, incidentes ou tendências. Não existe um processo de encaminhamento que assegure que o problema será resolvido.

2 Repetível, porém Intuitivo quando
Há uma consciência organizacional da necessidade de uma central de serviços e de um processo de gerenciamento de incidentes. Assistência está disponível de maneira informal por meio de uma rede de indivíduos que têm conhecimento. Essas pessoas têm algumas ferramentas comuns para auxiliar na resolução de incidentes. Não há treinamento formal, não há procedimentos padrão e comunicados e as responsabilidades ficam a cargo de cada pessoa.

3 Processo Definido quando
A necessidade de uma central de serviço e um processo de gerenciamento de incidente é reconhecida e aceita. Os procedimentos foram padronizados e documentados e ocorrem treinamentos informais. Entretanto, fica a cargo das pessoas obter treinamento e seguir padrões. Consolidação de perguntas frequentes (FAQs) e diretrizes de usuários são desenvolvidas, mas as pessoas devem procurá-las e podem não segui-las. Chamados e incidentes são rastreados manualmente e monitorados individualmente, porém não existe um sistema de reporte formal. A resposta em tempo adequado aos chamados e incidentes não é medida e os incidentes podem continuar sem solução. Os usuários foram claramente comunicados sobre onde e como registrar os problemas e incidentes.

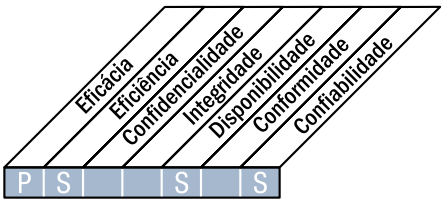
4 Gerenciado e Mensurável quando
Há um completo entendimento dos benefícios do processo de gerenciamento de incidente em todos os níveis da organização e a função da central de serviço foi estabelecida nas unidades organizacionais adequadas. As ferramentas e técnicas são automatizadas com uma base de conhecimento centralizado. Os profissionais da central de serviços interagem muito proximamente aos profissionais de gerenciamento de problemas. As responsabilidades são claras e a efetividade é monitorada. Os procedimentos para comunicação, escalonamento e resolução de incidentes são estabelecidos e comunicados. O pessoal da central de serviço é treinado e os processos são melhorados através do uso de software específico. A gerência desenvolve métricas para o desempenho da central de serviço.

5 Otimizado quando
A central de serviço e o processo de gerenciamento de incidente são estabelecidos e bem organizados, com serviço voltado ao cliente por ter conhecimento, ter foco no cliente e ser útil. Métricas são sistematicamente medidas e reportadas. FAQs abrangentes e completas são parte integrante da base de conhecimento. Há ferramentas que permitem aos usuários fazer o diagnóstico e aresolução dos incidentes. Os avisos são consistentes, e os incidentes são resolvidos rapidamente dentro de um processo de encaminhamento estruturado. A gerência utiliza ferramenta integrada para as estatísticas de desempenho do processo de gerenciamento de incidentes e da central de serviço. Os processos têm sido refinados no nível das melhores práticas da indústria, com base nos resultados de análises dos indicadores de performance, melhorias contínuas e comparação *(benchmarking)* com outras organizações.

Descrição do Processo

DS9 Gerenciar a Configuração

Assegurar a integridade das configurações de *hardware* e *software* requer o estabelecimento e a manutenção de um repositório de configuração preciso e completo. Esse processo inclui a coleta inicial das informações de configuração, o estabelecimento de um perfil básico, a verificação e a auditoria das informações de configuração e a atualização do repositório de configuração conforme necessário.Um gerenciamento de configuração eficaz facilita uma maior disponibilidade do sistema, minimiza as questões de produção e soluciona problemas com mais rapidez.



Controle sobre o seguinte processo de TI:

Gerenciar a configuração

que satisfaça aos seguintes requisitos do negócio para a TI:

otimizar a infraestrutura, os recursos e as capacidades de TI e responder pelos ativos de TI

com foco em:

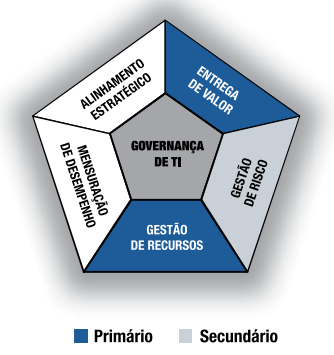
estabelecer e manter um repositório preciso e completo de atributos e perfis mínimos de configuração de ativos e comparar com a configuração atual dos ativos

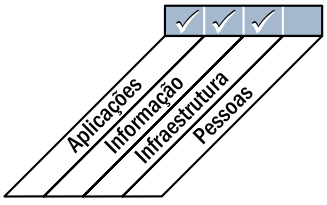
é alcançado por:

- Estabelecimento de um repositório central de todos os itens de configuração
- Identificação e manutenção dos itens de configuração
- Revisão da integridade dos dados de configuração

e medido por:

- Quantidade de problemas de conformidade de negócio causados pela configuração imprópria dos recursos
- Quantidade de desvios identificados entre o repositório de configuração e as configurações reais dos ativos
- Percentual de licenças adquiridas e não contabilizadas no repositório





Objetivos de Controle Detalhados

DS9 Gerenciar a Configuração

DS9.1 Repositório de Configuração e Perfis Básicos
Estabelecer uma ferramenta de suporte e um repositório central para conter todas as informações relevantes sobre os itens de configuração. Monitorar e registrar todos os bens e as mudanças ocorridas neles. Manter um perfil básico de itens de configuração de todo sistema e serviço como um ponto de verificação seguro para eventual retorno após as mudanças.

DS9.2 Identificação e Manutenção dos Itens de Configuração
Implantar procedimentos de configuração para suportar a Direção e registrar todas as alterações no repositório de configurações. Integrar esses procedimentos com gerenciamento de mudanças, gerenciamento de incidentes e gerenciamento de problemas.

DS9.3 Revisão da Integridade de Configuração
Periodicamente revisar os dados de configuração para verificar e confirmar a integridade da configuração atual e histórica. Realizar análise crítica periódica da política de uso de software, verificando a eventual existência de *software* pessoal, não autorizado ou excedente ao contrato de licenças vigente. Erros e desvios devem ser reportados, tratados e corrigidos.

Diretrizes de Gerenciamento

DS9 Gerenciar a Configuração

Origem	Entrada
AI4	Manuais de usuário, operação, suporte, técnico e administração;
AI7	Itens de configuração liberados;
DS4	Criticidade dos itens de configuração de TI

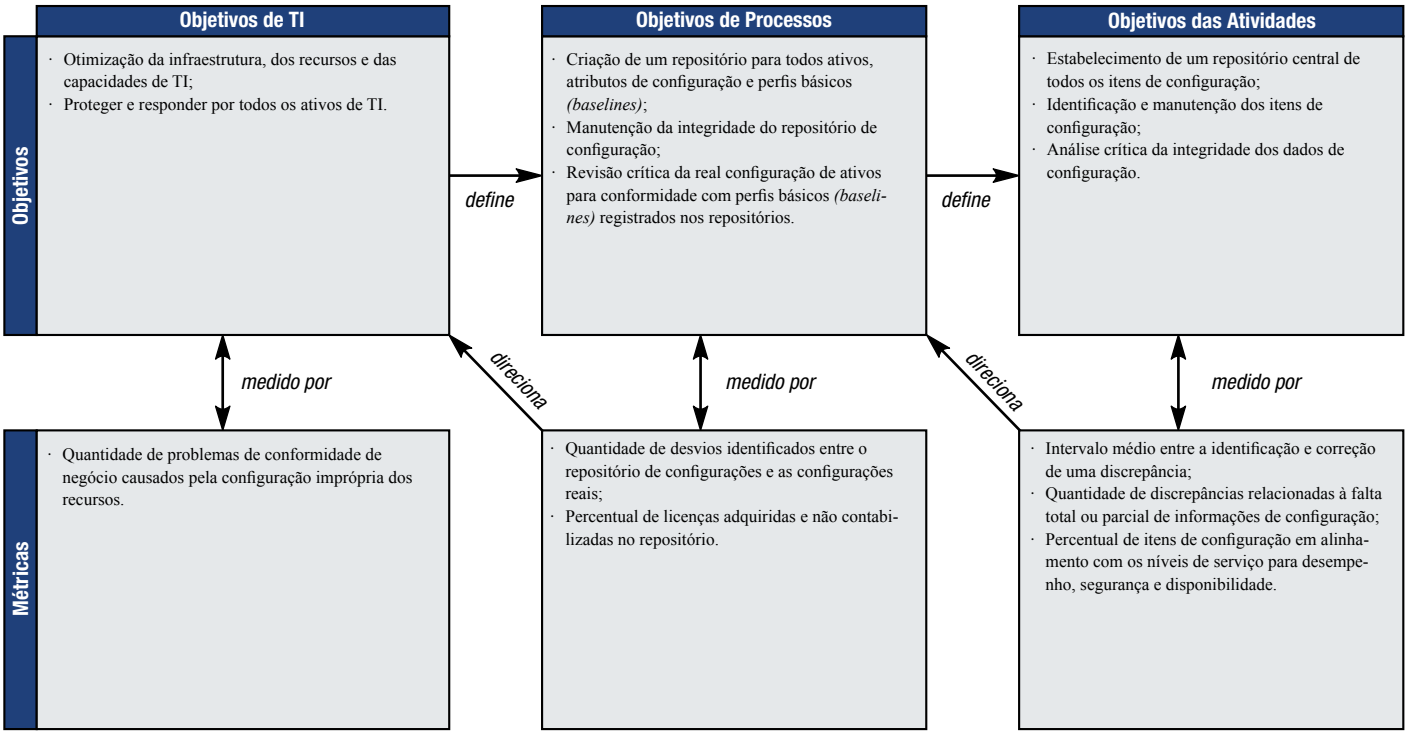
Saída	Destino						
Detalhes dos Ativos de TI e Configurações;	DS8	DS10	DS13				
Solicitações de mudança (como e onde aplicar a correção);	AI6						
Relatórios de desempenho de processos	ME1						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Gerência de Configurações
Desenvolver procedimentos de planejamento de gestão de configuração;					C	A	C	I	C		C	R
Coletar informação de configuração inicial e estabelecer perfis básicos *(baselines)*;						C	C	C			I	A/R
Verificar e auditar informação de configuração (incluindo detecção de *software* não autorizado);		I				A			I		I	A/R
Atualizar repositório de configuração						R	R	R			I	A/R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS9 Gerenciar a Configuração

O gerenciamento do processo de ***"gerenciar a configuração"*** que satisfaça ao requisito do negócio para a TI de ***"otimizar a infraestrutura, os recursos e as capacidades de TI e responder pelos ativos de TI"*** é:

0 Inexistente quando
A Diretoria não tem uma visão dos benefícios de contar com um processo implementado capaz de reportar e gerenciar a infraestrutura de TI, no que se refere a configurações de *hardware* e de *software*.

1 Inicial/ *Ad hoc* quando
A necessidade de gerenciamento de configuração é reconhecida. Atividades básicas de gerenciamento de configuração (como manutenção de inventários de *hardware* e *software*) são executadas individualmente. Nenhuma prática padronizada está definida.

2 Repetível, porém Intuitivo quando
A gerência está consciente da necessidade de controlar a configuração de TI e compreende os benefícios de ter informações de configuração precisas e completas, mas há muita confiança implicitamente no conhecimento e na habilidade do pessoal técnico. Ferramentas de gerenciamento de configuração estão sendo utilizadas até certo nível, porém diferem entre as plataformas. Nenhuma prática padronizada de trabalho foi definida. O conteúdo dos dados de configuração é limitado e não é utilizado por processos inter-relacionados, tais como gerenciamento de mudanças e gerenciamento de problemas.

3 Processo Definido quando
Os procedimentos e as práticas de trabalho foram documentados, padronizados e comunicados, mas o treinamento e a aplicação dos padrões dependem da iniciativa das pessoas. Ferramentas de gerenciamento de configuração similares estão sendo implementadas para as plataformas. Os desvios de procedimentos são dificilmente detectados, e as validações físicas são executadas inconsistentemente. Existe alguma automação para auxiliar no rastreamento de mudanças de equipamentos e *software*. Os dados de configuração estão sendo utilizados por processos inter-relacionados.

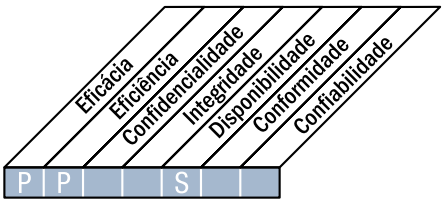
4 Gerenciado e Mensurável quando
A necessidade de gerenciar a configuração é reconhecida em todos os níveis da organização, e as boas práticas continuam a evoluir. Os padrões e procedimentos são comunicados e incorporados aos treinamentos, e os desvios são monitorados, rastreados e reportados. Ferramentas automatizadas (como tecnologias *push*) são utilizadas para impor os padrões e melhorar a estabilidade. Os sistemas de gerenciamento de configuração cobrem a maioria dos ativos de TI e permitem o gerenciamento apropriado de liberações e o controle de distribuição. Análises de exceções e verificações físicas são consistentemente aplicadas e as causas-raiz são investigadas.

5 Otimizado quando
Todos os recursos de TI são gerenciados dentro de um sistema de gerenciamento de configuração central que contém toda informação necessária sobre os componentes, seus inter-relacionamentos e eventos. Os dados de configuração são alinhados com o catálogo dos fornecedores. Há completa integração dos processos inter-relacionados, que utilizam e atualizam os dados de configuração de modo automatizado. Relatórios básicos de auditoria fornecem dados essenciais de *hardware* e *software* para reparo, serviço, garantia, atualização e avaliação técnica de cada unidade individual. São impostas regras que limitam a instalação de *software* não autorizado. A gerência prevê reparos e atualizações com base nos relatórios de análises, o que possibilita a programação de atualizações e a renovação da capacidade tecnológica. O monitoramento e o rastreamento de cada um dos ativos de TI os protegem e evitam furtos, mau uso e abusos.

DESCRIÇÃO DO PROCESSO

DS10 Gerenciar Problemas

O efetivo gerenciamento de problemas requer identificação e classificação dos problemas, análise de causas-raiz e respectiva resolução. O processo de gerenciamento de problemas também contempla a identificação de recomendações para melhoria, manutenção dos registros de problemas e revisão da situação das ações corretivas. Um processo efetivo de gerenciamento de problemas melhora os níveis de serviço, reduz os custos e aumenta a conveniência e a satisfação do cliente.



Controle sobre o seguinte processo de TI:

Gerenciar os problemas

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar a satisfação dos usuários finais com a oferta de serviços e níveis de serviço, e reduzir a entrega de serviços e soluções com problemas e re-trabalhos

com foco em:

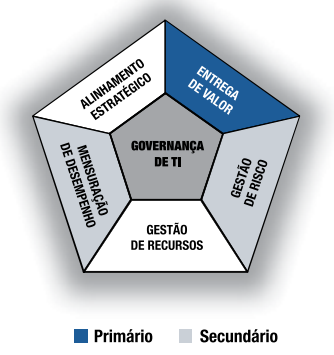
registrar, rastrear e resolver problemas operacionais; investigar a causa-raiz de todos os problemas importantes e definir as soluções para os problemas operacionais identificados.

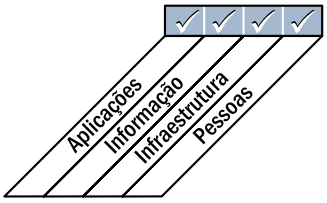
é alcançado por:

- Realização de análises da causa-raiz do problema reportado
- Análise das tendências
- Propriedade dos problemas e progresso em sua resolução

e medido por:

- Quantidade de problemas recorrentes com impacto sobre os negócios
- Percentual de problemas resolvidos dentro do período de tempo requerido
- Frequência dos reportes ou atualizações de problemas existentes, com base na severidade do problema.





Objetivos de Controle Detalhados

DS10 Gerenciar os Problemas

DS10.1 Identificar e Classificar os Problemas
Implementar processos para reportar e classificar os problemas identificados como parte do gerenciamento de incidentes. Os passos envolvidos na classificação de problemas são similares aos passos da classificação de incidentes; eles servem para determinar a categoria, o impacto, a urgência e a prioridade. Os problemas devem ser classificados adequadamente em grupos ou domínios relacionados (por exemplo, *hardware*, *software*, suporte ao *software*). Esses grupos devem corresponder às responsabilidades organizacionais da base de clientes e usuários e servir de base para alocação dos problemas à equipe de suporte.

DS10.2 Rastreamento e Resolução de Problemas
O sistema de gerenciamento de problemas deve fornecer recursos de trilha de auditoria adequados que permitam o rastreamento, a análise e a identificação da causa-raiz de todos os problemas reportados, considerando:
· Todos os itens de configuração associados
· Os problemas e incidentes pendentes
· Os erros conhecidos e suspeitos
· Rastreamento de tendências de problemas

Identificar e iniciar solução sustentável, tratando a causa-raiz e apresentando solicitações de mudanças de acordo com o processo de gerenciamento de mudanças estabelecido. Através do processo de resolução, o gerenciamento de problemas deve obter reportes periódicos do gerenciamento de mudanças sobre o progresso da resolução de problemas e erros. O gerenciamento de problemas deve monitorar continuamente o impacto dos problemas e erros conhecidos nos serviços de usuários. No caso de impactos severos, o gerenciamento de problemas deve encaminhar o problema, talvez o apresentando ao grupo apropriado para aumentar a prioridade da requisição de mudança (RDM) ou implementar mudanças urgentes apropriadas. O andamento da solução do problema deve ser monitorado de acordo com os níveis de serviço acordados (SLAs).

DS10.3 Encerramento do Problema
Estabelecer um procedimento de encerramento dos registros de problemas tanto na confirmação da eliminação bem-sucedida de um erro conhecido quanto após um acordo com as áreas de negócio sobre como lidar com o problema de forma alternativa.

DS10.4 Integração de Gerenciamento de Mudanças, Configuração e Problemas
Integrar os processos de configuração e gerenciamento de problemas e incidentes para assegurar um gerenciamento efetivo de problemas e possibilitar melhorias no processo.

Diretrizes de Gerenciamento

DS10 Gerenciar os Problemas

Origem	Entrada
AI6	Autorização de mudanças;
DS8	Relatórios de incidentes;
DS9	Configuração de TI / Detalhes de Ativos;
DS13	Registros de erros

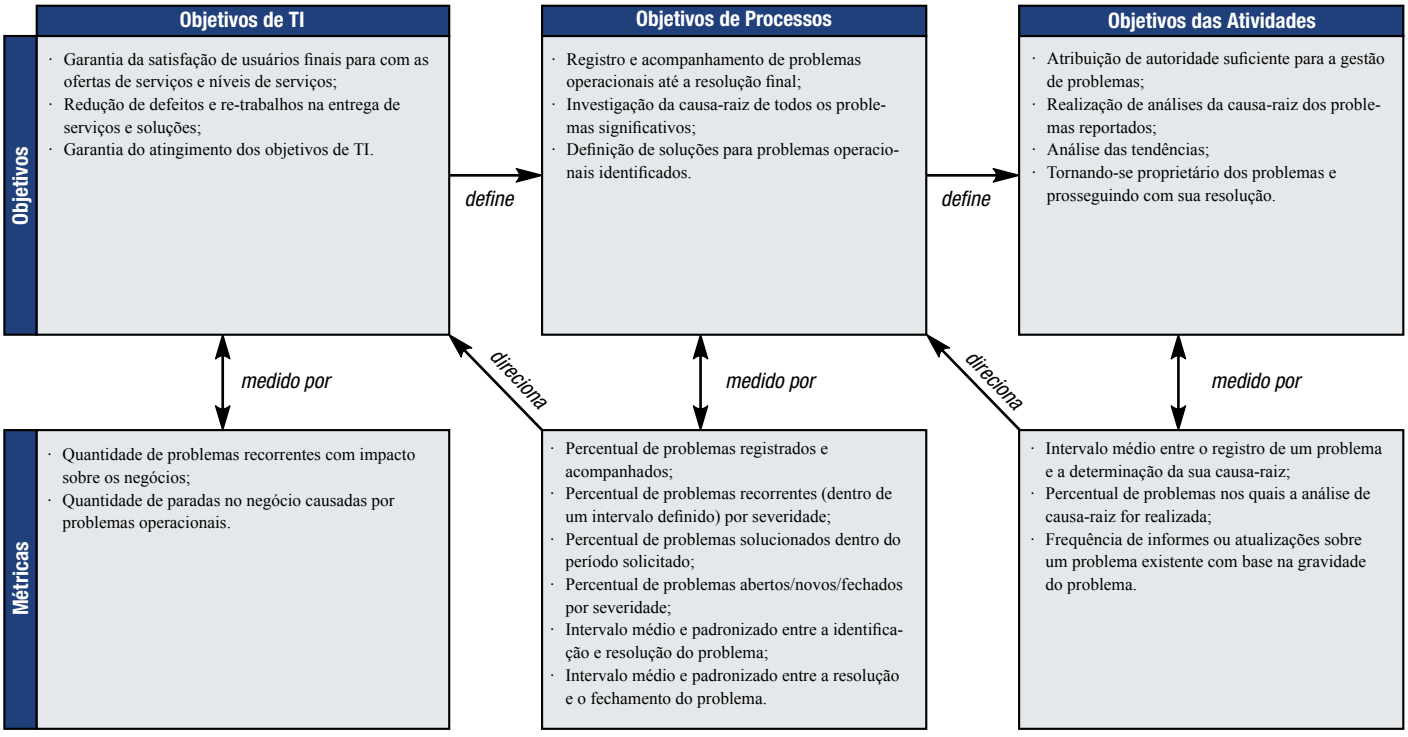
Saída	Destino
Solicitações de mudança (como e onde aplicar a correção);	AI6
Registros de problemas;	AI6
Relatórios de desempenho de processos;	ME1
Problemas e erros conhecidos e soluções alternativas	DS8

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Gerência de Problemas
Identificar e classificar os problemas;			I	I	C	A	C	C			I	R
Realizar análises de causa-raiz;						C		C				A/R
Resolver problemas;					C	A	R	R		R	C	C
Avaliar o status dos problemas;			I	I	C	A/R	C	C		C	C	R
Emitir recomendações para melhoria e criar a respectiva solicitação de mudança (RFC);					I	A	I	I		I		R
Manter registros de problemas					I	I		I			I	A/R

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS10 Gerenciar Problemas

O gerenciamento do processo de ***"gerenciar problemas"*** que satisfaça ao requisito do negócio para a TI de ***"assegurar a satisfação dos usuários finais com oferta e níveis de serviço e reduzir a entrega de serviços e soluções com problemas e retrabalhos"*** é:

0 Inexistente quando
Não há conscientização da necessidade de gerenciamento de problemas tampouco há diferenciação entre problemas e incidentes. Portanto, não há tentativa de identificar a origem dos incidentes.

1 Inicial/ *Ad hoc* quando
As pessoas reconhecem a necessidade de gerenciar os problemas e resolver as causas fundamentais. Pessoas-chave dão alguma assistência para resolver os problemas relacionados às suas respectivas áreas de especialidade, porém a responsabilidade pelo gerenciamento do problema não é atribuída a uma pessoa específica. A informação não é compartilhada, o que resulta em criação adicional de problemas e perda de tempo produtivo na busca de soluções.

2 Repetível, porém Intuitivo quando
Há uma ampla conscientização da necessidade e dos benefícios de gerenciar problemas relacionados a TI entre as unidades de negócios e área de serviços de informação. O processo de resolução tem evoluído a um ponto em que poucas pessoas-chave são responsáveis por identificar e resolver problemas. A informação é compartilhada entre o pessoal de maneira informal e reativa. O nível de serviço à comunidade usuária varia e é dificultado por conhecimento estruturado insuficiente disponível ao gerente de problemas.

3 Processo Definido quando
A necessidade de um efetivo sistema integrado de gerenciamento de problemas é aceita e evidenciada pelo apoio da gerência, e há orçamento disponível para recrutamento e treinamento. A resolução de problemas e os processos de encaminhamento foram padronizados. Os registros, rastreamento e resoluções de problemas são fragmentados dentro da equipe de resposta, utilizando as ferramentas disponíveis sem centralização. Desvios de normas ou padrões estabelecidos provavelmente não são detectados. A informação é compartilhada entre o pessoal de maneira proativa e formal. A revisão de incidentes pela gerência e a análise da identificação e resolução de problemas são informais e limitadas.

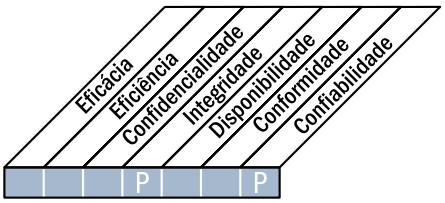
4 Gerenciado e Mensurável quando
O processo de gerenciamento de problemas é compreendido em todos os níveis da organização. As responsabilidades e propriedades são claras e estão estabelecidas. Os métodos e procedimentos são documentados, comunicados e mensurados pela efetividade. A maioria dos problemas é identificada, registrada, reportada e as resoluções são iniciadas. O conhecimento e a habilidade são cultivados, mantidos e desenvolvidos em um alto nível, fazendo com que a área seja vista como um ativo e a maior contribuição para atingir os objetivos de TI e melhoria dos serviços de TI. O gerenciamento de problemas é bem integrado aos processos inter-relacionados, tais como incidente, mudança, gerenciamento de disponibilidade e configuração, assistência aos clientes no gerenciamento de dados, operações e facilidades. Existem objetivos e métricas acordados para o processo de gerenciamento de problemas.

5 Otimizado quando
O processo de gerenciamento de problemas evolui para um processo de busca contínua e proativa, contribuindo com os objetivos de TI. Os problemas são antecipados e evitados. O conhecimento dos padrões do passado e de problemas futuros é mantido através de contatos frequentes com fornecedores e especialistas. O registro, reporte, análise e resoluções dos problemas são automatizados e totalmente integrados ao gerenciamento de dados de configuração. Os objetivos e métricas são mensurados consistentemente. A maioria dos sistemas está equipada com mecanismos automáticos de detecção e advertência, os quais são continuamente rastreados e avaliados. O processo de gerenciamento de problemas é analisado visando a melhoria contínua com base na análise das mensurações e reportados às partes interessadas.

Descrição do Processo

DS11 Gerenciar os Dados

O efetivo gerenciamento de dados requer a identificação dos requisitos de dados. O processo de gerenciamento de dados também contempla o estabelecimento de procedimentos efetivos para controlar a biblioteca de mídia, cópia de segurança *(backup)*, recuperação de dados e a dispensa de mídias de forma adequada. O efetivo gerenciamento de dados ajuda a assegurar a qualidade, a rapidez e disponibilidade dos dados de negócio.



