

Unidade IV

7 GOVERNANÇA DE TI

7.1 Governança corporativa

7.1.1 Conceitos de governança corporativa

Vejamos o que dizem Rodriguez e Brandão sobre governança corporativa.

Ainda não se conseguiu produzir uma definição sobre o tema governança corporativa que magnetize a mente das pessoas a ponto de eclipsar as demais formas de conceituá-la. Isso também se aplica a temas como "firma" e "estratégia" (existem várias teorias que explicam o que eles significam), os quais exigem o estudo de várias correntes de pensamento para que se possa ter uma ideia do que foi criado e condensado ou não sobre o assunto. Governança Corporativa é, com certeza, um tema complexo, de natureza multidisciplinar, composto por variáveis de campos de conhecimento como economia, finança, teoria organizacional, direito, sociologia, ética, comunicação e teoria da informação, dentre outros. Percebe-se que governança tem a ver com aspectos como a cúpula da organização, sua alta administração, relacionamentos, desempenho e distribuição dos resultados empresariais entre outros tópicos. O ponto comum das definições é o entendimento da governança como uma ferramenta – um sistema ou conjunto de práticas; mas seria ela apenas uma ferramenta? Não seria mais interessante se a governança fosse entendida como o próprio governo organizacional *per se*, com o sentido de coordenação ou administração de atividades econômicas pelo topo da organização? (RODRIGUEZ; BRANDÃO, 2010, p. 8).

O assunto governança corporativa, além carregar grande importância para as organizações, é premissa para o entendimento da governança de TI e, conseqüentemente, para a gestão das ferramentas tecnológicas utilizadas pelas empresas nos dias de hoje. Isso se dá porque os interesses de todas as partes interessadas no negócio (acionistas, empregados, clientes e fornecedores, entre outros) influenciam as estratégias organizacionais e determinam grande parte das ações no dia a dia das empresas. É justamente nesse contexto que a governança corporativa é concebida.

Mesmo não apresentando definição própria aceita por todas as entidades envolvidas, pode-se conceituar governança corporativa como uma lista de práticas objetivando a otimização do

desempenho de uma corporação, prezando pela proteção de investidores, empregados e credores, facilitando, desse modo, o acesso ao capital.

Outras definições apontam a governança corporativa como um mecanismo ou fundamento em que se baseiam os processos decisórios dentro das organizações, sempre em busca do equilíbrio entre a produtividade e competitividade da empresa, por meio de uma execução de práticas transparentes e responsáveis.



Saiba mais

Para conhecer um pouco mais sobre os conceitos de governança corporativa, acesse o site indicado a seguir, do Instituto Brasileiro de Governança Corporativa (IBGC):

<<http://www.ibgc.org.br>>.

O histórico que detalha o surgimento da governança corporativa envolve diversos fatos associados ao próprio desenvolvimento das corporações, do capitalismo e de tudo aquilo relacionado ao que se entende por estruturas organizacionais.

Segundo Rossetti e Andrade (2012), os fatos relacionados à evolução do capitalismo e das corporações que provocaram o surgimento da governança corporativa se originaram primeiro na ética calvinista, passando pelo surgimento do liberalismo e pela revolução industrial, até ocorrer a transposição histórica do poder da terra para o poder do capital. A partir de então, favoreceu-se de modo decisivo o surgimento das grandes corporações e das sociedades anônimas.

Também é impossível não contemplar o desenvolvimento da ciência da administração como um outro propulsor da importância da governança. Desse modo, o desenvolvimento do capitalismo, o gigantismo das corporações e a consequente dispersão do capital de controle levaram ao que se conhece como conflito na relação de agência.

O divórcio entre propriedade e gestão gerou duas figuras interessantes: os proprietários que não detêm o controle e os controladores efetivos que não detêm propriedade. Nessa configuração, o proprietário mantém apenas dois interesses específicos: o aumento do valor de mercado da empresa e o aumento do retorno de seus investimentos. Por outro lado, surge a figura da diretoria executiva, os gestores, com seus compromissos de atender as expectativas dos proprietários, além de atender suas próprias expectativas. Tal é o contexto do conflito na relação de agência.