Controle sobre o seguinte processo de TI:

Gerenciar os dados

que satisfaça aos seguintes requisitos do negócio para a TI:

otimizar o uso da informação e garantir que a informação esteja disponível quando requisitada

com foco em:

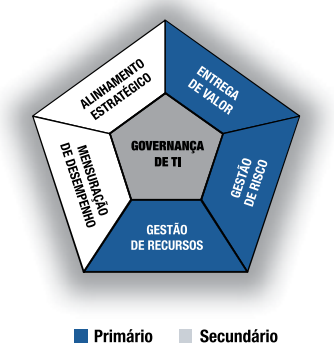
manter a completude, a precisão, a disponibilidade e a proteção dos dados

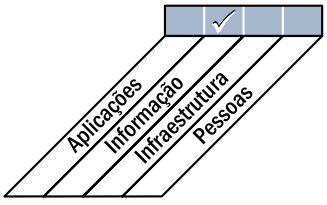
é alcançado por:

- Realização de cópia de segurança *(backup)* dos dados e testes de restauração
- Gerenciamento de armazenamento local e remoto dos dados (*onsite* e *offsite*)
- Descarte seguro de dados e equipamentos

e medido por:

- Satisfação do usuário com a disponibilidade dos dados
- Percentual de restaurações de dados bem-sucedidas
- Volume de incidentes nos quais dados confidenciais foram recuperados com sucesso após descarte da mídia.





Objetivos de Controle Detalhados

DS11 Gerenciar os Dados

DS11.1 Requisitos de Negócio para o Gerenciamento de Dados
Estabelecer arranjos para assegurar que todos os dados esperados sejam recebidos, processados de maneira completa, precisa e no tempo apropriado e que toda saída seja entregue de acordo com os requisitos de negócio. Suportar as necessidades de reinício e reprocessamento.

DS11.2 Arranjos de Armazenamento e Retenção
Definir e implementar procedimentos para um efetivo e eficiente armazenamento de dados, retenção e arquivamento para atender aos objetivos de negócio, à política de segurança da organização e às exigências regulatórias.

DS11.3 Sistema de Gerenciamento de Biblioteca de Mídia
Definir e implementar procedimentos para manter um inventário de mídia local, assegurando sua usabilidade e integridade.

DS11.4 Descarte de Dados e Equipamentos
Definir e implementar procedimentos para assegurar que os requisitos de negócios sejam atendidos no que diz respeito à proteção de dados confidenciais e softwares quando dados e equipamentos são descartados ou transferidos.

DS11.5 *Backup* e Restauração
Definir e implementar procedimentos de cópia de segurança *(backup)* e restauração de sistemas, aplicativos, dados e documentação em alinhamento com os requisitos de negócio e o plano de continuidade.

DS11.6 Requisitos de Segurança para o Gerenciamento de Dados
Definir e estabelecer políticas e procedimentos para identificar e aplicar requisitos de segurança aplicáveis ao recebimento, processamento, armazenamento físico e saída de dados para atender aos objetivos de negócio, à política de segurança da organização e a exigências regulatórias.

Diretrizes de Gerenciamento

DS11 Gerenciar os Dados

Origem	Entrada
PO2	Dicionário de dados; Classificações atribuídas a dados;
AI4	Manuais de usuário, operação, suporte, técnico e administração;
DS1	OLAs;
DS4	Plano de guarda e proteção de cópias de segurança *(backups)*;
DS5	Plano e políticas de segurança de TI

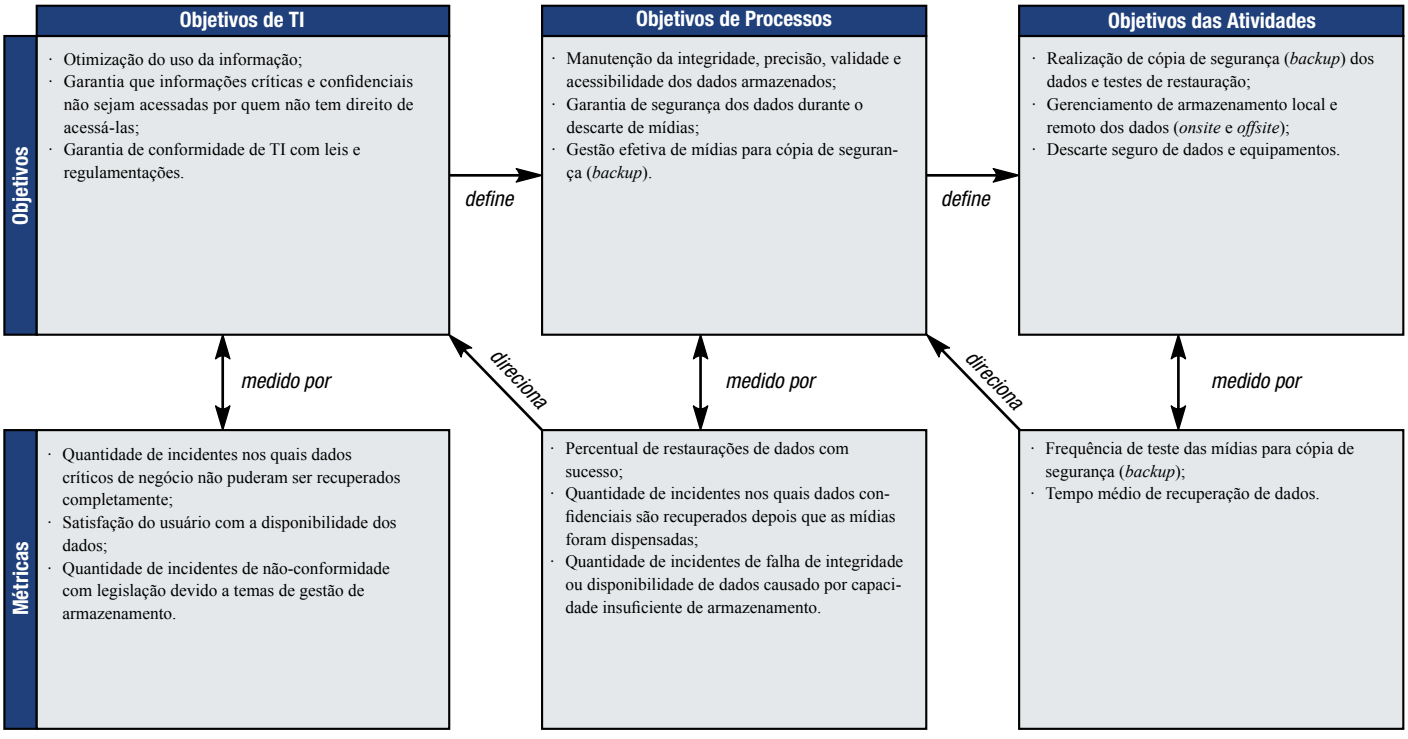
Saída	Destino
Relatórios de desempenho de processos;	ME1
Instruções de gestão de dados para os operadores	DS13

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Traduzir os requisitos de armazenamento e retenção de dados em procedimentos;				A	I	C	R				C
Definir, manter e implementar procedimentos para gerenciar biblioteca de mídias (fitoteca);				A		R	C	C	I		C
Definir, implementar e manter procedimentos para dispensa de forma segura de equipamentos e mídias;				A	C	R			I		C
Realizar cópia de segurança *(backup)* de acordo com o esquema;				A		R					
Definir, implementar e manter procedimentos para restauração de dados				A	C	R	C	C			I

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS11 Gerenciar os Dados

O gerenciamento do processo de ***"gerenciar os dados"*** que satisfaça ao requisito do negócio para a TI de ***"otimizar o uso da informação e garantir que a informação esteja disponível quando requisitada"*** é:

0 Inexistente quando
Os dados não são reconhecidos como ativos e recursos corporativos. Não existe proprietário atribuído aos dados ou nem responsabilidade individual pelo gerenciamento dos dados. A qualidade e segurança dos dados é deficiente ou inexistente.

1 Inicial/ *Ad hoc* quando
A organização reconhece a necessidade de um gerenciamento preciso de dados. Há um método *ad hoc* para especificar os requisitos de segurança de gerenciamento de dados, porém não existe um procedimento formal de comunicação. Não há treinamento específico em gerenciamento de dados. A responsabilidade final pelo gerenciamento dos dados não é clara. Existem procedimentos de cópia de segurança *(backup)*, restauração e descarte de dados.

2 Repetível, porém Intuitivo quando
Existe a consciência da necessidade de um gerenciamento de dados preciso em toda a organização. A propriedade dos dados em alto nível começa a ser definida. Os requisitos de segurança para o gerenciamento de dados são documentados por pessoas-chave. Algum monitoramento é realizado sobre as principais atividades de gerenciamento de dados (*backup*, restauração, disponibilização). As responsabilidades pelo gerenciamento de dados são atribuídas informalmente a pessoas-chave da área de TI.

3 Processo Definido quando
A necessidade de gerenciamento de dados dentro da TI e em toda a organização é compreendida e aceita. A responsabilidade pelo gerenciamento de dados é estabelecida. A propriedade dos dados é atribuída às áreas responsáveis, que controlam a integridade e segurança. Os procedimentos de gerenciamento de dados são formalizados dentro da TI, e são utilizadas algumas ferramentas de cópia de segurança *(backup)*, restauração e descarte de equipamento. Existe algum monitoramento sobre o gerenciamento de dados. As métricas básicas de desempenho são definidas. Existe treinamento para os profissionais de gerenciamento de dados.

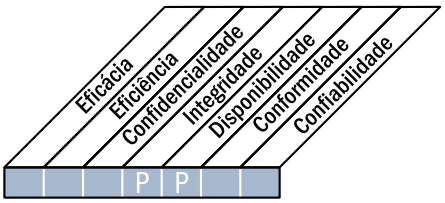
4 Gerenciado e Mensurável quando
A necessidade de um gerenciamento de dados é entendida e as ações necessárias são aceitas na organização. A responsabilidade pelo gerenciamento e as propriedades dos dados é claramente definida, estabelecida e amplamente comunicada na organização. Os procedimentos são formalizados e amplamente conhecidos e o conhecimento é compartilhado. Inicia-se o uso das ferramentas mais atuais. Os objetivos e indicadores de desempenho são acordados com os clientes e monitorados através de um processo bem definido. Existe treinamento formal dos profissionais de gerenciamento de dados.

5 Otimizado quando
A necessidade do gerenciamento de dados e o entendimento de todas as ações requeridas é compreendido e aceito na organização. Necessidades e requisitos futuros são explorados de forma proativa. As responsabilidades pela propriedade e o gerenciamento dos dados são claramente estabelecidas, amplamente conhecidas em toda a organização e atualizadas em tempo hábil. Os procedimentos são formalizados e amplamente conhecidos, o compartilhamento do conhecimento é uma prática padrão. Ferramentas sofisticadas são utilizadas com máxima automação do gerenciamento de dados. Os objetivos e indicadores de desempenho são acordados com os clientes, alinhados aos objetivos do negócio e monitorados de forma consistente através de um processo bem definido. As oportunidades de melhoria são constantemente exploradas. O treinamento para os profissionais de gerenciamento de dados é institucionalizado.

Descrição do Processo

DS12 Gerenciar o Ambiente Físico

A proteção de pessoas e equipamento de informática requer instalações físicas bem planejadas e gerenciadas. O processo de gerenciamento do ambiente físico inclui a definição dos requisitos do local físico, a escolha de instalações apropriadas, o projeto de processos eficazes de monitoramento dos fatores ambientais e o gerenciamento de acessos físicos. O gerenciamento eficaz do ambiente físico reduz as interrupções nos negócios provocadas por danos causados a equipamentos ou pessoas.



Controle sobre o seguinte processo de TI:

Gerenciar o ambiente físico

que satisfaça aos seguintes requisitos do negócio para a TI:

proteger os ativos de TI e os dados do negócio e minimizar o risco de interrupção nos negócios

com foco em:

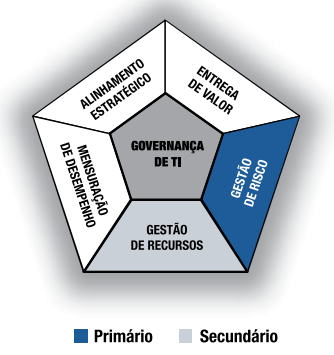
prover e manter um ambiente físico adequado que proteja os recursos de TI contraacesso indevido, danos ou roubo

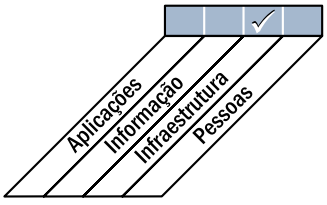
é alcançado por:

· Implementação de medidas de segurança física
· Seleção e gerenciamento de instalações físicas

e medido por:

· Tempo de indisponibilidade devido a incidentes no ambiente físico
· Quantidade de incidentes causados por falhas ou violação da segurança física
· Frequência das avaliações e revisões de riscos físicos





Objetivos de Controle Detalhados

DS12 Gerenciar o Ambiente Físico

DS12.1 Seleção do Local e Layout
Definir e selecionar o local para os equipamentos de TI, considerando o alinhamento da estratégia de tecnológica com a estratégia de negócio. A seleção e o planejamento do layout de uma instalação física devem levar em consideração os riscos associados a possíveis desastres naturais e não naturais, bem como as leis e regulamentações relevantes, tais como regulamentações de saúde ocupacional e segurança do trabalho.

DS12.2 Medidas de Segurança Física
Definir e implementar medidas de segurança física alinhadas com os requisitos de negócio para proteger o local e os ativos físicos. As medidas de segurança física devem ser capazes de efetivamente prevenir, detectar e mitigar riscos relacionados a roubo, temperatura, fogo, fumaça, água, vibração, terrorismo, vandalismo, quedas de energia, produtos químicos ou explosivos.

DS12.3 Acesso Físico
Definir e implementar procedimentos para conceder, limitar e revogar o acesso a instalações, prédios e áreas de acordo com as necessidades do negócio, inclusive em situações de emergências. Os acessos a instalações, prédios e áreas devem ser justificados, autorizados, registrados e monitorados. Isso se aplica a todas as pessoas que acessam as instalações, inclusive ao pessoal fixo, funcionários temporários, clientes, vendedores, visitantes ou outros terceiros.

DS12.4 Proteção contra Fatores Ambientais
Projetar e implementar medidas de proteção contra fatores ambientais. Equipamentos e dispositivos especializados para monitorar e controlar o ambiente devem ser instalados.

DS12.5 Gerenciamento de Instalações Físicas
Gerenciar as instalações físicas, incluindo equipamentos de energia e comunicação, em alinhamento com leis e regulamentações, requisitos técnicos e de negócio, especificações dos fabricantes e distribuidores de equipamentos e diretrizes de segurança e saúde ocupacional.

Diretrizes de Gerenciamento

DS12 Gerenciar o Ambiente Físico

Origem	Entrada
PO2	Classificações atribuídas a dados;
PO9	Análise de riscos;
AI3	Requisitos do ambiente físico

Saída	Destino						
Relatórios de desempenho de processos	ME1						

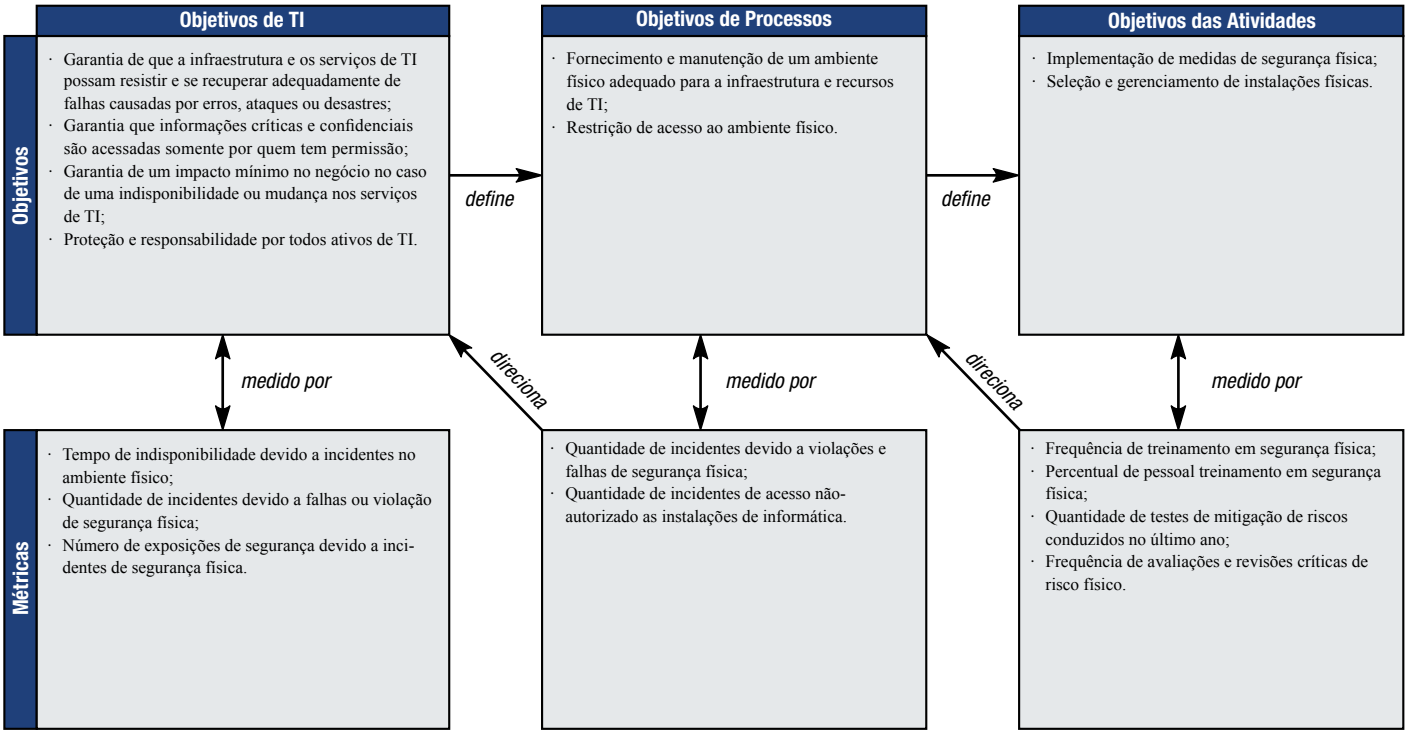
Tabela RACI

Atividades	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir o nível necessário de proteção física;					C	A/R	C				C
Selecionar e comissionar instalações físicas (data, center, escritório, etc);	I	C	C	C	C	A/R	C		C	C	C
Implementar medidas no ambiente físico;					I	A/R	I	I			C
Gerenciar o ambiente físico (manutenção, monitoração e relatórios incluídos);						A/R	C				
Definir e implementar procedimentos para autorização e manutenção de acesso físico				C	I	A/R	I	I	I		C

Funções

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS12 Gerenciar o Ambiente Físico

O gerenciamento de processo ***"Gerenciar o ambiente físico"*** que satisfaça ao requisito do negócio para a TI de ***"proteger os ativos de TI e dados de negócio e minimizar o risco de interrupção nos negócios"*** é:

0 Inexistente quando
Não há consciência da necessidade de proteger as instalações ou os investimentos em recursos de computação. Fatores ambientais, como proteção contra incêndios, poeira ou sujeira, energia elétrica, calor e umidade excessivos, não são monitorados nem controlados.

1 Inicial/ *Ad hoc* quando
A organização reconhece como requisito de negócio ter um ambiente físico adequado que proteja os recursos e as pessoas contra desastres naturais e não naturais. O gerenciamento de instalações e equipamentos é dependente das habilidades e capacidades técnicas de pessoas-chave. As pessoas podem transitar nas instalações sem qualquer restrição. Os responsáveis pelo gerenciamento não monitoram os controles ambientais das instalações ou o trânsito de pessoas.

2 Repetível, porém Intuitivo quando
Os controles ambientais são implementados e monitorados pela equipe de operações. A segurança física é um processo informal conduzido por um pequeno grupo de funcionários com alto nível de preocupação com a proteção das instalações físicas. Os procedimentos de manutenção das instalações não estão bem documentados e se baseiam em boas práticas de poucos indivíduos. Os objetivos da segurança física não são baseados em quaisquer padrões formais, e os responsáveis pelo gerenciamento não garantem que os objetivos da segurança sejam alcançados.

3 Processo Definido quando
A necessidade de controlar um ambiente de computação é compreendida e aceita dentro da organização. Os controles ambientais, a manutenção preventiva e a segurança física são itens orçados, aprovados e acompanhados pela Direção. Restrições de acesso são aplicadas e apenas pessoal aprovado tem acesso autorizado às instalações computacionais. Os visitantes são registrados e acompanhados sob a responsabilidade de alguém. As instalações físicas são discretas e não são facilmente identificáveis. As autoridades civis monitoram a conformidade com as regulamentações de segurança e de saúde. Os riscos são considerados de mínimo valor otimizando os custos de seguros.

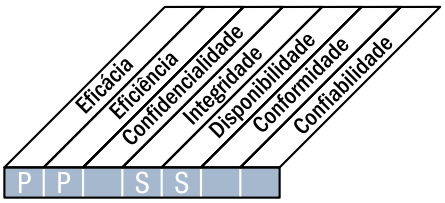
4 Gerenciado e Mensurável quando
A necessidade para manter um ambiente computacional controlado é totalmente compreendida, o que pode ser evidenciado pela estrutura organizacional e a alocação de orçamentos. Os requisitos de segurança física e ambientais são documentados e o acesso físico é rigorosamente controlado e monitorado. O proprietário desse processo e sua responsabilidade foram estabelecidos e comunicados. A equipe responsável pelas instalações computacionais está completamente treinada em situações de emergência, bem como nas práticas de segurança e saúde do trabalho. Mecanismos de controle padronizados são estabelecidos para restringir o acesso físico às instalações e consideram fatores ambientais e de segurança. Os responsáveis pelo gerenciamento monitoram a efetividade dos controles e a conformidade com os padrões estabelecidos. Os responsáveis pelo gerenciamento estabeleceram objetivos e métricas para avaliar o gerenciamento do ambiente computacional. A capacidade de recuperação dos recursos computacionais está incorporada ao processo de gerenciamento de riscos organizacionais. A informação integrada é utilizada para otimizar a cobertura de seguros e custos associados.

5 Otimizado quando
Existe um plano de longo prazo aprovado para as instalações físicas do ambiente computacional da organização. Padrões são definidos para todas as instalações, envolvendo escolha de local, construção, vigilância, segurança do pessoal, sistemas elétricos e mecânicos, proteção contra fatores ambientais (incêndios, raios, inundações). Todas as instalações são inventariadas e classificadas de acordo com o processo vigente de gerenciamento de riscos da organização. O acesso físico é controlado rigorosamente de acordo com a necessidade do cargo e monitorado continuamente e todos os visitantes são acompanhados em tempo integral. O ambiente é monitorado e controlado por equipamentos especializados, e as salas de equipamentos não têm identificação pública. Os objetivos e métricas são consistentemente avaliados. Os programas de manutenção preventiva seguem os cronogramas rigorosamente, e testes periódicos são realizados nos equipamentos críticos. Os padrões e a estratégia de gerenciamento das instalações estão alinhados com as metas de disponibilidade de serviços de TI e integrados ao planejamento de continuidade de negócio e gerenciamento de crises. Os responsáveis pelo gerenciamento examinam e otimizam as instalações de TI utilizando continuamente as medições, capitalizando oportunidades para melhorar a contribuição com o negócio.

Descrição do Processo

DS13 Gerenciar as Operações

O processamento preciso e completo de dados requer um gerenciamento eficaz do processamento de dados e diligente manutenção de *hardware*. Este processo inclui a definição de políticas e procedimentos de operações para o gerenciamento eficaz do processamento agendado, proteção de resultados sigilosos, monitoramento de infraestrutura e manutenção preventiva de *hardware*. O efetivo gerenciamento de operações ajuda a manter a integridade dos dados e reduzir atrasos e custos de operação de TI.



Controle sobre o seguinte processo de TI:

Gerenciar as Operações

que satisfaça aos seguintes requisitos do negócio para a TI:

manter a integridade dos dados e assegurar que a infraestrutura de TI possa resistir e se recuperar de erros e falhas

com foco em:

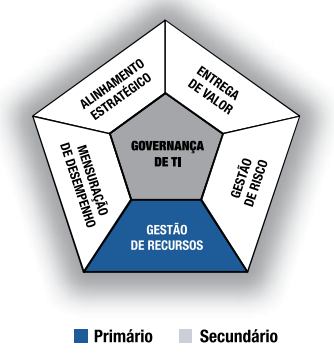
atingir os níveis de serviço operacionais para o processamento programado de dados, proteção das saídas de dados críticos, monitoramento e manutenção da infraestrutura

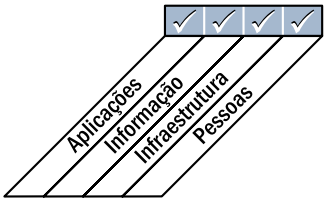
é alcançado por:

- Operação do ambiente de TI alinhado com os acordos de níveis de serviço e instruções definidas
- Manutenção da infraestrutura de TI

e medido por:

- Quantidade de níveis de serviço impactados por incidentes operacionais
- Quantidade de horas de paradas não programadas causadas por incidentes operacionais
- Percentual de ativos de hardware incluídos na programação de manutenção preventiva





Objetivos de Controle Detalhados

DS13 Gerenciar as Operações

DS13.1 Procedimentos e Instruções de Operações
Definir, implementar e manter procedimentos padronizados para as operações de TI e assegurar que a equipe de operações esteja familiarizada com todas as atividades operacionais relevantes. Os procedimentos operacionais devem abranger a mudança de turnos (passagem formal das atividades, atualização de informações, problemas operacionais, procedimentos de escalação e relatórios das responsabilidades atuais) para assegurar o nível de serviço acordado e a continuidade das operações.

DS13.2 Agendamento de *Jobs*
Organizar o agendamento de *jobs*, processos e tarefas na sequência mais eficiente, maximizando o processamento e a utilização para atender aos requisitos do negócio.

DS13.3 Monitoramento da Infraestrutura de TI
Definir e implementar procedimentos para monitorar a infraestrutura de TI e eventos relacionados. Assegurar que informações cronológicas suficientes estejam sendo armazenadas em registros operacionais para permitir a reconstrução, a revisão e a análise das sequências de operações e outras atividades pertinentes ou de apoio às operações.

DS13.4 Documentos Confidenciais e Dispositivos de Saída
Estabelecer proteção física apropriada, práticas de controle e gerenciamento de inventário sobre ativos críticos de TI como formulários especiais, documentos de negociação, impressoras de finalidades especiais ou códigos de segurança.

DS13.5 Manutenção Preventiva de *Hardware*
Definir e implementar procedimentos para assegurar a manutenção da infraestrutura em tempo hábil para reduzir a frequência e o impacto de falhas ou degradação de desempenho.

Diretrizes de Gerenciamento

DS13 Gerenciar as Operações

Origem	Entrada
AI4	Manuais de usuário, operação, suporte, técnico e administração;
AI7	Migração para produção; Liberação de *software* e planejamento de distribuição;
DS1	SLAs e OLAs;
DS4	Plano de guarda e proteção de cópias de segurança *(backups)*;
DS9	Configuração de TI / Detalhes de Ativos;
DS11	Instruções de gestão de dados para os operadores

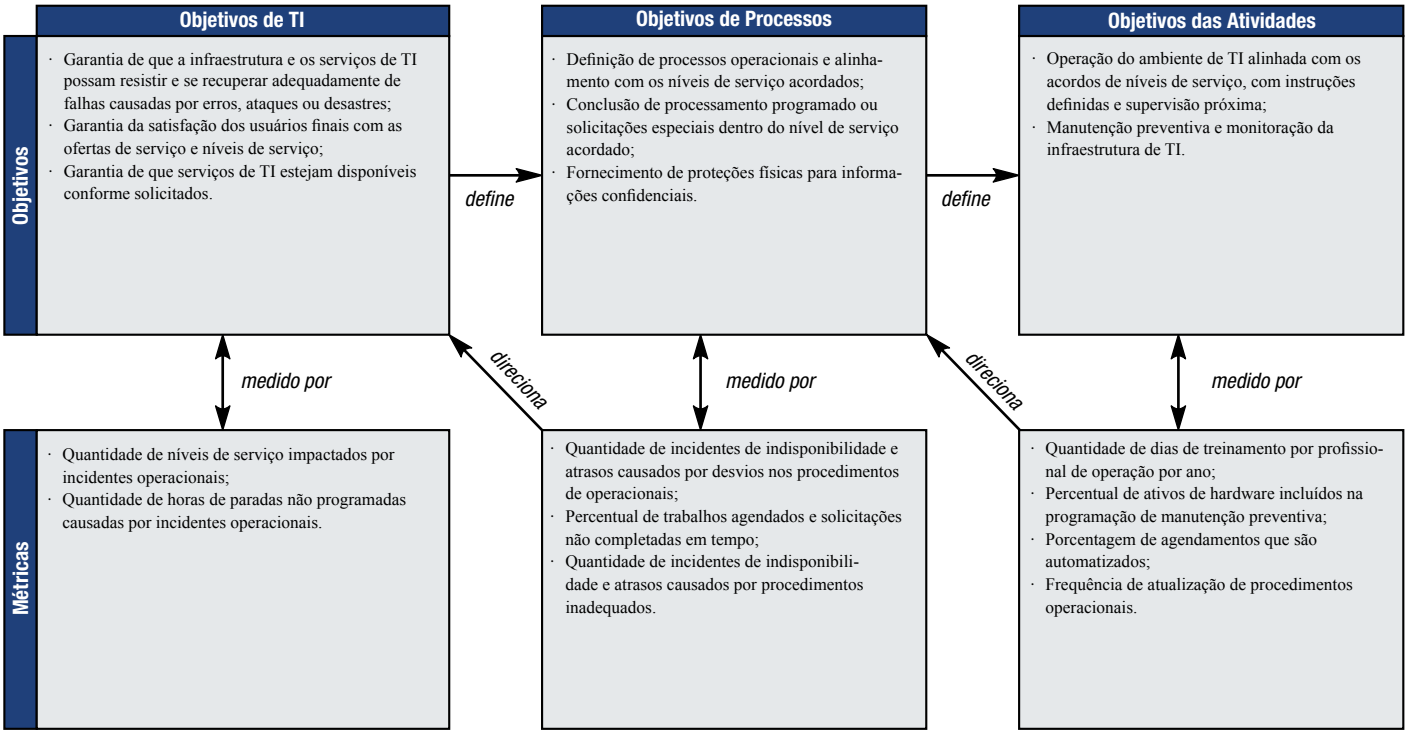
Saída	Destino
Chamados de incidentes;	DS8
Registros de erros;	DS10
Relatórios de desempenho de processos	ME1

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Criar / modificar procedimentos de operações (incluindo manuais, listas, documentações, procedimentos de escalação, etc)						A/R					I
Agendar carga de trabalho e *jobs (batch jobs)*;					C	A/R	C	C			
Monitorar a infraestrutura e processamento e resolver problemas;						A/R					I
Gerenciar e proteger os ativos físicos (papéis, mídias, etc);						A/R					C
Aplicar correções ou mudanças ao processamento ou infraestrutura;					C	A/R	C	C			C
Implementar / estabelecer um processo para salvaguarda de dispositivos de autenticação contra interferência, perda ou roubo;				A		R			I		C
Programar e realizar manutenção preventiva						A/R					

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

DS13 Gerenciar as Operações

O gerenciamento do processo de ***"Gerenciar as Operações"*** que satisfaça ao requisito do negócio para a TI de ***"manter a integridade dos dados e assegurar que a infraestrutura de TI possa resistir e se recuperar de erros e falhas"*** é:

0 Inexistente quando
A organização não dedica tempo nem recursos para estabelecer atividades básicas de suporte e operações de TI.

1 Inicial/ *Ad hoc* quando
A organização reconhece a necessidade de estruturação das funções de suporte de TI. Poucos procedimentos padrões estão estabelecidos, e as atividades de operação são reativas por natureza. A maioria dos processos operacionais é programada informalmente, e solicitações do processamento são aceitas sem prévia validação. Computadores, sistemas e aplicações que sustentam os processos de negócio são frequentemente interrompidos, retardados e se tornam indisponíveis. Tempo é perdido enquanto funcionários esperam por recursos. Mídias de armazenamento de saída às vezes aparecem em locais inesperados ou nunca aparecem.

2 Repetível, porém Intuitivo quando
A organização está consciente do papel-chave que as atividades de operação de TI representam ao prover funções de suporte de TI. Orçamentos para ferramentas são alocados caso a caso. As operações de apoio à TI são informais e intuitivas. Existe uma grande dependência de habilidades e capacidades técnicas de pessoas específicas. As instruções do que, quando e em que ordem se deve fazer algo não são documentadas. Existe algum treinamento em operação de TI e alguns padrões formais de operações.

3 Processo Definido quando
A necessidade de um gerenciamento de operações é entendida e aceita dentro da organização. Os recursos têm sido alocados e ocorre algum treinamento durante o serviço. Funções repetitivas são formalmente definidas, padronizadas e documentadas. Os eventos e resultados das atividades concluídas são registrados, porém com reporte limitado para gerenciamento. O uso de agendamento automatizado e de outras ferramentas é introduzido para limitar a intervenção do operador. Controles são utilizados para colocar novas rotinas em operação. É desenvolvida uma política formal para reduzir o número de eventos não agendados. Acordos de manutenção e de serviço com fornecedores ainda são informais.

4 Gerenciado e Mensurável quando
As responsabilidades pelo processo de operações e suporte são claramente definidas e um proprietário é designado. As operações são suportadas através de recursos orçados para dispêndios de capital e de recursos humanos. O treinamento é formalizado e constante. Agendamentos e atividades são documentados e comunicados tanto para o público interno de TI quanto para os clientes de negócio. É possível avaliar e monitorar as atividades diárias com acordos de desempenho padronizados e níveis de serviço estabelecidos. Quaisquer desvios das normas estabelecidas são rapidamente identificados e corrigidos. Os responsáveis pelo gerenciamento monitoram o uso dos recursos computacionais, o término de trabalhos ou as atribuições de atividades. Existe um esforço em andamento para elevar o nível de automação do processo como um meio de melhoria contínua. Acordos formais de serviços e manutenção são estabelecidos com os fornecedores. Há um completo alinhamento entre os processos de gerenciamento de problemas, de disponibilidade e capacidade, sustentados por análises das causas de erros e falhas.

5 Otimizado quando
As operações de apoio a TI são eficazes, eficientes e suficientemente flexíveis para atender às necessidades de nível de serviço com mínima perda de produtividade. Os processos de gerenciamento operacional de TI são padronizados e documentados em uma base de conhecimento e estão sujeitos a melhoria contínua. Os processos automatizados que apóiam os sistemas operam de modo imperceptível e contribuem para um ambiente estável. Todos os problemas e falhas são analisados com a finalidade de identificar a causa-raiz. Reuniões periódicas com o gerenciamento de mudança asseguram a inclusão de mudanças nos agendamentos da produção em tempo hábil. Em cooperação com os fornecedores, os equipamentos são analisados em função da idade e sintomas de mau funcionamento e normalmente a manutenção é preventiva.

Monitorar e Avaliar

ME1 Monitorar e Avaliar o Desempenho de TI

ME2 Monitorar e Avaliar os Controles Internos

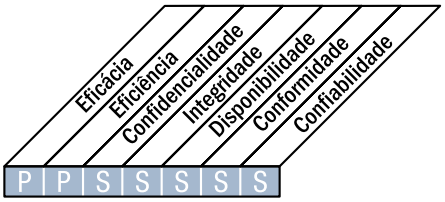
ME3 Assegurar a Conformidade com Requisitos Externos

ME4 Prover Governança de TI

DESCRIÇÃO DE PROCESSO

ME1 Monitorar e Avaliar o Desempenho de TI

A gestão eficaz de desempenho de TI exige um processo de monitoramento. Esse processo inclui a definição de indicadores de desempenho relevantes, informes de desempenho sistemáticos e oportunos e uma pronta ação em relação aos desvios encontrados. O monitoramento é necessário para assegurar que as atividades corretas estejam sendo feitas e que estejam em alinhamento com as políticas e diretrizes estabelecidas.



Controle sobre o seguinte processo de TI:

Monitorar e avaliar o desempenho de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

transparência e entendimento de custos, benefícios, estratégia, políticas e níveis de serviços de TI, em conformidade com os requisitos de governança

com foco em:

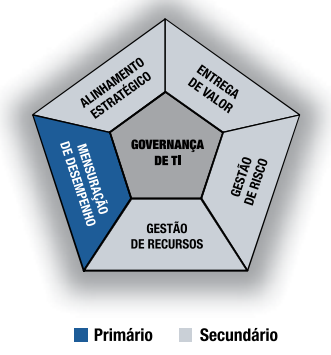
monitorar e entregar relatórios sobre as métricas dos processos de TI e identificar e implementar ações de melhoria de desempenho

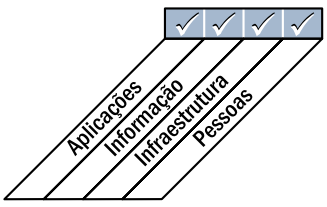
é alcançado por:

- Agrupamento e tradução dos relatórios de desempenho de processos para relatórios de gestão
- Análise crítica de desempenho frente a metas acordadas e a tomada de ações corretivas necessárias

e medido por:

- Satisfação da Alta Direção e das entidades de governança com os relatórios de desempenho
- Quantidade de ações de melhoria resultantes das atividades de monitoramento
- Percentual de processos críticos monitorados





OBJETIVOS DE CONTROLE DETALHADOS

ME1 Monitorar e Avaliar o Desempenho de TI

ME1.1 Abordagem de Monitoramento
Estabelecer uma abordagem e uma estrutura de monitoramento geral que definam o escopo, a metodologia e o processo a serem seguidos para avaliar a entrega de soluções e serviços de TI e monitorar a contribuição da TI para os resultados do negócio. A estrutura deve se integrar com o sistema de gestão de desempenho corporativo.

ME1.2 Definição e Coleta dos Dados de Monitoramento
Trabalhar com o negócio na definição de um conjunto equilibrado de metas de performance que sejam aprovadas pelas áreas de negócio e demais partes interessadas relevantes. Definir comparativos (*benchmarks*) com os quais comparar as metas e identificar os dados disponíveis a serem coletados para medir as metas. Estabelecer processos para coletar em tempo apropriado e de maneira correta os dados a serem inclusos em relatórios que demonstrem o progresso em relação às metas.

ME1.3 Método de Monitoramento
Implementar um método de monitoramento de performance (por exemplo, *balanced scorecard*) que registre as metas, capture as medições, apresente uma visão ampla e sucinta do desempenho da TI e se ajuste ao sistema de monitoramento corporativo.

ME1.4 Avaliação de Desempenho
Analisar periodicamente o desempenho com base nas metas, executar análise de causa-raiz dos problemas e iniciar ação corretiva para tratar as causas ocultas.

ME1.5 Relatórios para a Alta Direção
Desenvolver informes para a Alta Direção sobre a contribuição de TI para o negócio, especialmente em termos de desempenho do portfólio da organização, programas de investimentos em TI e soluções e serviços de cada programa. Nos relatórios gerenciais de status, informar até que ponto os objetivos planejados foram atingidos, os recursos orçados que foram utilizados, as metas de desempenho alcançadas e os riscos minimizados. Antecipar a revisão da Alta Direção sugerindo ações de remediação no caso de desvios importantes. Fornecer relatórios para a Alta Direção e solicitar o retorno *(feedback)* da revisão gerencial.

ME1.6 Ações Corretivas
Identificar e iniciar ações corretivas com base no monitoramento, na avaliação e nos relatórios de desempenho. Isso inclui acompanhamento de todo o processo de monitoramento, relatórios e avaliações com:
- Análise crítica, negociação e estabelecimento de respostas da gerência
- Atribuição de responsabilidade pelas correções
- Verificação dos resultados das ações acordadas

Diretrizes de Gerenciamento

ME1 Monitorar e Avaliar o Desempenho de TI

Origem	Entrada
PO5	Relatórios de custo/benefício;
PO10	Relatórios de desempenho de projetos;
AI6	Relatórios de status das mudanças;
DS1-13	Relatórios de desempenho de processos;
DS3	Planejamento de capacidade e desempenho (requisitos)
DS8	Relatórios sobre satisfação de usuários;
ME2	Relatórios sobre a eficácia dos controles de TI;
ME3	Relatórios sobre a conformidade das atividades de TI com requisitos externos legais e regulatórios;
ME4	Relatórios sobre o status de governança de TI

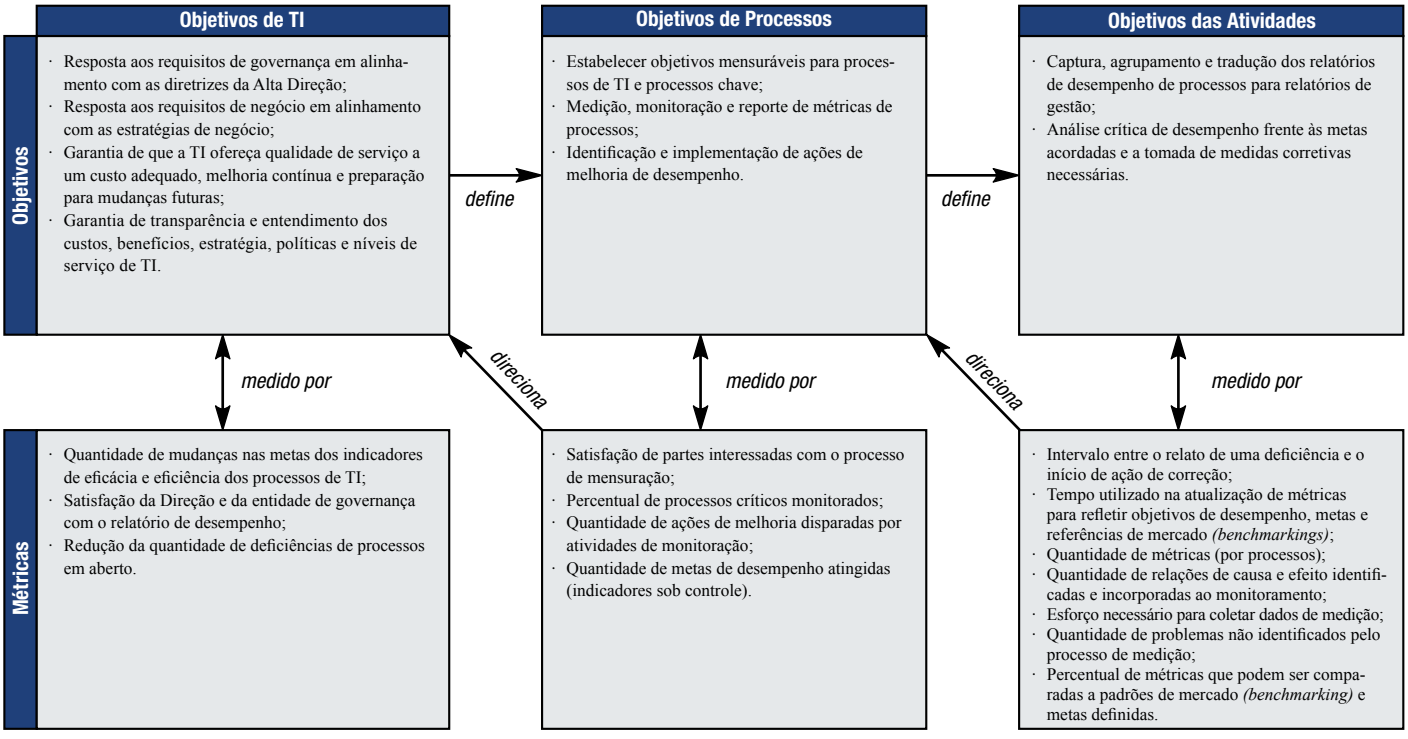
Saída	Destino						
Informações de desempenho para planejamento de TI;	PO1	PO2	DS1				
Planos de ação para remediações;	PO4	PO8					
Histórico de eventos e tendências de riscos;	PO9						
Relatórios de desempenho de processos	ME2						

Tabela RACI

Atividades \ Funções	Conselho de Administração	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Estabelecer uma abordagem de monitoração;		A	R	C	R	I	C	I	C	I		C
Identificar e coletar objetivos mensuráveis que sustentem os objetivos de negócio;		C	C	C	A	R	R		R			
Criar *scorecards*;					A		R	C	R	C		
Avaliar criticamente o desempenho;			I	I	A	R	R	C	R	C		
Reportar o desempenho;	I	I	I	R	A	R	R	C	R	C		I
Identificar e monitorar ações de melhoria de desempenho					A	R	R	C	R	C		C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



Modelo de Maturidade

ME1 Monitorar e Avaliar o Desempenho de TI

O gerenciamento do processo de ***"Monitorar e Avaliar o Desempenho de TI"*** que satisfaça ao requisito do negócio para a TI de ***"transparência e entendimento de custos, benefícios, estratégia, políticas e níveis de serviços de TI, em conformidade com os requisitos de governança"*** é:

0 Inexistente quando
A organização não tem um processo de monitoramento implementado. A TI não executa de forma independente o monitoramento dos projetos ou processos. Relatórios úteis, oportunos e precisos não são disponibilizados. A necessidade de objetivos de processo claramente entendidos não é reconhecida.

1 Inicial/ *Ad hoc* quando
A Direção reconhece a necessidade de coletar e avaliar informações sobre os processos de monitoramento. Processos de coleta e avaliação padronizados não foram identificados. O monitoramento é implementado, mas com métricas escolhidas caso a caso, de acordo com as necessidades de projetos e processos de TI específicos. Normalmente o monitoramento é implementado como resposta a um incidente que tenha causado algum tipo de perda ou embaraço à organização. A função contábil monitora os aspectos financeiros básicos da TI.

2 Repetível, porém Intuitivo quando
Foram identificadas métricas básicas a serem monitoradas. Existem métodos e técnicas de coleta e avaliação, porém os processos não foram adotados por toda a organização. A interpretação dos resultados do monitoramento é baseada na habilidade de pessoas-chave. Ferramentas limitadas são escolhidas e implementadas para coletar informação, porém a coleta não é baseada em uma abordagem planejada.

3 Processo Definido quando
A Direção comunicou e institucionalizou processos padrão de monitoramento. Programas de educação e treinamento em monitoramento foram implementados. Foi desenvolvida uma base de conhecimento formalizada contendo informações históricas de desempenho. As avaliações ainda são executadas em alguns processos e projetos de TI e não estão integradas entre todos os processos. Ferramentas para monitorar os processos e níveis de serviço de TI foram definidas. Métricas da contribuição da área de TI para o desempenho da organização foram definidas com base em critérios operacionais e financeiros tradicionais. Métricas de desempenho específicas para TI, métricas não financeiras, métricas estratégicas, métricas sobre satisfação do cliente e de níveis de serviço estão definidas. Uma estrutura para avaliar o desempenho foi definida.

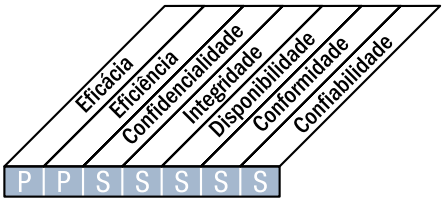
4 Gerenciado e Mensurável quando
A direção definiu as tolerâncias sob as quais os processos devem operar. Os relatórios de resultados do monitoramento estão sendo padronizados e normalizados. Há integração das métricas entre todos os processos e projetos de TI. Os sistemas de relatórios corporativos gerenciais de TI estão formalizados. Ferramentas automatizadas são integradas e disseminadas corporativamente para coletar e monitorar as informações operacionais em aplicações, sistemas e processos. A direção é capaz de avaliar o desempenho com base em critérios acordados e aprovados pelas partes interessadas. As métricas da área de TI estão alinhadas com as metas corporativas.

5 Otimizado quando
Um processo de melhoria contínua da qualidade é desenvolvido para atualizar políticas e padrões corporativos de monitoramento e incorporar as melhores práticas da indústria. Todos os processos de monitoramento são otimizados e apoiam os objetivos corporativos. As métricas orientadas ao negócio são regularmente utilizadas para avaliar o desempenho e estão integradas a estruturas de avaliação estratégicas, tais como o balanced scorecard de TI. O monitoramento e a reformulação contínuos dos processos são consistentes com os planos corporativos de melhoria dos processos de negócio. Avaliações comparativas *(benchmarking)* com a indústria e os principais concorrentes foram formalizadas, com critérios claros de comparação.

DESCRIÇÃO DE PROCESSO

ME2 Monitorar e Avaliar os Controles Internos

Estabelecer um programa eficaz de controles internos de TI requer um processo de monitoramento bem definido. Esse processo inclui o monitoramento e reporte das exceções de controle, dos resultados de autoavaliação e avaliação de terceiros. Um benefício importante do monitoramento dos controles internos é assegurar uma operação eficaz e eficiente e a conformidade com as leis e os regulamentos aplicáveis.



Controle sobre o seguinte processo de TI:

Monitorar e avaliar os controles internos

que satisfaça os seguintes requisitos do negócio para a TI:

assegurar que os objetivos de TI sejam atingidos e assegurar a conformidade com as leis e os regulamentos relacionados à TI

com foco em:

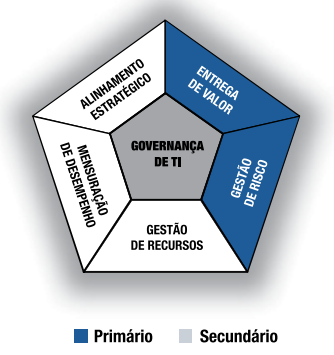
monitorar os processos de controle interno de atividades de TI e identificar ações de melhoria

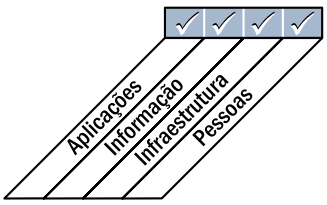
é alcançado por:

· Definição de um sistema de controles internos integrado na estrutura de processos de TI
· Monitoramento e reporte sobre a eficácia dos controles internos de TI
· Reporte das exceções dos controles internos para que os gestores tomem as medidas necessárias

e medido por:

· Quantidade de falhas críticas nos controles internos
· Quantidade de ações de melhoria dos controles internos
· Quantidade e abrangência das auto-avaliações dos controles internos





OBJETIVOS DE CONTROLE DETALHADOS

ME2 Monitorar e Avaliar os Controles Internos

ME2.1 Monitoramento da Estrutura de Controles Internos
Monitorar, comparar e aprimorar o ambiente e a estrutura de controles de TI continuamente para atingir os objetivos organizacionais.

ME2.2 Revisão Gerencial
Monitorar e avaliar a eficiência e a eficácia das revisões gerenciais dos controles internos de TI.

ME2.3 Exceções aos Controles
Identificar todas as exceções aos controles, assegurar que seja feita uma análise crítica das causas-raiz. Encaminhar e reportar adequadamente as exceções às partes interessadas. Realizar as ações corretivas necessárias.

ME2.4 Autoavaliação dos Controles
Avaliar o grau de abrangência e a efetividade dos controles internos da administração sobre os processos, as políticas e os contratos de TI através de um programa contínuo de autoavaliação.

ME2.5 Garantia dos Controles Internos
Conforme a necessidade, obter maior garantia da abrangência e da eficácia dos controles internos através de avaliações de terceiros.

ME2.6 Controles Internos Aplicados a Terceiros
Avaliar o status dos controles internos aplicados a cada fornecedor de serviço. Certificar-se de que fornecedores externos de serviço atendem às exigências legais e regulatórias e às obrigações contratuais.

ME2.7 Ações Corretivas
Identificar, iniciar, monitorar e implementar ações corretivas com base nas avaliações e nos relatórios de controle.

Diretrizes de Gerenciamento

ME2 Monitorar e Avaliar os Controles Internos

Origem	Entrada
AI7	Monitoramento dos controles internos;
ME1	Relatórios de desempenho de processos

Saída	Destino						
Relatórios sobre a eficácia dos controles de TI	PO4	PO6	ME1	ME4			

Tabela RACI

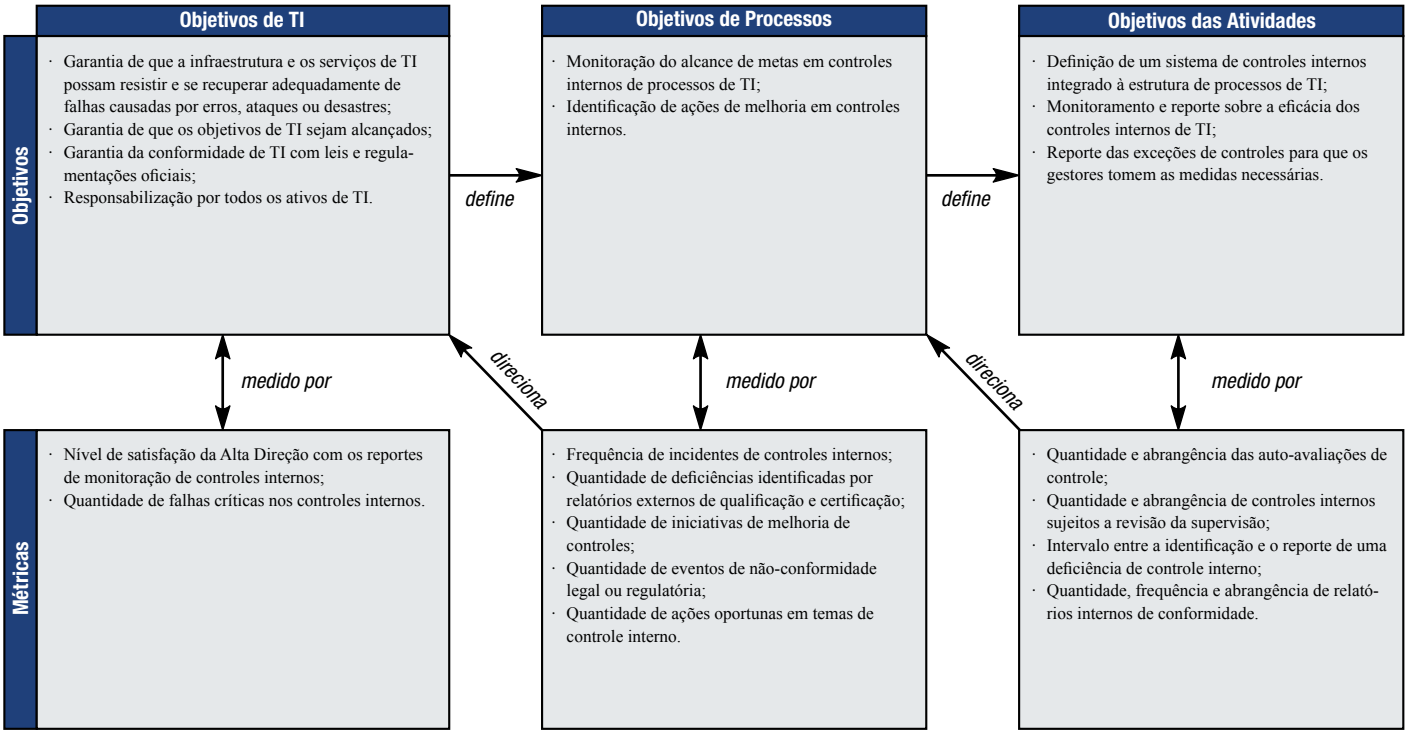
Funções

Atividades

Atividades	Conselho de Administração	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Monitorar e controlar atividades de controle interno de TI;					A		R		R	R		R
Monitorar o processo de auto-avaliação;				I	A		R		R	R		C
Monitorar o desempenho de revisões, auditorias e avaliações independentes;				I	A		R		R	R		C
Monitorar o processo para auditar controles operados por terceiros;		I	I	I	A		R		R	R		C
Monitorar o processo para identificar e avaliar criticamente exceções de controles;		I	I	I	A	I	R		R	R		C
Monitorar o processo para identificar e corrigir exceções de controles;		I	I	I	A	I	R		R	R		C
Reportar a partes interessadas chave	I	I	I		A/R							I

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

ME2 Monitorar e Avaliar os Controles Internos

O gerenciamento do processo de ***"Monitorar e Avaliar os Controles Internos"*** que satisfaça ao requisito do negócio para a TI de ***"assegurar que os objetivos de TI sejam atingidos e assegurar a conformidade com as leis e os regulamentos relacionados a TI"*** é:

0 Inexistente quando
A organização não tem procedimentos para monitorar a eficácia dos controles internos. Não existem métodos de relatórios gerenciais de controles internos. Há uma falta generalizada de conscientização sobre a garantia dos controles internos e a segurança operacional de TI. A administração e os funcionários têm uma completa falta de conscientização em relação a controles internos.

1 Inicial/ *Ad hoc* quando
A Direção reconhece a necessidade de gerenciamento e controle de TI. A adequação dos controles internos é avaliada de forma *ad hoc* com base em habilidades e experiências individuais. A Direção de TI não atribuiu formalmente a responsabilidade pela eficácia do monitoramento dos controles internos. Avaliações dos controles internos de TI são realizadas como parte das auditorias financeiras tradicionais, com um conjunto de metodologias e técnicas que não refletem as necessidades da área de TI.

2 Repetível porém Intuitivo quando
A organização usa relatórios informais de controles para iniciar ações corretivas. A avaliação dos controles internos é dependente da competência técnica de pessoas-chave. A organização tem maior consciência do monitoramento dos controles internos. A Direção de TI monitora rotineiramente a eficácia do que ela considera ser os controles internos críticos. Ferramentas e metodologias para monitorar os controles internos estão começando a ser utilizadas, porém de forma não planejada. Os fatores de risco específicos do ambiente de TI são identificados com base nas habilidades das pessoas.

3 Processo Definido quando
A Direção apoia e tem institucionalizado o monitoramento dos controles internos. Políticas e procedimentos foram desenvolvidos para avaliar e relatar as atividades de monitoramento dos controles internos. Foi definido um programa de educação e treinamento para o monitoramento dos controles internos. Foi definido um processo de autoavaliações e revisões da garantia de eficácia dos controles internos, com os papéis claramente definidos para os gestores dos processos de negócios e os gestores de TI. Ferramentas estão sendo utilizadas, porém não necessariamente estão integradas a todos os processos. Políticas de avaliação de risco dos processos de TI estão sendo utilizadas nas estruturas de controle desenvolvidas especificamente para a organização de TI. Estão definidos riscos específicos dos processos e políticas de mitigação de risco.

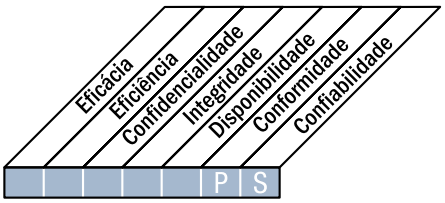
4 Gerenciado e Mensurável quando
A Direção implementou uma estrutura para o monitoramento dos controles internos de TI. A organização estabeleceu limites de tolerância para o processo de monitoramento de controles internos. Foram implementadas ferramentas para padronizar as avaliações e detectar exceções de controle automaticamente. Existe uma área formal de controle interno de TI, com profissionais especializados e certificados que utilizam uma estrutura de controle formal endossada pela alta administração. Uma equipe de TI tecnicamente qualificada participa rotineiramente das avaliações dos controles internos. Existe uma base de conhecimento de métricas com informações históricas sobre o monitoramento dos controles internos. São feitas avaliações estruturadas do monitoramento dos controles internos.

5 Otimizado quando
A Direção estabeleceu um programa corporativo de melhoria contínua que leva em consideração as lições aprendidas e as melhores práticas de monitoramento dos controles internos. A organização utiliza ferramentas integradas e atualizadas quando apropriado, que permite a efetiva avaliação dos controles críticos de TI e a rápida detecção dos incidentes de monitoramento dos controles de TI. Está implementado o compartilhamento de conhecimento da área de TI. Comparação *(benchmarking)* com base nos padrões e nas melhores práticas de mercado é formalizada.

Descrição de Processo

ME3 Assegurar a Conformidade com Requisitos Externos

A supervisão eficaz da conformidade requer o estabelecimento de um processo de revisão para assegurar a conformidade com as leis e regulamentações e os requisitos contratuais. Esse processo inclui identificar os requisitos de conformidade, otimizar e avaliar a resposta, assegurar que os requisitos sejam atendidos e integrar os relatórios de conformidade de TI com os das áreas de negócios.



Controle sobre o seguinte processo de TI:

Assegurar a conformidade com requisitos externos

que satisfaça aos seguintes requisitos do negócio para a TI:

estar em conformidade com leis, regulamentações e requisitos contratuais

com foco em:

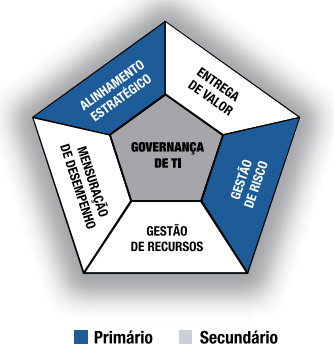
identificar todas as leis, regulamentações e contratos aplicáveis e o respectivo nível necessário de conformidade de TI e otimizar processos de TI para reduzir o risco de não-conformidade

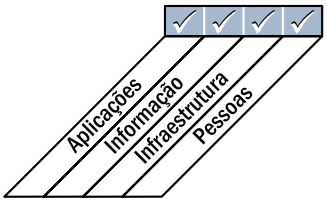
é alcançado por:

- Identificação dos requisitos legais, regulatórios e contratuais relacionados à TI
- Avaliação do impacto dos requisitos de conformidade
- Monitoramento e geração de relatórios sobre a conformidade com esses requisitos

e medido por:

- Custo da não-conformidade da TI, incluindo multas e penalidades
- Intervalo entre a identificação dos problemas de conformidade externa e sua resolução
- Frequência das revisões de conformidade





OBJETIVOS DE CONTROLE DETALHADOS

ME3 Assegurar a Conformidade com Requisitos Externos

ME3.1 Identificação dos Requisitos de Conformidade com Leis, Regulamentações e Contratos Externos
Continuamente identificar as exigências de leis, regulamentos e contratos locais e internacionais que precisam ser atendidos para a inclusão em políticas, padrões, procedimentos e metodologias de TI.

ME3.2 Otimização da Resposta aos Requisitos Externos
Revisar e ajustar políticas, padrões, procedimentos e metodologias de TI para assegurar que os requisitos legais, regulatórios e contratuais sejam atendidos e comunicados.

ME3.3 Avaliação da Conformidade com Requisitos Externos
Confirmar a conformidade de políticas, padrões, procedimentos e metodologias de TI com os requisitos legais e regulatórios.

ME3.4 Assegurar a Conformidade
Obter e assegurar a conformidade e adesão a todas as políticas internas derivadas de diretrizes legais internas ou externas e requisitos regulatórios ou contratuais externos, confirmando que ações corretivas foram tomadas oportunamente para resolver quaisquer desvios de conformidade pelos proprietário do processo.

ME3.5 Informes Integrados
Integrar os informes de TI sobre requisitos legais, regulatórios e contratuais aos informes similares de outras funções do negócio.

Diretrizes de Gerenciamento

ME3 Assegurar a Conformidade com Requisitos Externos

Origem	Entrada
*	Requisitos de conformidade legal e regulatória;
PO6	Políticas de TI

*Origem externa ao CobiT

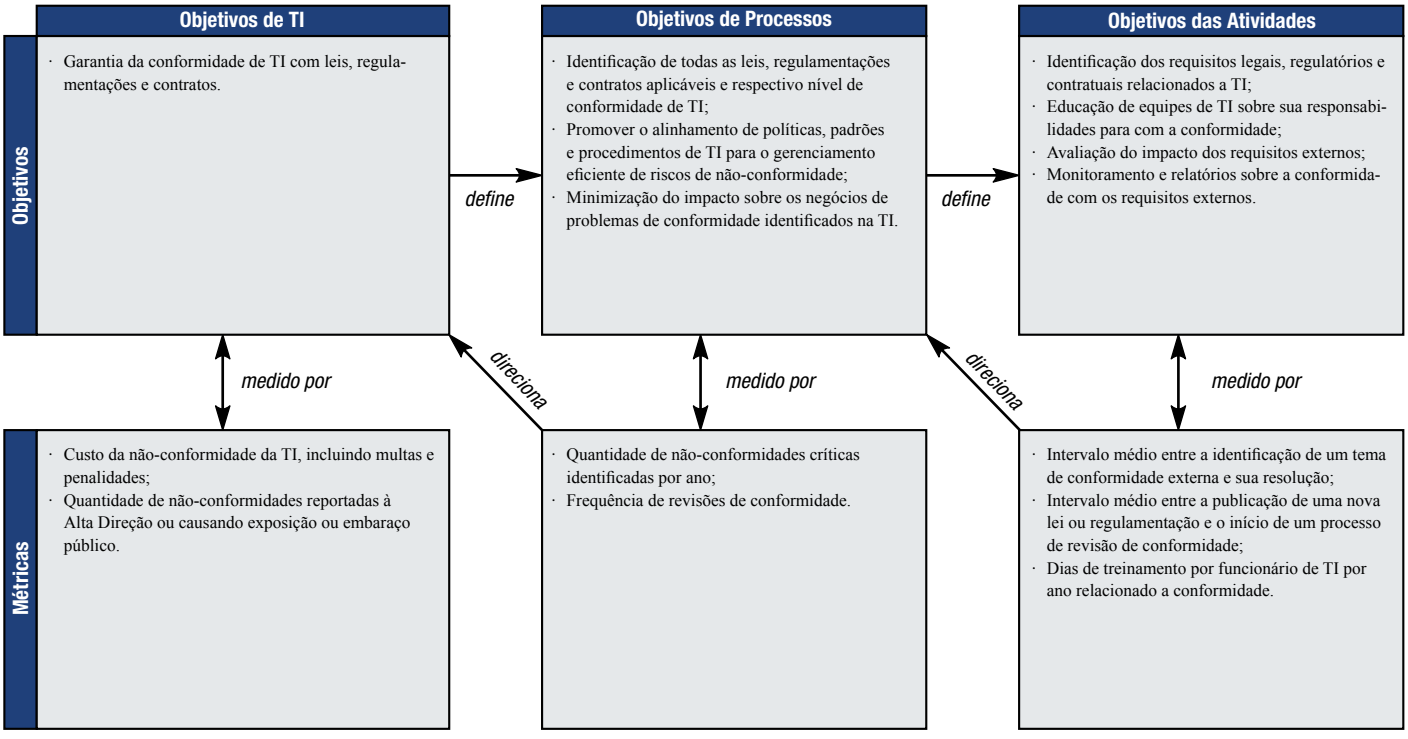
Saída	Destino						
Catálogo de requisitos legais e regulatórios relacionados com a entrega de serviços de TI;	PO4	ME4					
Relatórios sobre a conformidade das atividades de TI com requisitos externos legais e regulatórios	ME1						

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança	Conselho de Administração
Definir e executar um processo para identificar requisitos legais, contratuais, de políticas e regulatórios;				A/R	C	I	I	I	C	I	R	
Avaliar a conformidade das atividades de TI com as políticas, padrões e procedimentos de TI;	I	I	I	A/R	I	R	R	R	R	R	R	I
Reportar a conformidade positiva de atividades de TI com as políticas, padrões e procedimentos de TI;				A/R	C	C	C	C	C	C	R	
Fornecer dados para o alinhamento de políticas, padrões e procedimentos de TI em resposta a requisitos de conformidade;				A/R	C	C	C	C	C		R	
Integrar os relatórios de TI sobre requisitos regulatórios com produtos similares de outras áreas corporativas				A/R		I	I	I	R	I	R	

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

ME3 Assegurar a Conformidade com Requisitos Externos

O gerenciamento do processo de ***"assegurar a conformidade com requisitos externos"*** que satisfaça ao requisito do negócio para a TI de ***"estar em conformidade com leis, regulamentações e requisitos contratuais"*** é:

0 Inexistente quando
Há pouca consciência sobre requisitos externos que afetam a TI, sem que haja processo de conformidade com os requisitos contratuais, legais e regulatórios.

1 Inicial/ *Ad hoc* quando
Há consciência do impacto dos requisitos legais, regulatórios e contratuais na organização. Processos informais são adotados para manter a conformidade, porém somente quando surge a necessidade em novos projetos ou em resposta às auditorias ou análises críticas.

2 Repetível, porém Intuitivo quando
Há entendimento da necessidade de aderir aos requisitos externos e isso é comunicado. Onde a conformidade tornou-se um requisito recorrente, como no caso de regulamentações financeiras ou leis de privacidade, foram desenvolvidos procedimentos específicos de conformidade que são seguidos anualmente. Entretanto, não há uma abordagem padronizada. Existe grande confiança no conhecimento e na responsabilidade das pessoas, e existe a probabilidade de erros. Há treinamento informal sobre requisitos externos e aspectos de conformidade.

3 Processo Definido quando
Políticas, procedimentos e processos foram desenvolvidos, documentados e comunicados para assegurar a conformidade com as obrigações legais, contratuais e regulatórias, porém nem sempre podem ser cumpridos integralmente e podem estar desatualizados ou ser inviáveis. Há pouco monitoramento, e existem requisitos de conformidades que não foram tratados. É fornecido treinamento sobre os requisitos legais e regulatórios externos que afetam a organização e os processos de conformidade definidos. Existem contratos *pro forma* e processos de cunho legal padronizados que visam minimizar os riscos associados às responsabilidades contratuais.

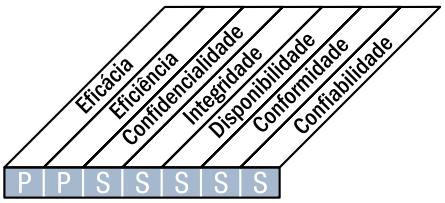
4 Gerenciado e Mensurável quando
Há um completo entendimento das questões e exposições provenientes dos requisitos externos e da necessidade de assegurar a conformidade em todos os níveis. Há um esquema de treinamento formal que assegura que toda a equipe esteja consciente de suas obrigações de conformidade. As responsabilidades são claras e a propriedade dos processos é entendida. O processo inclui a revisão do ambiente para identificar requisitos externos e mudanças constantes. Há um mecanismo implementado para monitorar a não-conformidade com os requisitos externos, reforçar as práticas internas e implementar ações corretivas. Problemas de não-conformidade são analisados em sua causa-raiz de uma forma padronizada, com o objetivo de identificar soluções sustentáveis. Boas práticas internas e padronizadas são utilizadas para suprir necessidades específicas, como regulamentações vigentes e contratos de serviço recorrentes.

5 Otimizado quando
Há um processo bem organizado, eficaz e obrigatório de adesão aos requisitos externos com base em uma função central única que fornece orientação e coordenação para a organização inteira. Há vasto conhecimento dos requisitos externos aplicáveis, inclusive de tendências futuras e mudanças previstas, assim como da necessidade de novas soluções. A organização participa de fóruns de discussão externos com grupos ligados ao segmento e sujeitos às respectivas regulamentações para entender a influência dos requisitos externos que os afetam. Melhores práticas foram desenvolvidas, assegurando a conformidade eficaz com os requisitos externos, com casos raros de exceção. Existe um sistema de rastreabilidade central e global na organização, permitindo à direção documentar o fluxo de trabalho, avaliar e melhorar a qualidade e a eficácia do processo de monitoramento da conformidade. Um processo de autoavaliação da conformidade com os requisitos externos está implementado e foi refinado no nível de boas práticas. O estilo de gestão e a cultura de conformidade da organização são suficientemente fortes, e os processos são suficientemente desenvolvidos para que o treinamento seja limitado a novas equipes e sempre que houver mudanças significativas.

DESCRIÇÃO DE PROCESSO

ME4 Prover Governança de TI

O estabelecimento de uma efetiva estrutura de governança envolve a definição das estruturas organizacionais, dos processos, da liderança, dos papéis e respectivas responsabilidades para assegurar que os investimentos corporativos em TI estejam alinhados e sejam entregues em conformidade com as estratégias e os objetivos da organização.



Controle sobre o seguinte processo de TI:

Prover Governança de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

integrar a governança de TI aos objetivos de governança corporativa e ter conformidade com leis, regulamentações e contratos

com foco em:

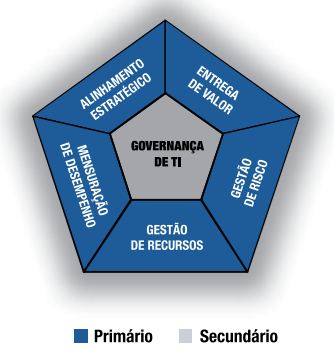
preparar relatórios gerenciais sobre a estratégia, o desempenho e os riscos de TI e atender aos requisitos de governança em alinhamento com as diretrizes da Alta Direção

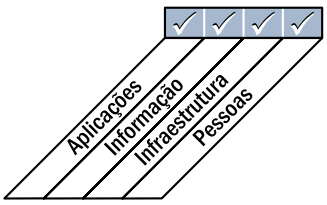
é alcançado por:

· Estabelecimento de uma estrutura de governança de TI integrada à governança corporativa
· Auditoria independente do status da governança de TI

e medido por:

· Frequência dos relatórios gerenciais sobre TI para as partes interessadas (inclusive maturidade)
· Frequência dos relatórios de TI para a Alta Direção (inclusive maturidade)
· Frequência das revisões independentes da conformidade de TI





OBJETIVOS DE CONTROLE DETALHADOS

ME4 Prover Governança de TI

ME4.1 Estabelecimento de uma Estrutura de Governança de TI
Definir, estabelecer e alinhar a estrutura de governança de TI com a governança organizacional e o ambiente de controle. Basear a estrutura em processos e modelos de controle de TI adequados e implementar práticas e responsabilidades claras para evitar falhas de controle interno e supervisão. Certificar-se de que a estrutura de governança de TI assegura a conformidade com leis e regulamentos, está alinhada com as estratégias e os objetivos da organização e corresponde a tais estratégias e objetivos. Produzir relatórios sobre o status da governança de TI e questões relacionadas.

ME4.2 Alinhamento Estratégico
Habilitar a Alta Direção no entendimento das questões estratégicas de TI, tais como os papéis de TI, as capacidades e os conhecimentos tecnológicos. Certificar-se de que há um entendimento compartilhado entre o negócio e a TI quanto ao potencial de contribuição de TI com a estratégia de negócio. Trabalhar com o conselho diretor para definir e implementar as estruturas de governança, como um comitê de estratégia de TI, para dar direção estratégica ao gerenciamento relativo a TI, assegurando que a estratégia e os objetivos sejam propagados de cima para baixo nas unidades de negócio e nas funções de TI e que o crédito e confiança sejam desenvolvidos entre o negócio e TI. Permitir o alinhamento de TI ao negócio no que tange à estratégia e à operação, incentivando a corresponsabilidade entre o negócio e TI para tomar decisões estratégicas e obter os benefícios dos investimentos em TI.

ME4.3 Entrega de Valor
Gerenciar os programas de investimentos e demais recursos e serviços de TI para assegurar que eles forneçam o maior valor possível no suporte aos objetivos e estratégia do negócio. Assegurar que sejam alcançados os resultados esperados pelo negócio quanto aos investimentos de TI, que o escopo completo de esforços necessários para o alcance desses resultados seja entendido, que estudos de caso abrangentes e consistentes sejam criados e aprovados pelas partes interessadas, que os ativos e investimentos sejam gerenciados durante seus ciclos de vida econômicos, que exista o gerenciamento ativo da realização dos benefícios (como contribuição com os novos serviços, ganhos de eficiência e resposta rápida para as demandas do cliente). Impor uma abordagem disciplinada de gerenciamento de portfólio, programas e projetos, insistindo que o negócio tenha responsabilidade sobre todos os investimentos de TI e assegurando que a TI otimize os custos da disponibilização dos serviços e da capacidades da TI.

ME4.4 Gerenciamento de Recursos
Supervisionar o investimento, o uso e a alocação dos recursos de TI por meio de avaliações periódicas das iniciativas e operações de TI, visando assegurar a existência recursos suficientes e o alinhamento com objetivos estratégicos e necessidades de negócios atuais e futuras.

ME4.5 Gestão de Riscos
Trabalhar com o conselho diretor para definir o apetite corporativo por riscos de TI e obter uma razoável segurança de que as práticas de gerenciamento de riscos de TI são adequadas para assegurar que os riscos atuais de TI não excedem o apetite de risco da Alta Direção. Integrar as responsabilidades de gerenciamento de riscos com a organização, assegurando que as áreas de negócios e TI regularmente avaliem e reportem os riscos relacionados a TI e seus impactos e que a posição dos riscos de TI da organização seja transparente para todas as partes interessadas.

ME4.6 Medição de Desempenho
Confirmar se os objetivos acordados de TI foram atingidos ou excedidos ou se o progresso na direção dos objetivos de TI atende as expectativas. Quando os objetivos acordados não foram atingidos ou o progresso não foi como esperado, revisar as ações de remediação da gerência. Reportar para a Alta Direção os portfólios, programas e desempenho de TI relevantes, suportados por relatórios que permitam à Alta Direção revisar o progresso da organização no que diz respeito aos objetivos definidos.

ME4.7 Avaliação Independente
Obter avaliação independente (interna ou externa) sobre a conformidade de TI com leis e regulamentos relevantes, com políticas padrões e procedimentos organizacionais, com práticas geralmente aceitas e a efetiva e eficiente performance de TI.

Diretrizes de Gerenciamento

ME4 Prover Governança de TI

Origem	Entrada
PO4	Estrutura de processos de TI;
PO5	Relatórios de custo/benefício;
PO9	Avaliação de riscos e relatórios;
ME2	Relatórios sobre a efetividade dos controles de TI;
ME3	Catálogo de requisitos legais e regulatórios relacionados com a entrega de serviços de TI

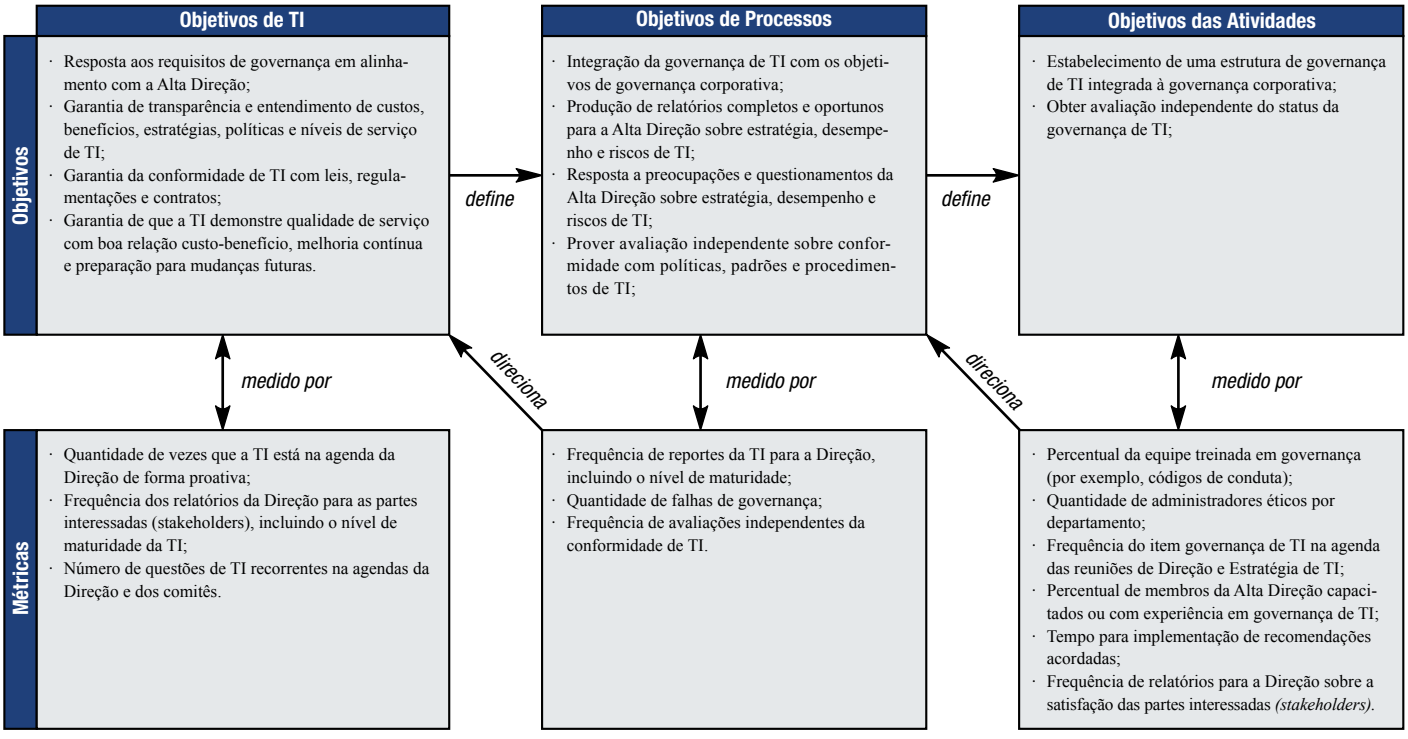
Saída	Destino						
Melhorias na estrutura de processos;	PO4						
Relatórios de status de governança de TI;	PO1	ME1					
Resultados de negócio esperados a partir dos investimentos em negócios habilitados por TI;	PO5						
Direcionamento estratégico corporativo para TI;	PO1						
Grau aceitável corporativo de riscos de TI	PO9						

Tabela RACI

Atividades	Conselho de Administração	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Estabelecer supervisão da Alta Direção sobre atividades de TI;	A	R	C	C	C							C
Revisar, endossar, alinhar e comunicar o desempenho, estratégia, gerenciamento de recursos, gerenciamento de riscos de TI com a estratégia de negócio;	A	R	I	I	R							C
Obter avaliação periódica independente sobre desempenho e conformidade com políticas, padrões e procedimentos;	A	R	C	I	C		I	I	I	I	I	R
Resolver questionamentos levantados por avaliações independentes e assegurar a implementação das recomendações acordadas;	A	R	C	I	C		I	I	I	I	I	R
Gerar relatórios sobre a governança de TI	A	C	C	C	R	C	I	I	I	I	I	C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Objetivos e Métricas



MODELO DE MATURIDADE

ME4 Prover Governança de TI

O gerenciamento do processo de ***"Prover Governança de TI"*** que satisfaça ao requisito do negócio para a TI de ***"integrar a governança de TI com os objetivos de governança corporativa e ter conformidade com as leis e as regulamentações"*** é:

0 Inexistente quando
Não existe qualquer processo identificável de governança de TI. A organização nem mesmo reconhece que há uma questão a ser tratada; por isso não há comunicação sobre o assunto.

1 Inicial / *Ad hoc* quando
Há reconhecimento de que existem questões sobre a governança de TI que precisam ser tratadas. Existem abordagens *ad hoc* aplicadas de forma individual ou caso a caso. A abordagem da Direção é reativa, e só existem comunicações inconsistentes e esporádicas sobre as questões e os enfoques para tratá-las. A Direção tem apenas um indicação aproximada de como a TI contribui para o desempenho do negócio. A Direção responde apenas reativamente aos incidentes que têm causado algum prejuízo ou constrangimento à organização.

2 Repetível, porém Intuitivo quando
Há consciência das questões de governança de TI. Atividades de governança de TI e indicadores de desempenho, entre os quais estão o planejamento de TI e os processos de entrega e monitoramento, estão em desenvolvimento. Processos de TI selecionados são identificados para aprimoramento com base nas decisões individuais. A Direção identificou os métodos e técnicas de avaliação e medição da governança de TI, mas o processo não tem sido adotado na organização. A comunicação sobre os padrões e responsabilidades da governança de TI fica a cargo de cada pessoa. As pessoas conduzem os processos de governança dentro de vários processos e projetos de TI. Os processos, as ferramentas e as métricas para avaliar a governança de TI são limitados e podem não ser utilizados em todas as suas capacidades devido à falta de experiência com as funcionalidades.

3 Processo Definido quando
A importância da necessidade da governança de TI é entendida pela Direção e comunicada à organização. É desenvolvido um conjunto básico de parâmetros para os indicadores de governança de TI em que as correlações entre as medições de resultado e os indicadores de desempenho são definidos e documentados. Os procedimentos têm sido padronizados e documentados. A Direção comunicou procedimentos padrão, e o treinamento é estabelecido. Ferramentas têm sido identificadas para auxiliar na supervisão da governança de TI. Painéis de controle *(dashboards)* têm sido definidos como parte do balanced scorecard de TI. Contudo, é deixado a cargo de o indivíduo fazer treinamento, seguir e aplicar os padrões. Os processos podem ser monitorados, porém os desvios que continuam sendo tratados pelas iniciativas de cada indivíduo provavelmente não são detectados pela Direção.

4 Gerenciado e Mensurável quando
Há completo entendimento das questões de governança de TI em todos os níveis. Há um claro entendimento de quem é o cliente, e as responsabilidades são definidas e monitoradas através de acordo de nível de serviço. As responsabilidades são claras, e a propriedade do processo é estabelecida. Os processos de TI e a governança de TI estão alinhados e integrados às estratégias de negócio e de TI. O aprimoramento nos processos de TI baseia-se primeiramente em um entendimento quantitativo, e é possível monitorar e avaliar a conformidade com os procedimentos e as métricas de processo. Todas as partes interessadas no processo estão cientes dos riscos, da importância da TI e das oportunidades que ela pode oferecer. A Direção tem definido tolerâncias sob as quais os processos devem operar. Há um uso limitado, primordialmente tático, da tecnologia, baseado em técnicas maduras e ferramentas de controle padrão. A governança de TI tem sido integrada aos planejamentos estratégico e operacional e aos processos de monitoramento. Os indicadores de desempenho de todas as atividades de governança de TI estão sendo registrados e monitorados, gerando aprimoramentos para toda a empresa. A responsabilidade pelo desempenho dos principais processos é clara, e o gerenciamento é recompensado tendo em vista medidas-chave de desempenho.

5 Otimizado quando
Há um entendimento avançado, que aponta para o futuro, das questões voltadas à governança de TI e suas soluções. O treinamento e a comunicação são sustentados por conceitos e técnicas mais avançados. Os processos têm sido bem refinados no nível de melhores práticas do seu segmento de indústria a partir dos resultados do aprimoramento contínuo e da modelagem de maturidade com outras organizações. A implementação das políticas de TI permite que a organização, as pessoas e os processos tenham rápida adaptação e completa assimilação dos requisitos de governança de TI. Todos os problemas e desvios têm suas causas-raiz analisadas, e ações eficientes são sistematicamente identificadas e executadas. A TI é utilizada de forma otimizada, integrada e extensiva para automatizar o fluxo de trabalho e disponibilizar ferramentas para melhorar a qualidade e a efetividade. Os riscos e retornos dos processos de TI são definidos, balanceados e comunicados por toda empresa. Especialistas externos são agregados, e *benchmarks* são utilizados como guias de orientação. O monitoramento, a autoavaliação e a comunicação sobre as expectativas de governança são difundidos na organização, e há uso otimizado de tecnologia para auxiliar na medição, na análise, na comunicação e no treinamento. A governança corporativa e a governança de TI são estrategicamente correlacionadas, alavancando os recursos humanos, tecnológicos e financeiros para aumentar as vantagens competitivas da organização. As atividades da governança de TI são integradas ao processo de governança corporativa.

Apêndice I
Tabelas Relacionando Objetivos e Processos

Este apêndice apresenta uma visão global de como os objetivos de negócios gerais relacionam-se com os objetivos de TI, os processos de TI e critérios de informação. Existem três tabelas:

1. A primeira tabela mapeia os objetivos de negócios, organizados de acordo com o balanced scorecard, com os objetivos de TI e critérios de informação. Isso ajuda a mostrar para um determinado objetivo de negócio quais os objetivos de TI que normalmente suportam este objetivo. O conjunto de 17 objetivos de negócios não deve ser considerado como uma lista completa de todos os possíveis objetivos de negócios; é uma seleção de objetivos de negócios relevantes que podem ter um claro impacto em TI (objetivos de negócios relacionados a TI).
2. A segunda tabela mapeia os objetivos de TI com os processos de TI do CobiT e com critérios de informação nos quais os objetivos de TI são baseados.
3. A terceira tabela prove um mapa reverso demonstrando para cada processo de TI os respectivos objetivos de TI que eles suportam.

As tabelas ajudam a demonstrar o escopo do CobiT e o relacionamento dos negócios em geral entre o CobiT e os direcionadores de negócios, permitindo que um típico objetivo de negócio relacionado a TI seja mapeado via objetivos de TI aos processos de TI que os suporta. As tabelas são baseadas em objetivos genéricos e deveriam ser usadas como um guia e adaptadas para uma organização específica.

Para prover uma ligação com os critérios de informação usados para requerimentos de negócios na terceira edição do CobiT, as tabelas também contém uma indicação do critério de informação mais importante suportados pelos objetivos de negócios e de TI.

Notas:

1. Os critérios de informações nos gráficos de objetivos de negócios são baseadas na aglomeração do critério para o objetivo de TI relacionado e uma avaliação subjetiva daqueles que são mais relevantes para o objetivo de negócio. Não se tentou indicar qual é primário ou secundário. Essas são apenas indicativos e os usuários podem seguir um processo similar quando estiverem avaliando seus próprios objetivos de negócios.
2. Os critérios de informações primários e secundários apresentados no gráfico de objetivos de TI são baseados na aglomeração do critério para cada processo de TI e uma avaliação subjetiva do que é primário ou secundário para o objetivo de TI, visto que alguns processos tem maior impacto nos objetivos de TI do que outros. Essas são apenas indicativos e os usuários podem seguir um processo similar quando estiverem avaliando seus próprios objetivos de TI.

RELACIONAMENTO DOS OBJETIVOS DE NEGÓCIOS AOS OBJETIVOS DE TI

		Objetivos de Negócios	Objetivos de TI								Critérios de Informação do CobiT						
											Eficácia	Eficiência	Confidencialidade	Integridade	Disponibilidade	Conformidade	Confiabilidade
Perspectiva Financeira	1	Prover um retorno de investimento adequado para os investimentos de TI relacionados aos negócios.	24									✓					
	2	Gerenciar os riscos de negócios relacionados a TI.	2	14	17	18	19	20	21	22			✓	✓	✓		
	3	Aprimorar governança corporativa e transparência.	2	18													✓
Perspectiva do Cliente	4	Aprimorar orientação para clientes e serviços.	3	23							✓						
	5	Oferecer produtos e serviços competitivos.	5	24							✓	✓					
	6	Estabelecer a continuidade e disponibilidade de serviços.	10	16	22	23					✓				✓		
	7	Criar agilidade em responder a requerimentos de negócios que mudam continuamente.	1	5	25						✓	✓					
	8	Atingir otimização dos custos para entrega de serviços.	7	8	10	24						✓					
	9	Obter informações confiáveis e úteis para o processo de decisões estratégicas.	2	4	12	20	26				✓			✓			✓
Perspectiva Interna	10	Aprimorar e manter a funcionalidade dos processos de negócios.	6	7	11						✓	✓					
	11	Reduzir custos de processos.	7	8	13	15	24					✓					
	12	Conformidade com leis externas, regulamentos e contratos.	2	19	20	21	22	26	27				✓			✓	
	13	Conformidade com políticas internas.	2	13									✓			✓	
	14	Gerenciar mudanças de negócios.	1	5	6	11	28				✓	✓					
	15	Aprimorar e manter a operação e produtividade do pessoal.	7	8	11	13					✓	✓					
Perspectiva de Aprendizagem	16	Gerenciar a inovação de produtos e negócios.	5	25	28						✓	✓					
	17	Contratar e manter pessoas habilitadas e motivadas.	9								✓	✓					

RELACIONAMENTO DOS OBJETIVOS DE TI AOS OBJETIVOS DE PROCESSOS

Objetivos de TI		Processos											Critérios de Informação do COBIT						
													Eficácia	Eficiência	Confidencialidade	Integridade	Disponibilidade	Conformidade	Confiabilidade
1	Responder aos requerimentos de negócios de maneira alinhada com a estratégia de negócios.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Responder aos requerimentos de governança em linha com a Alta Direção.	PO1	PO4	PO10	ME1	ME4							P	P					
3	Assegurar a satisfação dos usuários finais com a oferta e níveis de serviços.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Otimizar o uso da informação.	PO2	DS11											S		P			S
5	Criar agilidade para TI.	PO2	PO4	PO7	AI3								P	P		S			
6	Definir como funções de negócios e requerimentos de controles são convertidos em soluções automatizadas efetivas e eficientes.	AI1	AI2	AI6									P	P				S	
7	Adquirir e manter sistemas aplicativos integrados e padronizados.	PO3	AI2	AI5									P	P				S	
8	Adquirir e manter uma infraestrutura de TI integrada e padronizada.	AI3	AI5										S	P					
9	Adquirir e manter habilidades de TI que atendam as estratégias de TI.	PO7	AI5										P	P					
10	Assegurar a satisfação mútua no relacionamento com terceiros.	DS2											P	P	S	S	S	S	S
11	Assegurar a integração dos aplicativos com os processos de negócios.	PO2	AI4	AI7									P	P		S	S		
12	Assegurar a transparência e o entendimento dos custos, benefícios, estratégia, políticas e níveis de serviços de TI.	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Assegurar apropriado uso e a performance das soluções de aplicativos e de tecnologia.	PO6	AI4	AI7	DS7	DS8							P	S					
14	Responsabilizar e proteger todos os ativos de TI.	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Otimizar a infraestrutura, recursos e capacidades de TI.	PO3	AI3	DS3	DS7	DS9							S	P					
16	Reduzir os defeitos e re-trabalhos na entrega de serviços e soluções.	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Proteger os resultados alcançados pelos objetivos de TI.	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Estabelecer claramente os impactos para os negócios resultantes de riscos de objetivos e recursos de TI.	PO9											S	S	P	P	P	S	S
19	Assegurar que informações confidenciais e críticas são protegidas daqueles que não deveriam ter acesso às mesmas.	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Assegurar que transações automatizadas de negócios e trocas de informações podem ser confiáveis.	PO6	AI7	DS5									P			P	S	S	
21	Assegurar que os serviços e infraestrutura de TI podem resistir e recuperar-se de falhas devido a erros, ataques deliberados ou desastres.	PO6	AI7	DS4	DS12	DS13	ME2						P	S		S	P		
22	Assegurar o mínimo impacto para os negócios no caso de uma parada ou mudança nos serviços de TI.	PO6	AI6	DS4	DS12								P	S		S	P		
23	Garantir que os serviços de TI ficam disponíveis de acordo com o requerido.	DS3	DS4	DS8	DS13								P	P			P		
24	Aprimorar a eficiência dos custos de TI e sua contribuição para a lucratividade dos negócios.	PO5	DS6										S	P					S
25	Entregar projetos no tempo certo dentro do orçamento e com os padrões de qualidade esperados.	PO8	PO10										P	P		S			S
26	Manter a integridade da informação e da infraestrutura de processamento.	AI6	DS5										P	P		P	P		S
27	Assegurar a conformidade de TI com leis, regulamentos e contratos.	DS11	ME2	ME3	ME4										S	S		P	S
28	Assegurar que TI oferece serviços de qualidade com custo eficiente, contínuo aprimoramento e preparação para mudanças futuras.	PO5	DS6	ME1	ME4								P	P					P

APÊNDICE I

LIGANDO PROCESSO DE TI COM A MATRIZ DE OBJETIVOS DE TI

LIGANDO PROCESSOS DE TI COM A MATRIZ DE OBJETIVOS DE TI

	1 Responder os requerimentos de negócios de maneira alinhada com a estratégia de negócios.	2 Responder aos requerimentos de governança em linha com a Alta Direção.	3 Assegurar a satisfação dos usuários finais com a oferta e níveis de serviços.	4 Otimizar o uso da informação.	5 Criar agilidade para TI.	6 Definir como funções de negócios e requerimentos de controles são convertidos em soluções automatizadas efetivas e eficientes.	7 Adquirir e manter sistemas aplicativos integrados e padronizados.	8 Adquirir e manter uma infraestrutura de TI integrada e padronizada.	9 Adquirir e manter habilidades de TI que atendam as estratégias de TI.	10 Assegurar a satisfação mútua no relacionamento com terceiros.	11 Assegurar a integração dos aplicativos com os processos de negócios.	12 Assegurar a transparência e o entendimento dos custos, benefícios, estratégia, políticas e níveis de serviços de TI.	13 Assegurar apropriado uso e a performance das soluções de aplicativos e de tecnologia.	14 Responsabilizar e proteger todos os ativos de TI.	15 Otimizar a infraestrutura, recursos e capacidades de TI.	16 Reduzir os defeitos e retrabalhos na entrega de serviços e soluções.	17 Proteger o atingimento dos objetivos de TI.	18 Estabelecer claramente os impactos para os negócios resultantes de riscos de objetivos e recursos de TI.	19 Assegurar que informações confidenciais e críticas são protegidas daqueles que não deveriam ter acesso às mesmas.	20 Assegurar que transações automatizadas de negócios e trocas de informações podem ser confiáveis.	21 Assegurar que os serviços e infra-estrutura de TI podem resistir e recuperar-se de falhas devido a erros, ataques deliberados ou desastres.	22 Assegurar o mínimo impacto para os negócios no caso de uma parada ou mudança nos serviços de TI.	23 Garantir que os serviços de TI ficam disponíveis de acordo com o requerido.	24 Aprimorar a eficiência dos custos de TI e sua contribuição com a lucratividade dos negócios.	25 Entregar projetos no tempo certo dentro do orçamento e com os padrões de qualidade esperados.	26 Manter a integridade da informação e da infraestrutura de processamento.	27 Assegurar a conformidade de TI com leis, regulamentos e contratos.	28 Assegurar que TI oferece serviços de qualidade com custo eficiente, contínuo aprimoramento e preparação para mudanças futuras.
Planejar e Organizar																													
PO1 Definir um Plano Estratégico de TI	✓	✓																											
PO2 Definir a Arquitetura da Informação	✓			✓	✓						✓																		
PO3 Determinar o Direcionamento Tecnológico							✓								✓														
PO4 Definir os Processos, a Organização e os Relacionamentos de TI	✓	✓			✓																								
PO5 Gerenciar o Investimento de TI												✓												✓					✓
PO6 Comunicar as Diretrizes e Expectativas da Diretoria												✓	✓						✓	✓	✓	✓							
PO7 Gerenciar os Recursos Humanos de TI					✓				✓																				
PO8 Gerenciar a Qualidade			✓													✓										✓			
PO9 Avaliar e Gerenciar os Riscos de TI														✓			✓	✓											
PO10 Gerenciar Projetos	✓	✓																								✓			
Adquirir e Implementar																													
AI1 Identificar Soluções Automatizadas	✓					✓																							
AI2 Adquirir e Manter Software Aplicativo						✓	✓																						
AI3 Adquirir e Manter Infraestrutura de Tecnologia					✓			✓							✓														
AI4 Habilitar Operação e Uso			✓								✓		✓			✓													
AI5 Adquirir Recursos de TI							✓	✓	✓																				
AI6 Gerenciar Mudanças	✓					✓										✓						✓					✓		
AI7 Instalar e Homologar Soluções e Mudanças	✓										✓		✓			✓				✓	✓								
Entregar e Suportar																													
DS1 Definir e Gerenciar Níveis de Serviços	✓		✓									✓																	
DS2 Gerenciar Serviços Terceirizados			✓							✓		✓																	
DS3 Gerenciar o Desempenho e a Capacidade	✓														✓								✓						
DS4 Assegurar a Continuidade dos Serviços																					✓	✓	✓						
DS5 Assegurar a Segurança dos Sistemas														✓					✓	✓	✓				✓				
DS6 Identificar e Alocar Custos												✓												✓					✓
DS7 Educar e Treinar os Usuários			✓										✓		✓														
DS8 Gerenciar a Central de Serviço e os Incidentes			✓										✓										✓						
DS9 Gerenciar a Configuração														✓	✓														
DS10 Gerenciar Problemas			✓													✓	✓												
DS11 Gerenciar os Dados				✓															✓									✓	
DS12 Gerenciar o Ambiente Físico														✓					✓		✓	✓							
DS13 Gerenciar as Operações			✓																		✓		✓						
Monitorar e Avaliar																													✓
ME1 Monitorar e Avaliar o Desempenho de TI	✓	✓										✓																	
ME2 Monitorar e Avaliar os Controles Internos														✓			✓				✓							✓	
ME3 Assegurar Conformidade Com Requisitos Externos																												✓	
ME4 Prover Governança de TI		✓										✓					✓											✓	✓

Apêndice II

Mapeamento dos processos de TI às áreas de Foco da governança em TI, COSO, Recursos de TI do CobiT e critérios de informação do CobiT

Este apêndice fornece um mapeamento entre os processos de TI do CobiT e as cinco áreas foco de governança de TI, os componentes do COSO, os recursos e critérios de informação de TI. A tabela também fornece um indicador da importância relativa (alto, médio e baixo) baseado no *benchmarking* obtido via CobiT Online. Essa matriz demonstra em uma página e em alto nível como a metodologia do CobiT endereça a governança de TI e os requerimentos do COSO, demonstrando o relacionamento entre os processos de TI e os recursos e critérios de informação de TI. A letra P é usada quando existe uma relação primária e a letra S quando existe somente uma relação secundária. A inexistência de P ou S não significa que não há uma relação, significando apenas que ela é menos importante ou é marginal. Os valores de importância são baseados numa pesquisa e na opinião de especialistas, sedo providas apenas como um guia. Os usuários devem considerar quais os processos que são importantes dentro de suas organizações.

APÊNDICE II - MAPEAMENTO DOS PROCESSOS DE TI ÀS ÁREAS DE FOCO DA GOVERNANÇA EM TI, COSO, RECURSOS DE TI DO COBIT E CRITÉRIOS DE INFORMAÇÃO DO COBIT

		Áreas foco Governança de TI					COSO					Recursos de TI CobiT				Critérios de Informação do CobiT						
	Importância	Alinhamento Estratégico	Entrega de Valor	Gerenciamento de Recursos	Gerenciamento de Riscos	Medição de performance	Ambiente de Controle	Avaliação de Riscos	Controle de Atividades	Informação e Comunicação	Monitoramento	Aplicaticos	Informação	Infraestrutura	Pessoas	Eficácia	Eficiência	Confidencialidade	Integridade	Disponibilidade	Conformidade	Confiabilidade
Planejar e Organizar																						
PO1 Definir um Plano Estratégico de TI	H	P		S	S			P		S	S	✓	✓	✓	✓	P	S					
PO2 Definir a Arquitetura da Informação	L	P	S	P	S				P	P		✓	✓			S	P	S	P			
PO3 Determinar o Direcionamento Tecnológico	M	S	S	P	S			S	P	S		✓		✓		P	P					
PO4 Definir os Processos a Organização e os Relacionamentos de TI	L	S		P	P		P			S	S				✓	P	P					
PO5 Gerenciar o Investimento de TI	M	S	P	S		S		S	P			✓		✓	✓	P	P					S
PO6 Comunicar as Diretrizes e Expectativas da Diretoria	M	P			P		P			P			✓		✓	P					S	
PO7 Gerenciar os Recursos Humanos de TI	L	P		P	S	S	P			S					✓	P	P					
PO8 Gerenciar a Qualidade	M	P	S		S		P		P	S	P	✓	✓	✓	✓	P	P		S			S
PO9 Avaliar e Gerenciar os Riscos de TI	H	P			P			P				✓	✓	✓	✓	S	S	P	P	P	S	S
PO10 Gerenciar Projetos	H	P	S	S	S	S	S	S	P		S	✓		✓	✓	P	P					
Adquirir e Implementar																						
AI1 Identificar Soluções Automatizadas	M	P	P	S	S				P			✓		✓		P	S					
AI2 Adquirir e Manter Software Aplicativo	M	P	P		S				P			✓				P	P		S			S
AI3 Adquirir e Manter Infraestrutura de Tecnologia	L			P					P					✓		S	P		S	S		
AI4 Habilitar Operação e Uso	L	S	P	S	S				P	S		✓		✓	✓	P	P		S	S	S	S
AI5 Adquirir Recursos de TI	M		S	P					P			✓	✓	✓	✓	S	P				S	
AI6 Gerenciar Mudanças	H		P	S				S	P		S	✓	✓	✓	✓	P	P		P	P		S
AI7 Instalar e Homologar Soluções e Mudanças	M	S	P	S	S	S			P	S	S	✓	✓	✓	✓	P	S		S	S		
Entregar e Suportar																						
DS1 Definir e Gerenciar Níveis de Serviços	M	P	P	P		P	S		P	S	S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS2 Gerenciar Serviços Terceirizados	L		P	S	P	S	P	S	P		S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS3 Gerenciar o Desempenho e a Capacidade	L	S	S	P	S	S			P		S	✓		✓		P	P				S	
DS4 Assegurar a Continuidade dos Serviços	M	S	P	S	P	S	S		P	S		✓	✓	✓	✓	P	S				P	
DS5 Assegurar a Segurança dos Sistemas	H				P				P	S	S	✓	✓	✓	✓			P	P	S	S	S
DS6 Identificar e Alocar Custos	L		S	P		S			P			✓	✓	✓	✓		P					P
DS7 Educar e Treinar os Usuários	L	S	P	S	S		P			S					✓	P	S					
DS8 Gerenciar a Central de Serviço e os Incidentes	L		P			S	S			P	P	✓			✓	P	P					
DS9 Gerenciar a Configuração	M		P	P	S				P			✓	✓	✓		P	S			S		S
DS10 Gerenciar Problemas	M		P		S	S			P	S	S	✓	✓	✓	✓	P	P			S		
DS11 Gerenciar os Dados	H		P	P	P				P				✓						P			P
DS12 Gerenciar o Ambiente Físico	L			S	P			S	P					✓					P	P		
DS13 Gerenciar as Operações	L			P					P	S		✓	✓	✓	✓	P	P		S	S		
Monitorar e Avaliar																						
ME1 Monitorar e Avaliar o Desempenho de TI	H	S	S	S	S	P				S	P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME2 Monitorar e Avaliar os Controles Internos	M		P		P						P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME3 Assegurar a Conformidade Com Requisitos Externos	H	P			P				P	S	S	✓	✓	✓	✓						P	S
ME4 Prover Governança de TI	H	P	P	P	P	P	P	S		S	P	✓	✓	✓	✓	P	P	S	S	S	S	S

P = Primário S = Secundário

Nota: O mapeamento coso é baseado na metodologia coso original. O mapeamento também se aplica no geral à metodologia integrada - gerenciamento de risco corporativo coso mais recente, que expande conceitos sobre controles internos provendo um enfoque mais robusto e extensivo em aspectos mais amplos do gerenciamento de risco corporativo. Ele não pretende substituir a metodologia original de controles internos do coso, mas ao invés disso, incorpora a metodologia de controles internos. No entanto, os usuários cobit podem escolher referir-se a essa metodologia de gerenciamento de risco corporativo tanto para satisfazer suas necessidades de controle interno como mover-se para um processo de gerenciamento de riscos mais completo.

Apêndice III
Modelo de Maturidade para Controles Internos

Este apêndice fornece um modelo de maturidade genérico demonstrando a situação do ambiente de controle interno e o estabelecimento de controles internos numa empresa. Ele demonstra como o gerenciamento do controle interno e a percepção da necessidade do estabelecimento de melhores controles internos tipicamente desenvolve-se de um nível *ad hoc* para um otimizado. O modelo prove um guia de alto nível para ajudar os usuários CobiT apreciarem o que é requerido para efetivos controles internos em TI e para ajudar a posicionar a empresa na escala de maturidade.

APÊNDICE III - MODELO DE MATURIDADE PARA CONTROLES INTERNOS

Nível de Maturidade	Estágio do Ambiente de Controle Interno	Estabelecimento de Controles Internos
0 Inexistente	Não existe o reconhecimento da necessidade de controles internos. Controles não são parte da cultura ou missão da empresa. Existe um alto risco de deficiências de controles e de incidentes.	Não existe a intenção de avaliar a necessidade de controles internos. Incidentes são tratados quando aparecem.
1 Inicial / *Ad hoc*	Existe algum reconhecimento da necessidade de controles internos. O enfoque com relação a riscos e controles é *ad hoc* e desorganizado, sem comunicação ou monitoramento. Deficiências não são identificadas. Funcionários não estão conscientes de suas responsabilidades.	Não existe a consciência da necessidade da avaliação do que é preciso em termos de controles de TI. Quando é realizado, ocorre somente em base *ad hoc*, num nível superficial e como reação a incidentes significativos. As avaliações tratam somente dos incidentes ocorridos.
2 Repetível, porém Intuitivo	Controles estão em funcionamento mas não são documentados. A sua operação é dependente do conhecimento e da motivação da pessoas. Efetividade não é adequadamente avaliada. Existem muitas fragilidades de controles e elas não são adequadamente tratadas; o impacto pode ser severo. Ações gerenciais para resolver problemas de controles não são priorizadas ou consistentes. Os funcionários podem não estar conscientes de suas responsabilidades.	Avaliações da necessidade de controles ocorrem quando necessário para processos selecionados de TI visando determinar o nível de maturidade atual, o nível que deveria ser atingido e as lacunas existentes. Uma reunião com enfoque informal, envolvendo gerentes de TI e a equipe envolvida no processo é utilizado para definir um enfoque adequado de controles para o processo e para motivar um plano de ação aceito por todos.
3 Processo Definido	Controles estão em funcionamento e são adequadamente documentados. A efetividade operacional é avaliada periodicamente, e existe um número médio de problemas. No entanto, o processo de avaliação não é documentado. Embora a gerência trate a maioria dos problemas de controle de maneira previsível, algumas fragilidades de controle persistem e os impactos podem ainda ser severos. Os funcionários estão conscientes de suas responsabilidades relacionadas a controles. Os processos críticos de TI são identificados com base em direcionadores de valor e riscos. Uma análise detalhada é realizada para identificar os requisitos de controles e das causas das lacunas, bem como para desenvolver oportunidades de aprimoramento. Além das reuniões facilitadas, ferramentas e entrevistas são executadas para suportar as análises e assegurar que os proprietários de processos de TI dominem e direcionem o processo de avaliação e o aprimoramento.	Os processos críticos de TI são identificados com base em direcionadores de valor e riscos. Uma análise detalhada é realizada para identificar os requerimentos de controles e das causas dos gaps, bem como para desenvolver oportunidades de aprimoramento. Em adição a reuniões facilitadas, ferramentas e entrevistas são executadas para suportar as análises e assegurar que os proprietários de processos de TI dominam e direcionam o processo de avaliação e o aprimoramento.
4 Gerenciado e Mensurável	Existe um efetivo ambiente de controles internos e gerenciamento de riscos. Uma avaliação formal e documentada dos controles ocorre frequentemente. Muitos controles são automatizados e regularmente revisados. A gerência provavelmente detecta a maioria dos problemas de controle, mas nem todos os problemas são rotineiramente identificados. Existe um contínuo acompanhamento para solucionar as fragilidades de controles. O uso limitado e tático da tecnologia é aplicado para automatizar os controles.	A criticidade de processos de TI é regularmente definida com total suporte e concordância de proprietários de processos de negócios. A avaliação de requisitos de controles é baseado na política e na maturidade desses processos, seguindo uma análise mensurada envolvendo as partes interessadas chaves. A responsabilidade por essas avaliações é clara e incentivada. Estratégias de aprimoramento são suportadas por propostas de negócios. A performance para atingir os resultados desejados é consistentemente monitorada. Revisões de controle externas são organizadas ocasionalmente.
5 Otimizado	Um programa corporativo de risco e controles proporciona uma contínua e efetiva resolução de questões relacionadas a controles e riscos. O gerenciamento de controles internos e riscos é integrado com as práticas corporativas, suportado por um monitoramento automatizado em tempo real, com uma total responsabilização pelo monitoramento dos controles, gerenciamento de riscos e procedimentos para conformidade. A avaliação dos controles é contínua, baseada na auto-avaliação e análises de lacuna e de causa-raiz. Os funcionários estão proativamente envolvidos no aprimoramento de controles.	Mudanças de negócios consideram a criticidade dos processos de TI e cobrem qualquer necessidade para reavaliar a capacidade de controle do processo. Os proprietários de processos de TI realizam autoavaliações frequentes para verificar se os controles estão no nível correto de maturidade a fim de atingir as necessidades de negócios e consideram os atributos de maturidade para encontrar maneiras de tornar os controles mais eficientes e efetivos. A organização faz comparações com boas práticas externas e procura consultoria externa sobre a efetividade dos controles internos. No caso de processos críticos, são realizadas revisões independentes para prover garantia de que os controles estão no nível desejado de maturidade e funcionam como planejado.

Apêndice IV
CobiT 4.1 Material de Referência Principal

APÊNDICE IV - COBIT 4.1 MATERIAL DE REFERÊNCIA PRINCIPAL

Para as atividades mais recentes de desenvolvimento e atualização do COBIT, uma ampla base de mais de 40 padrões detalhados de TI, metodologias, orientações e boas práticas foram utilizados para garantir que o COBIT trate de todas as áreas de governança e controle de TI de maneira completa.

O COBIT enfatiza o que é necessário para atingir um adequado gerenciamento e controle de TI e por isso está posicionado em um alto nível. Os padrões detalhados e as boas práticas de TI estão situados em um nível mais baixo, descrevendo como gerenciar e controlar detalhes de TI específicos. O COBIT atua como integrador desses diferentes materiais de orientação, resumindo objetivos-chaves em uma metodologia que também se relaciona com os requisitos de governança e de negócios.

Para esta atualização do COBIT (COBIT 4.1), seis dos mais importantes padrões globais, metodologias e práticas relacionados a TI foram utilizados como principais referências para assegurar cobertura, consistência e alinhamento apropriados. São eles:

- COSO:
  Internal Control – Integrated Framework, 1994
  Enterprise Risk Management – Integrated Framework, 2004
- Office of Government Commerce (OGC®):
  IT Infrastructure Library® (ITIL®), 1999-2004
- International Organisation for Standardisation:
  ISO/IEC 27000
- Software Engineering Institute (SEI®):
  SEI Capability Maturity Model (CMM®), 1993
  SEI Capability Maturity Model Integration (CMMI®), 2000
- Project Management Institute (PMI®):
  A Guide to the Project Management Body of Knowledge (PMBOK®), 2004
- Information Security Forum (ISF):
  The Standard of Good Practice for Information Security, 2003

Referências adicionais utilizadas no desenvolvimento do COBIT 4.1 incluem:

- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, IT Governance Institute*, USA, 2006
- *CISA Review Manual*, ISACA, 2006

Apêndice V
Referência Cruzada entre a 3ª Edição do CobiT e o CobiT 4.1

APÊNDICE V - REFERÊNCIA CRUZADA ENTRE A 3ª EDIÇÃO DO COBIT E O COBIT 4.1

ALTERAÇÕES OCORRIDAS NO MODELO

As principais alterações ocorridas no modelo COBIT como resultado da atualização do COBIT 4.0 foram as seguintes:
- O domínio M tornou-se ME para Monitoramento e Avaliação.
- M3 e M4 eram processos de auditoria e não de TI. Eles foram removidos pois eram adequadamente cobertos por outros padrões de auditoria de TI, embora referências foram fornecidas no modelo atualizado para destacar a necessidade de gerenciamento e uso de funções de avaliações.
- ME3 é o processo relacionado a supervisão regulatória, o que antes era coberto pelo PO8.
- ME4 cobre o processo de supervisão da governança de TI, mantendo o propósito do COBIT como metodologia de governança de TI. Por posicionar este processo como o último na cadeia, enfatiza-se o suporte que cada processo prévio fornece para o objetivo final de implementar uma efetiva governança de TI para a organização.
- Com a remoção do PO8 e a necessidade de manter a numeração para o PO9 Avaliação de riscos e o PO10 Gerenciar projetos consistentes com o COBIT 3, o PO8 tornou-se Gerenciar a qualidade (antigo processo PO11). O domínio PO agora tem 10 processos e não 11.
- O domínio AI exigiu duas alterações: a adição de um processo de aquisição e a necessidade de incluir no AI5 os aspectos de gerenciamento de releases. Nesta última alteração, concluiu-se que esse deveria ser o último processo do domínio AI, o qual se o AI7. O espaço que sobrou no AI5 foi usado para adicionar o novo processo de aquisição. O domínio AI agora tem sete processos ao invés de seis.

O COBIT 4.1 é uma atualização incremental do COBIT 4.0 e inclui:
- Uma visão executiva aprimorada
- Explanação dos objetivos e métricas na seção de definição do método
- Melhores definições dos conceitos-chaves. É importante mencionar que a definição de objetivo de controle mudou por se tornar mais uma definição de uma prática de gerenciamento.
- Objetivos de controle aprimorados como resultado de práticas de controles atualizadas e da atividade de desenvolvimento do Val IT. Alguns objetivos de controles foram agrupados e /ou reformulados para evitar a sobreposição e tornar a lista de objetivos de controles um processo mais consistente. Essas alterações resultaram na renumeração dos objetivos de controle restantes. Alguns objetivos de controle foram reformulados para torná-los mais orientados para ação e consistente nas palavras. As revisões incluem:
  - AI5.5 e AI5.6 foram combinados com o AI5.4
  - AI7.9, AI7.10 e AI7.11 foram combinados com o AI7.8
  - ME3 foi revisado para incluir conformidade com requisitos contratuais, além de requisitos legais e regulatórios
- Os controles de aplicativos foram retrabalhados para serem mais efetivos, baseados no trabalho para suportar a efetividade na avaliação e relatórios de controles. Isto resultou em uma lista de seis controles de aplicativos que substituíram os 18 controles de aplicativos do COBIT 4.0, com detalhes adicionais providos no COBIT Control Practices, 2nd Edition.
- A lista de objetivos de negócios e de TI no apêndice I foi aprimorada a partir dos novos entendimentos obtidos durante a pesquisa de validação executada pela University of Antwerp Management School (Bélgica).
- O material destacável foi expandido para prover uma lista de referência rápida dos processos COBIT e o diagrama geral contendo os domínios foi revisado para incluir uma referência aos elementos de controle de processos e aplicativos da metodologia COBIT.
- Melhorias identificadas por usuários COBIT (COBIT 4.0 e COBIT Online) foram revisadas e incorporadas quando apropriado.

OBJETIVOS DE CONTROLE

Como pode ser visto na descrição acima sobre as alterações ocorridas no modelo, e o trabalho para esclarecer manter o foco do conteúdo nos objetivos de controle, a atualização do modelo COBIT mudou consideravelmente os objetivos de controle. Esses componentes foram reduzidos de 215 para 210, pois todo o material genérico foi mantido apenas no nível do modelo e não se repete em cada processo. Além disso, todas as referências a controles de aplicativos foram movidas para o modelo, e objetivos de controles específicos foram agregados em novas definições. Para apoiar atividades de transição em relação aos objetivos de controle, os dois conjuntos de tabelas a seguir mostram uma referência cruzada entre os novos e os antigos objetivos de controles.

DIRETRIZES DE GERENCIAMENTO

Entradas e saídas foram adicionadas para ilustrar o que cada processo necessita de outros processos e o que eles normalmente entregam. Atividades e responsabilidades associadas também foram incluídas. As entradas e os objetivos de atividades substituíram os fatores críticos de sucesso do COBIT 3. As métricas agora são baseadas em um cascateamento consistente dos objetivos de negócios, TI, processos e atividades. As métricas do COBIT 3 também foram revisadas e aprimoradas para torná-las mais representativas e mensuráveis.

COBIT 3ª Edição	COBIT 4.1
PO1 Definição do plano estratégico de TI.	
1.1 TI como parte dos planos de curto e longo prazo da organização	1.4
1.2 Plano de TI de longo prazo	1.4
1.3 Planejamento de longo prazo de TI - enfoque e estrutura	1.4
1.4 Alterações no plano de longo prazo de TI	1.4
1.5 Planejamento de curto-prazo para a função de TI	1.5
1.6 Comunicação de planos de TI	1.4
1.7 Monitoração e avaliação de planos de TI	1.3
1.8 Avaliação dos sistemas atuais	1.3
PO2 Definição da arquitetura de informação.	
2.1 Modelo da arquitetura de informação	2.1
2.2 Dicionário de dados corporativos e regras de sintaxe de dados	2.2
2.3 Esquema de classificação de dados	2.3
2.4 Níveis de segurança	2.3
PO3 Definição do direcionamento tecnológico.	
3.1 Planejamento da infraestrutura tecnológica	3.1
3.2 Monitoração de tendências futuras e regulatórias	3.3
3.3 Contingência da infraestrutura tecnológica	3.1
3.4 Planos de aquisição de *hardware* e *software*	3.1, AI3.1
3.5 Padrões de tecnologia	3.4, 3.5
PO4 Definição da organização de TI e relacionamentos.	
4.1 Planejamento de TI ou comitê de gerenciamento	4.3
4.2 Posicionar a função de TI na organização	4.4
4.3 Revisão dos resultados organizacionais	4.5
4.4 Papéis e responsabilidades	4.6
4.5 Responsabilidade pela avaliação de qualidade	4.7
4.6 Responsabilidade pela segurança lógica e física	4.8
4.7 Propriedade e custódia	4.9
4.8 Propriedade de dados e sistemas	4.9
4.9 Supervisão	4.10
4.10 Segregação de funções	4.11
4.11 Pessoal de TI	4.12
4.12 Descrição de cargos para o pessoal de TI	4.6
4.13 Pessoal-chave de TI	4.13
4.14 Políticas e procedimentos de pessoal contratado	4.14
4.15 Relacionamentos	4.15
PO5 Gerenciamento de investimento de TI.	
5.1 Orçamento anual da operação de TI	5.3
5.2 Monitoração do custo e benefício	5.4
5.3 Justificativa de custo e benefício	1.1, 5.3, 5.4, 5.5
PO6 Comunicar as diretrizes e metas da Diretoria.	
6.1 Informação positiva sobre ambiente de controle	6.1
6.2 Responsabilidade da gerência pelas políticas	6.3, 6.4 6.5
6.3 Comunicação de políticas organizacionais	6.3, 6.4, 6.5
6.4 Política de implementação de recursos	6.4
6.5 Manutenção de políticas	6.3, 6.4, 6.5
6.6 Conformidade com políticas, procedimentos e padrões	6.3, 6.4, 6.5
6.7 Compromisso com qualidade	6.3, 6.4, 6.5
6.8 Política de segurança no ambiente de controle interno	6.2
6.9 Propriedades de direitos intelectuais	6.3, 6.4, 6.5
6.10 Políticas sobre questões específicas	6.3, 6.4, 6.5
6.11 Comunicação para conscientização de segurança de TI	6.3, 6.4, 6.5
PO7 Gerenciamento de recursos humanos.	
7.1 Recrutamento e promoção de funcionários	7.1
7.2 Qualificação de funcionários	7.2
7.3 Papéis e responsabilidades	7.4
7.4 Treinamento de funcionários	7.5
7.5 Treinamento cruzado ou pessoal de *backup*	7.6
7.6 Procedimentos de verificação de antecedentes de pessoal	7.7
7.7 Avaliações de performance de funcionários	7.8
7.8 Alterações no contrato de trabalho e desligamentos	7.8
PO8 Assegurar conformidade com regulamentos externos.	
8.1 Revisão de requisitos externos	ME3.1
8.2 Práticas e procedimentos para conformidade com requisitos externos	ME3.2
8.3 Conformidade com segurança e ergonomia	ME3.1
8.4 Privacidade, proteção intelectual e fluxo de dados	ME3.1
8.5 Comércio eletrônico	ME3.1
8.6 Conformidade com contratos de seguro	ME3.1
PO9 Avaliação de riscos	
9.1 Avaliação de riscos de negócio	9.1, 9.2, 9.4
9.2 Enfoque de avaliação de riscos	9.4
9.3 Identificação de riscos	9.3
9.4 Medição de riscos	9.1, 9.2, 9.3, 9.4
9.5 Plano de ação para riscos	9.5
9.6 Aceitação de riscos	9.5
9.7 Seleção de salvaguardas	9.5
9.8 Compromisso com avaliação de riscos	9.1
PO10 Gerenciamento de Projetos.	
10.1 Metodologia de gerenciamento de projetos	10.2
10.2 Participação da área usuária no início de projetos	10.4
10.3 Participação e responsabilidade do time de projeto	10.8
10.4 Definição de projeto	10.5
10.5 Aprovação de projeto	10.6
10.6 Aprovação de fases de projeto	10.6
10.7 Plano master do projeto	10.7
10.8 Plano de avaliação de sistemas	10.10
10.9 Planejamento de métodos de avaliações	10.12
10.10 Gerenciamento formal dos riscos do projeto	10.9
10.11 Plano de testes	AI7.2
10.12 Plano de treinamento	AI7.1
10.13 Plano de revisão pós implementação	10.14 (parte)
PO11 Gerenciamento de qualidade.	
11.1 Plano geral de qualidade	8.5
11.2 Enfoque QA	8.1
11.3 Planejamento de QA	8.1
11.4 Revisão de QA da aderência a padrões e procedimentos de TI	8.1, 8.2
11.5 Metodologia de desenvolvimento de sistemas (SDLC)	8.2, 8.3
11.6 Metodologia SDLC pra grandes mudanças na tecnologia atual	8.2, 8.3
11.7 Atualizações da metodologia SDLC	8.2, 8.3
11.8 Coordenação e comunicação	8.2
11.9 Metodologia de aquisição e manutenção da infraestrutura de tecnologia	8.2
11.10 Relacionamento da implementação de terceiros	8.2, DS2.3
11.11 Padrões de documentação de programas	AI4.2, AI4.3, AI4.4
11.12 Padrões de testes de programas	AI7.2, AI7.4
11.13 Padrões de testes de sistemas	AI7.2, AI7.4
11.14 Testes paralelo/piloto	AI7.2, AI7.4
11.15 Documentação de testes de sistemas	AI7.2, AI7.4
11.16 Avaliação de QA da aderência a padrões de desenvolvimento	8.2
11.17 Revisão de QA do atingimento dos objetivos de TI	8.2
11.18 Métricas de qualidade	8.6
11.19 Relatórios de revisões de QA	8.2

CobiT 3ª Edição	CobiT 4.1
AI1 Identificação de solução automatizadas.	
1.1 Definição de requisitos de informação	1.1
1.2 Formulação de planos de ação alternativos	1.3, 5.1, PO1.4
1.3 Formulação da estratégia de aquisição	1.3, 5.1 PO1.4
1.4 Requerimentos de serviços de terceiros	5.1, 5.3
1.5 Estudo de viabilidade tecnológica	1.3
1.6 Estudo de viabilidade econômica	1.3
1.7 Arquitetura da informação	1.3
1.8 Relatórios de análise de riscos	3.1, 3.2, 3.3, 5.4
1.9 Controles de segurança eficientes sob o ponto de vista de custos	1.1, 1.2
1.10 Desenho de trilhas de auditoria	1.1, 1.2
1.11 Ergonomia	1.1
1.12 Seleção de *software* de sistemas	1.1, 1.3
1.13 Controles de aquisição	5.1
1.14 Aquisição de produtos de *software*	5.1
1.15 Manutenção de *software* de terceiros	5.4
1.16 Contrato de programação de aplicativos	5.4
1.17 Aceitação de facilidades	5.4
1.18 Aceitação de tecnologia	3.1, 3.2, 3.3, 5.4
AI2 Aquisição e manutenção de *softwares* aplicativos.	
2.1 Métodos de projeto	2.1
2.2 Mudanças relevantes nos sistemas atuais	2.1, 2.2, 2.6
2.3 Aprovação de projeto	2.1
2.4 Definições e documentação de requerimentos de arquivos	2.2
2.5 Especificação de programas	2.2
2.6 Desenho de entrada de dados fonte	2.2

CobiT 3ª Edição	CobiT 4.1
2.7 Definições e documentação de requerimentos de entrada	2.2
2.8 Definições de interface	2.2
2.9 Interface usuários-máquina	2.2
2.10 Definições e documentação de requerimentos de processamento	2.2
2.11 Definições e documentação de requerimentos de saídas	2.2
2.12 Conjunto de controles	2.3, 2.4
2.13 Disponibilidade como fator-chave de desenho	2.2
2.14 Aspectos de integridade de TI na programação de *software* aplicativos	2.3, DS11.5
2.15 Teste de *software* aplicativos	2.8, 7.4
2.16 Material de referência e de suporte para usuários	4.3, 4.4
2.17 Reavaliação do desenho do sistema	2.2
AI3 Aquisição e manutenção da infraestrutura de tecnologia.	
3.1 Avaliações de novos equipamentos e sistemas	3.1, 3.2, 3.3
3.2 Manutenção preventiva de equipamentos	DS13.5
3.3 Segurança de sistemas de *software*	3.1, 3.2, 3.3
3.4 Instalação de sistemas de *software*	3.1, 3.2, 3.3
3.5 Manutenção de sistemas de *software*	3.3
3.6 Controles de mudanças de sistemas de *software*	6.1, 7.3
3.7 Uso e monitoramento de facilidades de sistemas	3.2, 3.3, DS9.3
AI4 Procedimentos de desenvolvimento e manutenção.	
4.1 Requisitos operacionais e nível de serviços	4.1

CobiT 3ª Edição	CobiT 4.1
4.2 Manual de procedimentos de usuários	4.2
4.3 Manual de operação	4.4
4.4 Materiais de treinamento	4.3, 4.4
AI5 Instalação e aceite de sistemas.	
5.1 Treinamento	7.1
5.2 Performance de sistemas aplicativos	7.6, DS3.1
5.3 Plano de implementação	7.2, 7.3
5.4 Conversão de sistemas	7.5
5.5 Conversão de dados	7.5
5.6 Planos e estratégia de testes	7.2
5.7 Alterações de testes	7.4, 7.6
5.8 Critério e performance de testes paralelos e pilotos	7.6
5.9 Teste final de aceite	7.7
5.10 Teste de segurança e validação	7.6
5.11 Testes operacionais	7.6
5.12 Promoção para produção	7.8
5.13 Avaliação do atendimento dos requerimentos de usuários	7.9
5.14 Revisão de pós-implementação pela gerência	7.9
AI6 Gerenciamento de mudanças.	
6.1 Início de requerimento de mudança e controles	6.1, 6.4
6.2 Avaliação de impactos	6.2
6.3 Controle de mudanças	7.9
6.4 Mudanças de emergência	6.3
6.5 Documentação e procedimentos	6.5
6.6 Manutenção autorizada	DS5.3
6.7 Política de liberação de *software*	7.9
6.8 Distribuição de *software*	7.9

CobiT 3ª Edição	CobiT 4.1
DS1 Definição e gerenciamento de níveis de serviços.	
1.1 Estrutura de SLA - Nível de serviço acordado	1.1
1.2 Aspectos de SLAs	1.3
1.3 Procedimentos de *performance*	1.1
1.4 Monitoramento e relatórios	1.5
1.5 Revisão de SLAs e contratos	1.6
1.6 Itens modificáveis	1.3
1.7 Programa de aprimoramento de serviços	1.6
DS2 Gerenciamento de serviços de terceiros.	
2.1 Interface de fornecedores	2.1
2.2 Relacionamento de proprietários	2.2
2.3 Contratos com terceiros	AI5.2
2.4 Qualificação de terceiros	AI5.3
2.5 Contratos de terceirização	AI5.2
2.6 Continuidade de serviços	2.3
2.7 Relacionamentos de segurança	2.3
2.8 Monitoramento	2.4

CobiT 3ª Edição	CobiT 4.1
DS3 Gerenciamento de capacidade e performance.	
3.1 Requisitos de disponibilidade e performance	3.1
3.2 Plano de disponibilidade	3.4
3.3 Monitoramento e relatórios	3.5
3.4 Ferramentas de modelagem	3.1
3.5 Gerenciamento de performance proativo	3.3
3.6 Previsão de carga de trabalho	3.3
3.7 Gerenciamento de capacidade de recursos	3.2
3.8 Disponibilidade de recursos	3.4
3.9 Agendamento de recursos	3.4
DS4 Assegurar continuidade de serviços.	
4.1 Estrutura de continuidade de TI	4.1
4.2 Filosofia e estratégia do plano de continuidade de TI	4.1
4.3 Conteúdo do plano de continuidade de TI	4.2

CobiT 3ª Edição	CobiT 4.1
4.4 Minimização de requisitos de continuidade de TI	4.3
4.5 Manutenção do plano de continuidade de TI	4.4
4.6 Teste de plano de continuidade de TI	4.5
4.7 Treinamento do plano de continuidade de TI	4.6
4.8 Distribuição do plano de continuidade de TI	4.7
4.9 Procedimentos alternativos de *backup* pela área usuária	4.8
4.10 Recursos críticos de TI	4.3
4.11 Local e equipamentos de contingência	4.8
4.12 Instalação externa de armazenagem	4.9
4.13 Procedimentos de recuperação	4.10
DS5 Assegurar segurança dos sistemas.	
5.1 Gerenciamento de medidas de segurança	5.1
5.2 Identificação, autenticação e acesso	5.3

COBIT 3ª Edição	COBIT 4.1
5.3 Segurança no acesso online aos dados	5.3
5.4 Gerenciamento de contas de usuários	5.4
5.5 Gerenciamento da revisão de contas de usuários	5.4
5.6 Controle de usuários de contas de usuários	5.4, 5.5
5.7 Acompanhamento da segurança	5.5
5.8 Classificação de dados	PO2.3
5.9 Gerenciamento da central de identificação e de direitos de acesso	5.3
5.10 Relatórios de violação e atividades de segurança	5.5
5.11 Tratamento de incidentes	5.6
5.12 Revalidação	5.1
5.13 Confiança em contrapartes	5.3, AC6
5.14 Autorização de transações	5.3
5.15 Não repúdio	5.11
5.16 Caminho confiável	5.11
5.17 Proteção das funções de segurança	5.7
5.18 Gerenciamento de chaves criptográficas	5.8
5.19 Prevenção, detecção e correção de *software* malicioso	5.9
5.20 Arquitetura de *firewall* e conexão com redes públicas	5.10
5.21 Proteção de valores eletrônicos	13.4
DS6 Identificação e alocação de custos.	
6.1 Itens cobráveis	6.1
6.2 Procedimentos de custeamento	6.3
6.3 Cobrança de usuários e procedimentos de recuperação	6.2, 6.4
DS7 Educação e treinamento de usuários.	
7.1 Identificação de necessidades de treinamento	7.1
7.2 Organização do treinamento	7.2
7.3 Princípios de segurança e conscientização	PO7.4
DS8 Assistência e aconselhamento a clientes.	
8.1 *Help desk*	8.1, 8.5
8.2 Registro de requisições de clientes	8.2, 8.3, 8.4
8.3 Procedimentos para escalar requisições de clientes	8.3
8.4 Monitoramento de soluções	10.3
8.5 Análise de tendências e relatórios	10.1

COBIT 3ª Edição	COBIT 4.1
DS9 Gerenciamento de configuração.	
9.1 Registro de configuração	9.1
9.2 Documentação inicial da configuração	9.1
9.3 Levantamento da situação atual	9.3
9.4 Controle de configuração	9.3
9.5 *Software* não autorizado	9.3
9.6 Armazenamento de *software*	AI3.4
9.7 Procedimentos de gerenciamento de configuração	9.2
9.8 Responsabilidade por *software*	9.1, 9.2
DS10 Gerenciamento de problemas e incidentes.	
10.1 Sistema de gerenciamento de problemas	10.1, 10.2 10.3, 10.4
10.2 Procedimento de escalação de problemas	10.2
10.3 Acompanhamento de problemas e trilhas de auditoria	8.2, 10.2
10.4 Emergências e autorizações de acessos temporários	5.4, 12.3, ai6.3
10.5 Prioridades de processamento emergencial	10.1, 8.3
DS11 Gerenciamento de dados	
11.1 Procedimentos de preparação de dados	AC1
11.2 Procedimentos de autorização de documentos-fonte	AC1
11.3 Obtenção de dados de documentos-fonte	AC1
11.4 Tratamento de erros de documentos-fonte	AC1
11.5 Retenção de documentos-fonte	DS11.2
11.6 Procedimentos de autorização de entrada de dados	AC2
11.7 Validação da precisão, totalidade e autorização	AC3
11.8 Tratamento de erros de dados de entrada	AC2, AC4
11.9 Integridade do processamento de dados	AC4
11.10 Validação e edição do processamento de dados	AC4
11.11 Tratamento de erros de processamento de dados	AC4
11.12 Tratamento de saídas e retenção	AC5, 11.2
11.13 Distribuição de saídas	AC5, AC6

COBIT 3ª Edição	COBIT 4.1
11.14 Balanceamento e reconciliação de saídas	AC5
11.15 Revisão de erros e tratamento de erros	AC5
11.16 Providências de segurança para relatórios de saídas	11.6
11.17 Proteção de informação sensível durante transmissão e transporte	AC6, 11.6
11.18 Proteção de informação sensível descartada	11.4, AC6
11.19 Gerenciamento de armazenagem	11.2
11.20 Períodos de retenção e termos de armazenamento	11.2
11.21 Sistema de gerenciamento de biblioteca de mídias	11.3
11.22 Responsabilidade pelo gerenciamento de biblioteca de mídias	11.3
11.23 Cópias de segurança *(backup)* e restauração	11.5
11.24 Trabalhos de *backup*	11.4
11.25 Armazenagem de *backup*	4.9, 11.3
11.26 Arquivamento	11.2
11.27 Proteção de mensagens confidenciais	11.6
11.28 Autenticação e integridade	AC6
11.29 Integridade de transações eletrônicas	5.11
11.30 Integridade continua de dados armazenados	11.2
DS12 Gerenciamento de facilidades.	
12.1 Segurança física	12.1, 12.2
12.2 Instalações de TI em local discreto	12.1, 12.2
12.3 Acompanhamento de visitantes	12.3
12.4 Saúde e segurança de pessoal	12.1, 12.5, ME3.1
12.5 Proteção contra fatores ambientais	12.4, 12.9
12.6 Suprimento contínuo de energia	12.5
DS13 Gerenciamento da operação	
13.1 Procedimentos de processamento de operações e manual de instruções	13.1
13.2 Processo de inicialização e outras documentações de operação	13.1
13.3 Agendamento de trabalhos	13.2
13.4 Discrepâncias de agendamento padrão de trabalhos	13.2
13.5 Continuidade de processamento	13.1
13.6 Registro histórico de operação	13.1
13.7 Proteção de formulários especiais e equipamentos de saída	13.4
13.8 Operação remota	5.11

COBIT 3ª Edição	COBIT 4.1
M1 Monitoramento de processos	
1.1 Coleta de dados de monitoramento	1.2
1.2 Avaliação de performance	1.4
1.3 Avaliação de satisfação de cliente	1.2
1.4 Relatórios de gerenciamento	1.5
M2 Avaliação da adequacidade dos controles internos	
2.1 Monitoramento de controles internos	2.2
2.2 Operação adequada de controles internos	2.1
2.3 Nível de reporte de controles internos	2.2, 2.3
M3 Obtenção de avaliação independente	
3.1 Certificação/avaliação independente da segurança e de controles internos de serviços de TI	2.5, 4.7
3.2 Certificação/avaliação independente da segurança e dos controles internos de serviços de terceiros	2.5, 4.7
3.3 Avaliação independente da efetividade de avaliações de serviços de TI	2.5, 4.7
3.4 Avaliação independente da efetividade de avaliações de serviços de terceiros	2.5, 4.7
3.5 Avaliação independente de conformidade com leis, requisitos regulatórios e acordos contratuais	2.5, 4.7
3.6 Avaliação independente de conformidade com leis, requisitos regulatórios e acordos contratuais por terceiros	2.5, 2.6, 4.7
3.7 Competência da função de avaliações independentes	2.5, 4,7
3.8 Envolvimento proativo da auditoria	2.5, 4.7
M4 Providenciar auditoria independente.	
4.1 Definição de responsabilidade	2.5, 4.7
4.2 Independência	2.5, 4.7
4.3 Padrões e ética profissional	2.5, 4.7
4.4 Competência	2.5, 4.7
4.5 Planejamento	2.5, 4.7
4.6 Performance do trabalho de auditoria	2.5, 4.7
4.7 Relatórios	2.5, 4.7
4.8 Atividades de acompanhamento	2.5, 4.7

COBIT 3ª Edição	COBIT 4.1
PO1 Definição do plano estratégico de TI.	
1.1 Gerenciamento de valor de TI	5.3
1.2 Alinhamento negócios - TI	Novo
1.3 Avaliações da capacidade e da performance atuais	1.7, 1.8
1.4 Plano estratégico de TI	1.1, 1.2, 1.3, 1.4, 1.6, AI1.2, AI1.3
1.5 Planos táticos de TI	1.5
1.6 Gerenciamento do portfólio de TI	Novo
PO2 Definição da arquitetura de informação	
2.1 Modelo da arquitetura de informação corporativa	2.1
2.2 Dicionário de dados corporativos e regras de sintaxe de dados	2.2
2.3 Esquema de classificação de dados	2.3, 2.4, DS5.8
2.4 Gerenciamento da integridade	Novo
PO3 Definição do direcionamento tecnológico	
3.1 Planejamento do direcionamento tecnológico	3.1, 3.3, 3.4
3.2 Planejamento da infraestrutura tecnológica	Novo
3.3 Monitoração de tendências futuras e regulatórias	3.2
3.4 Padrões de tecnologia	3.5
3.5 Conselho deliberativo de arquitetura de TI	3.5
PO4 Definição de processos, organização e relacionamentos de TI	
4.1 Estrutura de processos de TI	Novo
4.2 Comitê Estratégico de TI	Novo
4.3 Comitê Executivo de TI	4.1
4.4 Posicionamento organizacional da área de TI	4.2
4.5 Estrutura Organizacional de TI	4.3
4.6 Estabelecimento de papéis e responsabilidades	4.4, 4.12
4.7 Responsabilidade pela garantia de qualidade de TI	4.5
4.8 Responsabilidade por riscos, segurança e conformidade	4.6

COBIT 3ª Edição	COBIT 4.1
4.9 Proprietários de dados e sistemas	4.7, 4.8
4.10 Supervisão	4.9
4.11 Segregação de Funções	4.10
4.12 Pessoal de TI	4.11
4.13 Pessoal-chave de TI	4.13
4.14 Políticas e procedimentos de pessoal contratado	4.14
4.15 Relacionamento	4.15
PO5 Gerenciamento do investimento em TI	
5.1 Estrutura de gerenciamento financeiro	Novo
5.2 Priorização dentro do orçamento de TI	Novo
5.3 Orçamento de TI	5.1, 5.3
5.4 Gerenciamento de custos	5.2, 5.3
5.5 Gerenciamento de benefícios	5.3
PO6 Comunicar as diretrizes e metas da Diretoria	
6.1 Políticas e ambiente de controle de TI	6.1
6.2 Riscos corporativos e estrutura de controle de TI	6.8
6.3 Gerenciamento de políticas de TI	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 Implementação de políticas, padrões e procedimentos	6.2, 6.3, 6.4, 6.5, 6.6, 6.7 6.9, 6.10, 6.11
6.5 Comunicação das diretrizes e objetivos de TI	6.2, 6.3, 6.5 6.6, 6.7, 6.9, 6.10, 6.11
PO7 Gerenciamento de recursos humanos de TI	
7.1 Recrutamento e retenção de pessoal	7.1
7.2 Competências do pessoal	7.2
7.3 Definição de papéis do pessoal	Novo
7.4 Treinamento do pessoal	7.3, DS7.3
7.5 Dependência de indivíduos	7.4
7.6 Procedimentos de liberação de pessoal	7.5
7.7 Avaliações de performance de funcionários	7.6
7.8 Mudança de trabalho e desligamento	7.7, 7.8
PO8 Gerenciamento de Qualidade	
8.1 Sistema de gerenciamento de qualidade	11.2, 11.3 11.4

COBIT 3ª Edição	COBIT 4.1
8.2 Padrões e práticas de qualidade de TI	11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.16, 11.17, 11.19
8.3 Padrões de desenvolvimento e aquisições	11.5, 11.6, 11.7
8.4 Foco no cliente	Novo
8.5 Aprimoramento contínuo	Novo
8.6 Medição, monitoramento e revisão da qualidade	11.18
PO9 Avaliação e gerenciamento de riscos de TI	
9.1 Estrutura de gerenciamento de riscos de TI	9.1, 9.4, 9.8
9.2 Estabelecimento do contexto de risco	9.1, 9.4
9.3 Identificação de eventos	9.3, 9.4
9.4 Avaliação de riscos	9.1, 9.2, 9.4
9.5 Resposta ao risco	9.5, 9.6, 9.7
9.6 Manutenção e monitoramento do plano de ação de risco	Novo
PO10 Gerenciar projetos	
10.1 Estrutura de gestão de programas	Novo
10.2 Estrutura de gerenciamento de projetos	10.1
10.3 Enfoque de gerenciamento de projetos	Novo
10.4 Comprometimento das partes interessadas	10.2
10.5 Declaração do escopo do projeto	10.4
10.6 Fase de início de projeto	10.5, 10.6
10.7 Plano integrado de projeto	10.7
10.8 Recursos do projeto	10.3
10.9 Gerenciamento de riscos de projeto	10.10
10.10 Plano de qualidade de projeto	10.8
10.11 Controle de mudança de projeto	Novo
10.12 Planejamento de projeto de validação	10.9
10.13 Medição de desempenho, monitoramento e reporte do Projeto	Novo
10.14 Conclusão do Projeto	10.13 (parte)

COBIT 3ª Edição	COBIT 4.1
AI1 Identificar solução automatizadas.	
1.1 Definição e manutenção de requisitos técnicos e funcionais de negócio	1.1, 1.9, 1.10, 1.11, 1.12
1.2 Relatório de análise de risco	1.8, 1.9, 1.10
1.3 Estudo de viabilidade e formulação de ações alternativas	1.3, 1.7, 1.12
1.4 Decisão e aprovação de requerimentos e estudo de viabilidade	Novo
AI2 Adquirir e manter *software* aplicativo	
2.1 Projeto em nível macro	2.1, 2.2
2.2 Projeto detalhado	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 Controle e auditabilidade de aplicativos	2.12, 2.14
2.4 Segurança e disponibilidade de aplicativos	2.12
2.5 Configuração e implementação de *software* aplicativo adquirido	Novo
2.6 Principais atualizações dos sistemas existentes	2.2
2.7 Desenvolvimento de *software* aplicativo	Novo
2.8 Garantia de qualidade de *software*	2.15
2.9 Gestão dos requisitos das aplicações	Novo
2.10 Manutenção de *software* aplicativo	Novo

COBIT 3ª Edição	COBIT 4.1
AI3 Adquirir e manter infraestrutura de tecnologia	
3.1 Plano de aquisição de infraestrutura tecnológica	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 Proteção e disponibilidade de infraestrutura de recurso	1.18, 3.1, 3.3, 3.4, 3.7
3.3 Manutenção da infraestrutura	1.18, 3.1, 3.3, 3.4, 3.5, 3.7
3.4 Viabilidade do ambiente de teste	Novo
AI4 Habilitar operação e uso	
4.1 Planejamento para soluções operacionais	4.1
4.2 Transferência de conhecimento ao gerenciamento do negócio	PO11.11, 4.2
4.3 Transferência de conhecimento aos usuários finais	PO11.11, 2.16, 4.4
4.4 Transferência de conhecimento às equipes de operações e suporte	PO11.11, 2.16, 4.3, 4.4
AI5 Adquirir recursos de TI	
5.1 Controle de aquisição	1.2, 1.3, 1.13, 1.14
5.2 Gerenciamento de contratos de fornecedores	DS2.3, DS2.5
5.3 Seleção de fornecedores	1.4, DS2.4
5.4 Aquisição de recursos de TI	1.15, 1.16, 1.17, 1.18
AI6 Gerenciar mudanças	
6.1 Padrões e procedimentos de mudança	3.6, 6.1

COBIT 3ª Edição	COBIT 4.1
6.2 Avaliação de impacto, priorização e autorização	6.2
6.3 Mudanças de emergência	DS10.4, 6.4
6.4 Acompanhamento de status e relatórios de mudanças	6.1
6.5 Finalização da mudança e documentação	6.5
AI7 Instalar e homologar soluções e mudanças	
7.1 Treinamento	PO10.11, PO10.12, 5.1
7.2 Plano de teste	PO10.11, PO11.12, PO11.13, PO11.14, PO11.15, 5.3, 5.6
7.3 Plano de implantação	3.6, 5.3
7.4 Ambiente de Teste	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 Conversão de dados e sistemas	5.4, 5.5
7.6 Teste de mudanças	5.2, 5.7, 5.8, 5.10, 5.11
7.7 Teste de aceitação final	5.9
7.8 Promoção para produção	5.12
7.9 Revisão pós-implantação	5.13, 5.14

COBIT 3ª Edição	COBIT 4.1
DS1 Definir e Gerenciar Níveis de Serviço.	
1.1 Estrutura de gestão de níveis de serviço	1.1, 1.3
1.2 Definição de Serviços	Novo
1.3 Acordos de Nível de Serviço	1.2, 1.6
1.4 Acordos de Nível Operacional	Novo
1.5 Monitoramento e Relatório de Realizações de Nível de Serviços	1.4
1.6 Revisão dos Acordos de Nível de Serviços e Contratos	1.5, 1.7
DS2 Gerenciar serviços de terceiros.	
2.1 Identificação do Relacionamento com todos os Fornecedores	2.1
2.2 Gestão do Relacionamento com Fornecedores	2.2
2.3 Gerenciamento de Risco do Fornecedor	PO11.10, 2.6, 2.7
2.4 Monitoramento de Desempenho do Fornecedor	2.8

COBIT 3ª Edição	COBIT 4.1
DS3 Gerenciar capacidade e desempenho.	
3.1 Desempenho e planejamento de capacidade	AI5.2, 3.1 3.4
3.2 Capacidade e desempenho correntes	3.7
3.3 Capacidade e desempenho futuros	3.5, 3.6
3.4 Disponibilidade de recursos de TI	3.2, 3.8, 3.9
3.5 Monitoramento e relatórios	3.3
DS4 Assegurar continuidade de serviços.	
4.1 Estrutura de continuidade	4.1, 4.2
4.2 Planos de continuidade de TI	4.3
4.3 Recursos críticos de TI	4.4, 4.10
4.4 Manutenção do plano de continuidade de TI	4.5
4.5 Teste do plano de continuidade de TI	4.6
4.6 Treinamento do plano de continuidade de TI	4.7
4.7 Distribuição do plano de continuidade	4.8
4.8 Recuperação e retomada dos serviços de TI	4.9, 4.11

COBIT 3ª Edição	COBIT 4.1
4.9 Armazenamento de cópias de segurança em locais remotos	4.12, 11.25
4.10 Revisão pós-retomada dos serviços	4.13
DS5 Garantir a Segurança dos Sistemas.	
5.1 Gestão da segurança de TI	5.1, 5.12
5.2 Plano de segurança de TI	Novo
5.3 Gestão de identidade	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 Gestão de conta de usuário	5.4, 5.5, 5.6, 5.13, 10.4
5.5 Teste de segurança, vigilância e monitoramento	5.6, 5.7, 5.10
5.6 Definição de incidente de segurança	5.11
5.7 Proteção da tecnologia de segurança	5.17
5.8 Gestão de chave criptográfica	5.18
5.9 Prevenção, detecção e correção de *software* malicioso	5.19
5.10 Segurança de rede	5.20

COBIT 3ª Edição	COBIT 4.1
5.11 Comunicação de dados confidenciais	5.15, 5.16, 11.29, 13.8
DS6 Identificar e alocar custos	
6.1 Definição de serviços	6.1
6.2 Contabilidade de TI	6.3
6.3 Modelagem de custo e cobrança	6.2
6.4 Manutenção do modelo de custo	6.3
DS7 Educar e treinar os usuários	
7.1 Identificação das necessidades de ensino e treinamento	7.1
7.2 Entrega de treinamento e ensino	7.2
7.3 Avaliação do treinamento recebido	Novo
DS8 Gerenciar a Central de Serviço e os Incidentes	
8.1 Central de serviço	8.1
8.2 Registro dos chamados dos clientes	8.2, 10.3
8.3 Escalonamento de incidentes	8.2, 8.3, 10.5
8.4 Encerramento de incidente	8.2
8.5 Análise de tendências e relatórios	8.1
DS9 Gerenciar a configuração	
9.1 Repositório de configuração e perfis básicos	9.1, 9.2, 9.8

COBIT 3ª Edição	COBIT 4.1
9.2 Identificação e manutenção dos itens de configuração	9.7, 9.8
9.3 Análise crítica da integridade da configuração	9.3, 9.4, 9.5
DS10 Gerenciar os problemas	
10.1 Identificar e classificar os problemas	8.5, 10.1, 10.5
10.2 Rastreamento e resolução de problemas	Novo
10.3 Encerramento do problema	8.4, 10.1
10.4 Integração de gerenciamento de mudanças, configuração e problemas	Novo, 10.1
DS11 Gerenciar os Dados	
11.1 Requisitos de negócio para o gerenciamento de dados	Novo
11.2 Arranjos de armazenamento e retenção	11.12, 11.19, 11.20, 11.26, 11.30
11.3 Sistema de gerenciamento de biblioteca de mídia	11.21, 11.22, 11.25
11.4 Descarte	11.18, 11.24
11.5 *Backup* e restauração	AI2.14, 11.23

COBIT 3ª Edição	COBIT 4.1
11.6 Requisitos de segurança para o gerenciamento de dados	11.16, 11.17, 11.27
DS12 Gerenciar o Ambiente Físico	
12.1 Seleção do local e *layout*	12.1, 12.2, 12.4
12.2 Medidas de segurança física	12.1, 12.2
12.3 Acesso físico	10.4, 12.3
12.4 Proteção contra fatores ambientais	12.5
12.5 Gerenciamento de instalações físicas	12.4, 12.6, 12.9
DS13 Gerenciar as Operações	
13.1 Procedimentos e instruções de operações	13.1, 13.2, 13.5, 13.6
13.2 Agendamento de *Jobs*	13.3, 13.4
13.3 Monitoramento da infraestrutura de TI	Novo
13.4 Dispositivos de saída e documentos confidenciais	5.21, 13.7
13.5 Manutenção preventiva de *hardware*	AI3.2

COBIT 3ª Edição	COBIT 4.1
ME1 Monitorar e Avaliar o Desempenho de TI	
1.1 Abordagem de Monitoramento	1.0*
1.2 Definição e coleta dos dados de monitoramento	1.1, 1.3
1.3 Método de monitoramento	Novo
1.4 Avaliação de desempenho	1.2
1.5 Relatórios para direção	1.4
1.6 Ações corretivas	Novo
ME2 Monitorar e avaliar os controles internos	
2.1 Monitoramento da estrutura de controles internos	2.0*, 2.2
2.2 Revisão Gerencial	2.1, 2.3
2.3 Exceções aos Controles	Novo

COBIT 3ª Edição	COBIT 4.1
2.4 Auto avaliação dos controles	2.4
2.5 Garantia dos controles internos	Novo
2.6 Controles internos aplicados a terceiros	3.6
2.7 Ações corretivas	Novo
ME3 Assegurar a conformidade com requisitos externos	
3.1 Identificação dos requisitos de conformidade com leis, regulamentações e contratos	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4
3.2 Otimização da resposta aos requisitos externos	PO8.2
3.3 Avaliação da conformidade com os requisitos externos	Novo

COBIT 3ª Edição	COBIT 4.1
3.4 Assegurar a conformidade	Novo
3.5 Informes integrados	Novo
ME4 Prover a governança de TI	
4.1 Estabelecimento de uma estrutura de governança de TI	Novo
4.2 Alinhamento estratégico	Novo
4.3 Entrega de valor	Novo
4.4 Gerenciamento de recursos	Novo
4.5 Gestão de riscos	Novo
4.6 Medição de desempenho	Novo
4.7 Avaliação Independente	Novo

*ME 1,0 e ME2.0 foram incluídos no *Control Practices* pelo ITGI em 2004.

Apêndice VI
Enfoque de Pesquisa e Desenvolvimento

APÊNDICE VI - ENFOQUE DE PESQUISA E DESENVOLVIMENTO

O desenvolvimento do conteúdo da estrutura CobiT é supervisionado pelo Comitê de Direção CobiT, formado por representantes internacionais da indústria, setor acadêmico, governo e profissionais de governança, auditoria, controle e segurança de TI. Grupos internacionais de trabalho foram estabelecidos para fornecer avaliação de qualidade e revisão de especialistas das entregas intermediárias do projeto de pesquisa e desenvolvimento. O direcionamento geral do projeto é provido pelo ITGI.

EDIÇÕES PRÉVIAS DO COBIT

Começando com a estrutura CobiT definida na primeira edição, a aplicação de padrões, direcionamento e pesquisas internacionais sobre boas práticas levaram ao desenvolvimento dos objetivos de controle. Foram desenvolvidos guias de auditoria para verificar se os objetivos de controles são adequadamente implantados. A pesquisa para a primeira e a segunda edições incluíram análises de fontes internacionais identificadas efetuadas por equipes na Europa *(Free University of Amsterdam)*, Estados Unidos *(California Polytechnic University)* e Austrália *(University of New South Wales)*. Os pesquisadores tiveram como incumbência compilar, revisar, avaliar e incorporar de maneira adequada padrões técnicos internacionais, códigos de conduta, padrões de qualidade, padrões profissionais em auditoria, práticas e requisitos internacionais de mercado, conforme eles se relacionam com a estrutura e os objetivos de controles individuais. Depois da fase de coleta e análise, os pesquisadores foram desafiados a examinar cada domínio e processo profundamente e sugerir objetivos de controle novos ou modificados aplicáveis particularmente aos processos de TI. A consolidação dos resultados foi realizada pelo Comitê de Direção CobiT.

O projeto do CobiT 3ª Edição consistiu no desenvolvimento das orientações de gerenciamento e na atualização do CobiT 2ª Edição baseado nas referências internacionais novas e revisadas. Além disso, a estrutura CobiT foi revisada e aprimorada para ampliar o controle gerencial, introduzir o gerenciamento de performance e melhor desenvolver a governança de TI. Para fornecer à direção uma aplicação que lhes permitisse avaliar e escolher alternativas de implementação de controles e melhorias no ambiente de tecnologia de informação e de medição de performance, as orientações de gerenciamento incluem modelos de maturidade, fatores críticos de sucesso, KGIs e KPIs relacionados com os objetivos de controles.

As orientações de gerenciamento foram desenvolvidas utilizando-se um painel internacional de 40 especialistas acadêmicos, da área de governo, e profissionais de governança, avaliação, controle e segurança de TI. Esses especialistas participaram de uma reunião de trabalho conduzida por facilitadores profissionais, utilizando as orientações de desenvolvimento definidas pelo Comitê de Direção CobiT. A reunião de trabalho foi fortemente apoiada pelo *Gartner Group* e pela *PricewaterhouseCoopers* que, além de liderar o trabalho, também alocou muitos de seus especialistas em controle, gerenciamento de performance e segurança da informação. Os resultados da reunião de trabalho foram os rascunhos dos modelos de maturidade, CSFs, KGIs e KPIs para cada um dos 34 processos CobiT. A avaliação da qualidade das entregas iniciais foi conduzida pelo Comitê de Direção CobiT e os resultados foram divulgados para avaliação no site do ISACA na Internet. As orientações de gerenciamento ofereceram um novo conjunto de ferramentas orientadas ao gerenciamento e, ao mesmo tempo, proporcionam integração e consistência com a estrutura CobiT.
A atualização dos objetivos de controle no CobiT 3ª Edição com base nas novas e revisadas referências internacionais foi conduzida por membros dos capítulos do ISACA, sob a orientação do Comitê de Direção CobiT. A intenção não era realizar uma análise global de todo material ou um novo desenvolvimento dos objetivos de controle, mas proporcionar uma atualização incremental.

A atualização dos objetivos de controle no CobiT 3ª Edição baseada nas novas e revisadas referências internacionais foram conduzidas por membros dos capítulos ISACA, debaixo de orientação do Comitê de Direção CobiT. A intenção não era realizar uma análise global de todo material ou um novo desenvolvimento dos objetivos de controle, mas proporcionar uma atualização incremental. Os resultados do desenvolvimento de orientações de gerenciamento foram usados para revisar a estrutura CobiT, especialmente as considerações, objetivos e procedimentos recomendados nas descrições de processos. O CobiT 3ª Edição foi publicado em julho de 2000.

PROJETO DE ATUALIZAÇÃO MAIS RECENTE

No seu esforço de continuamente desenvolver a base de conhecimento CobiT, o Comitê de Direção CobiT iniciou nos últimos dois anos uma pesquisa em diversos aspectos detalhados do CobiT. Esses projetos de pesquisa forcaram nos componentes dos objetivos de controles e orientações de gerenciamento. Algumas específicas áreas que foram cobertas são mencionadas a seguir.

Control Objectives Research

· CobiT – Alinhamento da governança de TI de baixo para cima
· CobiT – Alinhamento da governança de TI de cima para baixo
· CobiT e outros padrões detalhados – Detalhado mapa entre o CobiT e o ITIL, CMM, COSO, PMBOK, ISF's Standard of

Good Practice for Information Security e ISO 27000 para possibilitar a harmonização com esses padrões em linguagem, definições e conceitos

Pesquisa sobre Orientações de Gerenciamento

- Análise do relacionamento de KGI-KPI
- Revisão da qualidade de KGIs/KPIs/CSFs – Baseado na análise de relacionamento de KPI/KGI, dividindo os CSFs em 'o que você precisa de outros' e 'o que você mesmo precisa fazer'
- Análise detalhada de conceitos de métricas – Detalhado desenvolvimento com especialistas em métricas para aprimorar os conceitos de métricas, criando o cascateamento de métricas do 'processo-TI-negócios' e definições de critérios de qualidade para métricas
- Relacionando os objetivos de negócios, objetivos de TI e processos de TI – Pesquisa detalhada em oito mercados diferentes que resultou em um entendimento mais detalhado sobre como os processos CobiT permitem atingir objetivos de TI específicos e, por extensão, objetivos de negócios; os resultados foram então generalizados
- Revisão do conteúdo do modelo de maturidade – Asseguradas a consistência e a qualidade dos níveis de maturidade entre e dentro dos processos, incluindo uma melhor definição dos atributos do modelo de maturidade

Todos esses projetos foram iniciados e direcionados pelo Comitê de Direção CobiT, enquanto o gerenciamento dia a dia e o acompanhamento foram executados por um grupo reduzido do CobiT. A execução dos projetos de pesquisa mencionados foi baseada largamente em equipes de especialistas e voluntários membros do ISACA, usuários CobiT, conselheiros especialistas e acadêmicos. Grupos de desenvolvimento locais foram criados em Bruxelas (Bélgica), Londres (Inglaterra), Chicago (Illinois, EUA), Camberra (Austrália), Cidade do Cabo (África do Sul), Washington (DC, EUA) e Copenhagen (Dinamarca), dos quais cinco a 10 usuários CobiT reuniram-se em média duas a três vezes por ano para trabalhar na pesquisa ou revisão específica atribuída pela equipe central do CobiT. Além disso, alguns projetos de pesquisa específicos foram designados a escolas, como a Universidade da Antuérpia *(UAMS, University of Antwerp Management School)* e a Universidade do Havaí.

Os resultados desses esforços de pesquisa, em conjunto com o feedback providos pelos usuários CobiT durante os anos e outras questões observadas durante o desenvolvimento de novos produtos tais como as práticas de controles foram inseridas no projeto principal do CobiT para atualizar e aprimorar os objetivos de controle, orientações de gerenciamento e estrutura CobiT. Dois laboratórios de desenvolvimento principais, cada um envolvendo mais de 40 especialistas em governança, gerenciamento e controle de TI (gerentes, consultores, acadêmicos e auditores) de diversas partes do mundo, foram criados para revisão e atualização detalhada do conteúdo dos objetivos de controle e orientações de gerenciamento. Grupos menores trabalharam no aperfeiçoamento e na finalização do importante resultado produzido por esses eventos relevantes.

A minuta final foi submetida a um processo de revisão abrangente com aproximadamente 100 participantes. Os comentários volumosos recebidos foram analisados em uma reunião de trabalho final realizada pelo Comitê de Direção CobiT.

Os resultados dessas reuniões de trabalho foram processados pelo Comitê de Direção CobiT, pela equipe principal do CobiT e pelo ITGI, para criar o novo material CobiT disponível neste volume. Com a existência do CobiT *Online*, a tecnologia disponível permite manter o conteúdo principal do CobiT atualizado com maior facilidade, e utilizar esse recurso como um repositório central. O conteúdo será mantido através de *feedback* da base de usuários e revisões periódicas do conteúdo por áreas específicas. Publicações periódicas (impressas e eletrônicas) serão produzidas para suportar uma referência *off-line* ao conteúdo CobiT.

Apêndice VII
Glossário

APÊNDICE VII - GLOSSÁRIO

Análise de causa-raiz *(Root cause analysis)* – Processo de diagnóstico para estabelecer a origem de eventos, os quais podem ser usados para aprendizagem através de suas consequências, tipicamente de erros ou problemas.

Arquitetura corporativa *(Enterprise architecture)* – Descrição do desenho fundamental dos componentes de um sistema de negócios, ou de um elemento de um sistema de negócios (por exemplo, tecnologia), o relacionamento entre eles e a maneira como suportam os objetivos da organização.

Arquitetura corporativa de TI *(Enterprise architecture for IT)* – Descrição do *design* fundamental dos componentes de TI de negócios, o relacionamento entre eles e a maneira como suportam os objetivos da organização.

Arquitetura da informação *(Information architecture)* – Um componente da arquitetura de TI (em conjunto com aplicativos e tecnologia). Veja arquitetura de TI.

Arquitetura de TI *(IT architecture)* – Descrição dos fundamentos do *design* dos componentes de TI de um negócio, o relacionamento entre eles e a maneira como suportam os objetivos de negócios.

Atividade *(Activity)* – A principal ação executada para a operação de um processo CobiT.

Autenticação *(Authentication)* – Ato de averiguar a identidade de uma entidade do sistema (por exemplo, usuário, sistema, ponto de rede) e a elegibilidade da entidade para acessar a informação disponível em computadores. Designada para proteção contra atividades fraudulentas no logon, a autenticação também pode se referir à verificação da correção de um dado.

Balanced scorecard – Um conjunto coerente de métricas de performance organizadas em quatro categorias. Inclui as métricas financeiras tradicionais, além das perspectivas de clientes, processos internos de negócios, aprendizagem e crescimento. Foi desenvolvido por Robert S. Kaplan e David P. Norton em 1992.

Benchmarking – Enfoque sistemático usado para comparar o desempenho de uma organização em relação a seus pares e concorrentes, em um esforço para conhecer as melhores formas de conduzir o negócio (por exemplo, *benchmarking* de qualidade, eficiência logística e várias outras métricas).

Capacidade *(Capability)* – Possuir os atributos necessários para executar ou atingir um objetivo.

Capability Maturity Model (CMM) – O CMM para *Software*, do *Software Engineering Institute (SEI)*. Modelo usado por muitas organizações para identificar boas práticas que as ajudam a avaliar e aumentar a maturidade dos seus procedimentos de desenvolvimento de *software*.

Central de serviços *(Service desk)* – Ponto de contato dos usuários de serviços de TI com a organização de TI.

CEO – Chief executive officer – Presidente, posição mais alta na organização.

CFO – Chief financial officer – Indivíduo com a responsabilidade principal de gerenciar os riscos financeiros de uma organização.

CIO – Chief information officer – Indivíduo com a responsabilidade pelo grupo de TI na organização. Em alguns casos, o papel do CIO foi estendido para tornar-se o chief knowledge officer (CKO), que trata do conhecimento, não somente da informação. Veja também CTO.

Comitê estratégico de TI *(IT strategy committee)* – Comitê no nível da Alta Direção para assegurar que seus membros estejam envolvidos nas questões e decisões relevantes de TI. O Comitê é responsável principalmente pelo gerenciamento dos portfólios de investimentos em TI, serviços de TI e outros recursos de TI. O Comitê é o proprietário do portfólio.

Consultado *(Consulted)* – Na tabela RACI refere-se às pessoas cuja opinião será obtida em uma atividade (comunicação bi-direcional).

Continuidade *(Continuity)* – Prevenir, mitigar e se recuperar de uma interrupção. Os termos 'plano de recuperação de negócios', 'plano de recuperação de desastres' e 'plano de contingência' também podem ser utilizados nesse contexto; todos se concentram nos aspectos de recuperação da continuidade.

Controle automatizado de aplicativo *(Automated application control)* – Conjunto de controles inseridos em uma solução automatizada (aplicação).

Controle de acesso *(Acess Control)* – Processo que limita e controla o acesso a recursos de um sistema de computador; um controle lógico ou físico com a finalidade de proteger contra entrada ou uso não autorizados.

Controle detectivo *(Detective control)* – Controle utilizado para identificar eventos (indesejáveis ou desejados), erros e outras ocorrências que uma empresa determinou como tendo efeito material em um processo ou produto.

Controle interno *(Internal control)* – Políticas, planos e procedimentos e a estrutura organizacional criada para prover uma razoável certeza de que os objetivos de negócio serão atingidos e eventos indesejáveis serão impedidos e corrigidos.

Controles gerais de computador *(General computer controls)* – Controles que se referem ao ambiente onde sistemas aplicativos são desenvolvidos, atualizados e processados, sendo portando aplicáveis a todas as aplicações processadas nesse ambiente. O objetivo dos controles gerais é assegurar o próprio desenvolvimento e a implantação de aplicativos, a integridade de programas e arquivos de dados e a operação de computador. Assim como os controles de aplicativos, os controles gerais podem ser manuais ou programados. Exemplos de controles gerais incluem o desenvolvimento e a implantação estratégias e políticas de sistemas de informação, a organização do pessoal de sistemas de informação para evitar funções conflitantes e o planejamento para prevenção de desastres e recuperação.

Controle preventivo *(Preventive control)* – Controle interno utilizado para prevenir eventos indesejáveis, erros e outras ocorrências que a organização entendeu que poderiam ter um efeito negativo material em um processo ou produto final.

COSO – Committee of Sponsoring Organisations of the Treadway Commission – O seu relatório de 1992 denominado *Internal Control – Integrated Framework* é um padrão aceito mundialmente para governança corporativa. Veja o site www.coso.org.

CSF – Fatores críticos de sucesso - As questões ou ações mais relevantes da gerência para obter controle sobre os processos de TI.

CTO – *Chief technology officer* – Foca nas questões técnicas da organização. O título CTO é utilizado às vezes como sinônimo de CIO.

Dicionário de dados *(Data dictionary)* – Base de dados que contém o nome, o tipo, a faixa de valores, fontes e autorizações de acesso para cada elemento em uma base de dados. Também indica quais programas aplicativos usam aquele dado de maneira que, possa ser gerada uma lista de todos os programas afetados quando uma estrutura de dados é selecionada. O dicionário de dados pode ser um sistema de informação isolado *(stand-alone)* usado para o gerenciamento ou para fins de documentação ou ainda para controlar toda a operação de uma base de dados.

Direcionadores de performance *(Performance drivers)* – Métricas consideradas os direcionadores dos indicadores históricos *('drivers' of lag indicators)*. Podem ser mensurados antes que o resultado seja claro e, portando são chamados de indicadores futuros *('lead indicators')*. Existe um relacionamento presumido entre os dois que sugere que uma melhora de *performance* no indicador futuro irá conduzir a uma melhor *performance* no indicador histórico. Também são chamados de indicadores-chave de performance *(key performance indicators – KPIs)* e são usados para indicar se os objetivos irão provavelmente ser atingidos.

Diretriz *(Guideline)* – Descrição de uma forma específica para atingir algo mas menos detalhada do que um procedimento.

Domínio *(Domain)* – No CobiT, refere-se ao agrupamento de objetivos de controle em estágios lógicos no ciclo de vida de investimentos em TI (Planejar e Organizar, Adquirir e Implementar, Entregar e prover Suporte, e Monitorar e Avaliar).

Esquema de classificação de dados *(Data classification scheme)* – Esquema corporativo de classificação de dados por fatores como criticidade, confidencialidade e propriedade.

Framework – Veja Modelo de controle.

Gerenciamento de configuração *(Configuration management)* – O controle de mudanças de um conjunto de itens de configuração no ciclo de vida de um sistema.

Gerenciamento de performance *(Performance management)* – Em TI refere-se à habilidade de gerenciar qualquer tipo de medida, incluindo a mensuração de aspectos relacionados a funcionários, equipes, processos, operacionais e financeiros. O termo conota um controle bem próximo e um monitoramento regular da medição.

Governança corporativa *(Enterprise governance)* – Conjunto de responsabilidades e práticas exercidas pela Alta Direção e Executivos com o objetivo de prover direção estratégica, assegurando que os objetivos sejam atingidos, assegurando que os riscos sejam gerenciados apropriadamente e verificando se os recursos da organização são utilizados com responsabilidade.

Incidente de TI *(IT incident)* – Qualquer evento que não faz parte da operação normal de um serviço e que causa, ou pode causar, uma interrupção ou a redução da qualidade do serviço (alinhado com o ITIL)

Informado *(Informed)* – Na tabela RACI, refere-se às pessoas que são mantidas informadas sobre o andamento de uma atividade (uma via de comunicação).

ISO 17799 – Padrão internacional que define os controles de confidencialidade, integridade e disponibilidade da informação.

ISO 27001 *(Information Security Management)* – Gerenciamento da segurança da informação – especificação com Diretriz para Uso; substituição da BS7799-2. Visa prover a base para auditoria de terceiros e está harmonizada com outros padrões de gerenciamento, tais como ISO/IEC 9001 e 14001.

ISO 9001:2000 – Código de práticas para gerenciamento de qualidade da *International Organisation for Standardisation (ISO)*. Especifica os requerimentos para um sistema de gerenciamento de qualidade para consistentemente prover um produto ou serviço que atinja metas de qualidade específicas.

Item de configuração *(Configuration item – CI)* – Componente de uma infraestrutura – ou um item, como uma solicitação de mudança, associado a uma infraestrutura – o qual está (ou estará) debaixo do gerenciamento de configuração. Os CIs podem variar muito em complexidade, tamanho e tipo, desde um sistema inteiro (incluindo todo o *hardware, software* e documentação) até um simples módulo ou pequeno *hardware*.

ITIL – Refere-se à Biblioteca de Infraestrutura de TI *(IT Infrastructure Library)* criada pelo *UK Office of Government Commerce (OGC)*; conjunto de diretrizes de gerenciamento e procedimentos operacionais de serviços de TI.

KGI – Indicador-chave de sucesso *(Key goal indicator)* – Mensurações que informam aos gerentes depois dos fatos se um processo de TI atingiu os requisitos de negócios, usualmente expresso em termos de critério de informação.

KPI – Indicador-chave de performance *(Key performance indicator)* – Mensurações que determinam o andamento de um processo para permitir que um objetivo seja atingido. Eles são indicativos de tendências futuras quanto a se um objetivo será provavelmente atingido; são bons indicadores de capacidades, práticas e especialização. Medem os objetivos de atividades que são as medidas que os proprietários de processos precisam tomar para um efetivo desempenho do processo.

Mandato da auditoria *(Audit charter)* – Documento aprovado pela Alta Direção que define o propósito, a autoridade e a responsabilidade da atividade de auditoria interna.

Maturidade *(Maturity)* – Nos negócios, indica o grau de confiança ou dependência que o negócio pode atribuir a um processo no atingimento de suas metas ou objetivos.

Medição *(Measure)* – Padrão utilizado para avaliar e comunicar a performance em relação aos resultados esperados. Medições são normalmente de natureza quantitativa (números, dólares, percentagens etc.), mas também podem tratar de informações qualitativas, como a satisfação de clientes. As mensurações de monitoramento e de reporte ajudam a organização a acompanhar o andamento da efetiva implementação de uma estratégia.

Medidas de resultado *(Outcome measures)* – Medição que representa as consequências das medidas previamente tomadas e às vezes chamadas de indicadores históricos *(lag indicators)*. Frequentemente enfocam os resultados conhecidos como indicadores-chave de sucesso *(key goal indicators - KGIs)* e são usados para indicar se os objetivos foram atingidos. Eles podem ser mensurados apenas depois do fato e, por isso, são chamados de *'lag indicators'*.

Melhores práticas *(Best practice)* – Atividade ou processo provado usado com sucesso por múltiplas organizações.

Métricas *(Metrics)* – Descrições específicas de como avaliações quantitativas e periódicas da performance serão medidas. Uma métrica completa define a unidade utilizada, a frequência, o valor ideal esperado, o procedimento para efetuar a medição e o procedimento para interpretar a avaliação.

Modelo de controle *(Control framework)* – Conjunto de controles fundamentais que facilitam a execução de um processo de negócio de responsabilidade de um proprietário para evitar perdas financeiras ou de informação em uma organização.

OLA – Acordo de nível operacional *(Operational level agreement)* – Um acordo interno cobrindo a entrega de serviços que suporta a organização de TI na sua entrega de serviços.

Organização *(Organisation)* – A maneira como uma empresa está estruturada; pode significar também entidade.

QMS – Sistema de gerenciamento de qualidade *(Quality management system)* – Um sistema que define as políticas e os procedimentos necessários para aprimorar e controlar os vários processos que levarão a uma performance organizacional otimizada.

Objetivo de controle *(Control objective)* – Uma declaração do resultado desejado ou do propósito a ser atingido com a implementação de um procedimento de controle em um processo em particular.

Organização *(Enterprise)* – Grupo de pessoas que trabalham juntas para atingir um propósito em comum, tipicamente no contexto de uma Organização, como uma corporação, agência pública, filantrópica ou de custódia.

Padrão *(Standard)* – Requisito obrigatório. Os exemplos incluem a ISO/IEC 20000 (padrão internacional), um padrão de segurança interno para a configuração do UNIX ou um padrão governamental que estabelece como os registros financeiros devem ser mantidos. O termo 'padrão' também se refere a um código de práticas ou especificações publicado por organizações que definem padrões, como a ISO ou BSI.

Painel de controle *(Dashboard)* – Ferramenta para definir as expectativas de uma organização em relação a cada nível de responsabilidade e monitoramento contínuo da performance em comparação com as metas definidas anteriormente.

Painel de controle de investimento em TI *(IT investment dashboard)* – Ferramenta que define as expectativas para uma organização a cada nível e o monitoramento contínuo em comparação com as metas de gastos e retorno de projetos de investimento em TI em termos de valores para o negócio.

Performance – Em TI, a implementação real ou o fato de atingir o objetivo de um processo.

Plano de infraestrutura tecnológica *(Technology infrastructure plan)* – Plano que contempla a tecnologia, os recursos humanos e as facilidades que permitem o processamento atual e futuro e o uso dos aplicativos.

Plano estratégico de TI *(IT strategic plan)* – Plano de longo prazo, ou seja, com horizonte de três a cinco anos, no qual as direções de negócios e de TI colaborativamente descrevem como os recursos de TI contribuirão com o objetivos estratégicos da organização.

Plano tático de TI *(IT tactical plan)* – Plano de médio prazo, ou seja, como o horizonte de seis a 18 meses, que traduz a direção do plano estratégico de TI nas iniciativas necessárias, os requisitos de recursos e as formas como os recursos e benefícios serão monitorados e gerenciados.

PMBOK – Project Management Body of Knowledge – Um padrão de gerenciamento de projetos desenvolvido pelo *Project Management Institute (PMI).*

PMO – Project management officer – A função individual responsável pela implantação de uma iniciativa específica para suportar o papel de gerenciamento de projeto e o avanço da disciplina de gerenciamento de projeto.

Política *(Policy)* – Geralmente é um documento que registra os princípios de alto nível ou direcionamento de ações que foram definidos. O propósito de uma política é influenciar e direcionar tanto o presente quanto o futuro processo de decisão para estar em linha com a filosofia, os objetivos e os planos estratégicos estabelecidos pelos executivos de uma empresa. Além disso, as políticas precisam descrever as consequências por não-conformidade com a política, os meios para tratar exceções e como a conformidade com a política será verificada e medida.

Portfólio *(Portfolio)* – Um grupo de programas, projetos, serviços ou bens selecionados, gerenciados e monitorados para otimizar o retorno do negócio.

Prática de controle *(Control practice)* – Mecanismo-chave de controle que permite atingir o objetivo de controle através do uso responsável dos recursos, apropriado gerenciamento dos riscos e alinhamento de TI com os negócios.

Práticas-chave de gerenciamento *(Key management practices)* – Práticas de gerenciamento necessárias para executar os processos de negócio com êxito.

PRINCE2 – Projects in a Controlled Environment, desenvolvida pelo OGC – Desenvolvido pelo OGC; um método de gerenciamento de projetos que cobre o gerenciamento, o controle e a organização de um projeto.

Problema – Em TI, um ou mais incidentes com causa desconhecida.

Procedimento *(Procedure)* – Um documento contendo os passos que especificam como executar uma atividade. Procedimentos são definidos como parte de processos.

Processo *(Process)* – Geralmente um conjunto de procedimentos influenciados pelas políticas e os procedimentos que recebem entradas de várias fontes, inclusive de outros processos, manipulam as entradas e produzem resultados, incluindo outros processos. Existe uma clara razão de negócio por sua existência, proprietários responsáveis, papéis claros, responsabilidades pela execução do processo e meios de medir a performance.

Processo de negócio *(Business process)* – Veja Processo.

Programa *(Programme)* – Grupo estruturado de projetos interdependentes que inclui o escopo total de negócios, processos, pessoas, tecnologia e atividades organizacionais que são requeridos (tanto necessário como suficiente) para atingir um resultado de negócio claramente especificado.

Programa aplicativo *(Application program)* – Um programa que processa dados de negócio através de atividades como entrada de dados, atualização e consultas. Contrasta com programas de sistema, como um sistema operacional ou um programa de controle de rede, e com programas utilitários, como *copy* ou *sort*.

Projeto *(Project)* – Conjunto de atividades estruturadas preocupado com a entrega para a empresa de uma capacidade definida (necessária, mas não suficiente para atingir um resultado de negócio necessário) com base em uma agenda e um orçamento aceitos.

Proprietários da informação *(Data owners)* – Normalmente gerentes ou diretores, que tem a responsabilidade pela integridade, precisão, relatórios e uso de um dado computadorizado.

Provedor de serviços *(Service provider)* – Entidade externa à empresa que presta serviços à organização.

Resiliência *(Resilience)* – Em negócios, a habilidade de um sistema ou rede de se recuperar automaticamente de qualquer interrupção, em geral com consequências mínimas.

Responsável *(Responsible)* – Na tabela RACI, refere-se à pessoa que precisa garantir que as atividades serão executadas com sucesso.

Responsabilizado *(Accountable)* – Na tabela RACI, refere-se à pessoa ou ao grupo que tem a autoridade de aprovar ou aceitar a execução de uma atividade.

Risco *(Risk)* – Em negócios, o potencial de que uma certa ameaça irá explorar as vulnerabilidades de um recurso ou grupo de recursos para causar perda e/ou prejuízos; usualmente medido por uma combinação de impacto e probabilidade de ocorrência.

SDLC – Ciclo de vida de desenvolvimento de sistema *(System development life cycle)* – Fases entregues no desenvolvimento ou aquisição de um sistema. As fases normalmente incluem estudo de viabilidade, estudo de requisitos, projeto detalhado, programação, testes, implantação e revisão pós-implantação, mas não incluem a entrega de serviços ou atividades de mensuração de benefícios.

Segregação de funções *(Segregation/separation of duties)* – Controle interno básico que impede ou detecta erros e irregularidades por designar a indivíduos distintos as responsabilidades por iniciar e registrar uma transação da função de custódia dos bens. Comumente utilizada em grandes organizações de TI de maneira que nenhuma pessoa sozinha tenha condições de introduzir um código fraudulento ou malicioso sem detecção.

SLA – Acordo de nível de serviços *(Service level agreement)* – Um acordo preferencialmente documentado entre o provedor do serviço e o cliente/usuário que define as metas mínimas de performance de um serviço e como elas serão mensuradas.

Tabela RACI *(chart)* – Mostra quem é responsável *(responsible)*, responsabilizado *(accountable)*, consultado e informado dentro de uma estrutura organizacional.

TI – Tecnologia da informação *(IT – Information technology)* – Refere-se ao *hardware, software*, comunicação e outras facilidades usadas para entrada de dados, armazenagem, processamento, transmissão e saída de dados de qualquer forma.

TCO – Custo total de propriedade *(Total cost of ownership)* – Em TI inclui:
- Custo original do computador e *software*
- Atualizações de *hardware* e *software*
- Manutenção
- Suporte técnico
- Treinamento
- Certas atividades executadas por usuários

Usuário de TI *(IT user)* – A pessoa que usa TI para atingir um objetivo de negócio.

Apêndice VIII
CobiT e Produtos Relacionados

APÊNDICE VIII - COBIT E PRODUTOS RELACIONADOS

O modelo COBIT nas versões 4.0 e superiores incluem o seguinte:
- Modelo – Explica como o COBIT organiza a governança de TI, objetivos de controles e boas práticas por domínios e processos de TI e os relaciona com os requisitos de negócios.
- Descrição de processos – Incluem os 34 processos de TI cobrindo as áreas de responsabilidade de TI do início ao fim.
- Objetivos de controle – Fornece boas práticas gerais de objetivos de gerenciamento para processos de TI.
- Diretrizes de gerenciamento – Oferece ferramentas para ajudar a designação de responsabilidades, medição de performance, benchmark e tratamento de deficiências em capacidade.
- Modelos de maturidade – Provê perfis de processos de TI que descrevem possíveis situações atuais e futuras.

Desde a sua concepção, o conteúdo principal do COBIT tem evoluído e o número de trabalhos derivados do COBIT cresceu. São as seguintes as publicações derivadas do COBIT:
- *Board Briefing on IT Governance, 2nd Edition* – Elaborado para ajudar os executivos a entender porque a governança de TI é importante, quais são os problemas e as suas responsabilidades em gerenciar TI.
- *COBIT® Online* – Permite aos usuários personalizarem uma versão do COBIT para sua própria organização e depois armazená-la e manuseá-la como desejado. Oferece pesquisas *on-line* e em tempo real, questões geralmente feitas, *benchmarking* e um recurso de discussão para troca de experiências e dúvidas.
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* – Fornece diretrizes sobre riscos a serem evitados e valor a ser obtido com a implantação de objetivos de controles e instruções de como implementá-los. As práticas de controle são fortemente recomendadas para uso com o *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition.*
- *IT Assurance Guide: Using COBIT®* – Provê diretrizes sobre como o COBIT pode ser usado para suportar diversas atividades de avaliação e oferece sugestões de passos de testes em todos os processos e objetivos de controle de TI do COBIT . Substitui as informações constantes do *Audit Guidelines* sobre diretrizes de auditoria e auto-avaliação em comparação com os objetivos de controle no COBIT 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition* – Provê diretrizes sobre como assegurar a conformidade para o ambiente de TI com base nos objetivos de controle do COBIT®.
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition* – Prove um mapa genérico para implementar a governança de TI usando os recursos do COBIT® e do Val IT e um conjunto de ferramentas de suporte.
- *COBIT® Quickstart* – Prove um mapa inicial de controles para organizações menores e possíveis primeiros passos para organizações maiores.
- *COBIT® Security Baseline* – Foca nos passos essenciais para implementar a segurança da informação na organização. A segunda edição estava em fase de desenvolvimento no momento em que isto estava sendo escrito.
- *CobiT Mappings* – Atualmente disponíveis em www.isaca.org/downloads:
  - *Aligning COBIT®, ITIL and ISO 17799 for Business Benefit*
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of COSO Enterprise Risk Management With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT® , 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* – Apresenta a segurança da informação em termos de negócios e contém ferramentas para ajudar a desvendar problemas relacionados a segurança.

Val IT é um termo abrangente usado para descrever as publicações e futuros produtos e atividades adicionais que tratam do método Val IT *(Val IT framework)*.

As publicações recentes relacionadas ao Val IT são:
- *Enterprise Value: Governance of IT Investments – The Val IT Framework*, que explica como uma organização pode obter valor otimizado dos investimentos em TI e baseia-se no método CobiT®. Está organizado em:
  - Três processos – Governança de Valor, Gerenciamento de Portfólio e Gerenciamento de Investimento
  - *IT key management practices* – Práticas de gerenciamento essenciais que influenciam positivamente o atingimento dos resultados ou propósitos esperados de uma atividade específica. Suportam os processos de Val IT e têm quase o mesmo papel dos objetivos de controle do CobiT®.

- *Enterprise Value: Governance of IT Investments – The Business Case*, que foca nos elementos-chave do processo de gerenciamento de investimentos.
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, que descreve como uma companhia global de serviços financeiros gerencia o portfólio de investimentos em TI no contexto do método Val IT.

Para informações mais completas e atualizadas sobre o CobiT, Val IT, produtos relacionados, estudos de caso, oportunidades de treinamento e outras informações específicas sobre o método visite os sites www.isaca.org/cobit e www.isaca.org/valit.

LEADING THE IT GOVERNANCE COMMUNITY

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, IL 60008 USA
PHONE: +1.847.590.7491
FAX: +1.847.253.1443
E-MAIL: *info@itgi.org*
WEB SITE: *www.itgi.org*