Lembrete

O tema da governança corporativa tem uma ligação muito forte com o tema da estratégia. Isso porque governança nos remete para o futuro, assim como estratégia.

7.1.2 Princípios da governança corporativa

Conhecido também como valores da governança corporativa, os princípios se colocam como o ponto de intersecção entre concepções, práticas e processos de alta gestão que conferem sustentação a ideias associadas ao governo das empresas.

Os princípios da governança corporativa são: senso de justiça, transparência, prestação de contas e compliance.

O senso de justiça está relacionado à equidade no tratamento dos acionistas da corporação, de modo a haver um respeitoso tratamento dos direitos dos controladores, minoritários e majoritários.

A transparência, muito valorizada no mundo corporativo, impacta os negócios e é condição fundamental para a credibilidade das suas informações financeiras e estratégicas, sobretudo se a empresa é de capital aberto.

A prestação de contas e o compliance completam os princípios e envolvem a responsabilidade e a conformidade com normas regulamentadoras, bem como estatutos sociais e regimentos internos das organizações.

Rossetti e Andrade (2012) ainda mencionam que valores da governança corporativa podem ser facilmente, de modo implícito ou explícito, verificados nos códigos de boas práticas, que normalmente enraizam posturas éticas na condução dos negócios, quando considerados.

7.1.3 Ambiente e órgãos da governança corporativa

A governança é bem estruturada numa organização quando seus órgãos e ambientes são constituídos e têm as estruturas bem estabelecidas. O arcabouço estrutural está subdividido em quatro ambientes: propriedade, controle, administração e auditoria.

Alguns órgãos situam-se em mais de um ambiente e são compreendidos como estruturas com funções exclusivas e autônomas, estabelecendo vínculos entre si e atestando que a governança corporativa remete também a um sistema de relações, internas e externas, que favorecem a direção e o monitoramento das corporações.

A figura a seguir mostra ambientes e órgãos de governança encontrados em grande parte das organizações.

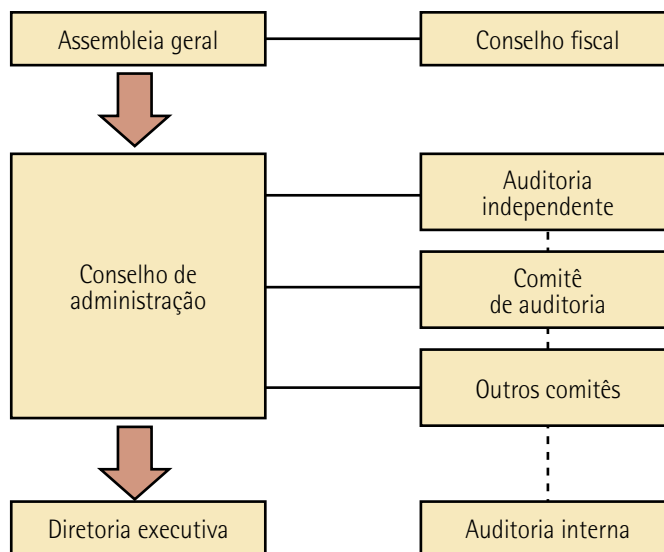


Figura 19 – Ambientes de governança corporativa

A assembleia geral é constituída pelos proprietários (acionistas controladores e minoritários), sendo considerada o órgão soberano da sociedade. Isso decorre do fato de seus poderes abrangerem todos os negócios da corporação. Suas decisões estão voltadas para a defesa, a perenidade e o crescimento da empresa. Uma das suas principais funções é eleger os membros do conselho de administração e do conselho fiscal, além de tratar da prestação de contas e demonstrações financeiras.

Embora não seja previsto em muitos países, o conselho fiscal é eleito pela assembleia geral, podendo ser composto ou não por acionistas, com um total de, no mínimo, três ou, no máximo, cinco membros. Apesar de não executar a administração, tem como incumbência fiscalizar as ações dos administradores e a gestão dos negócios, denunciando fraudes, erros e crimes, além de analisar as demonstrações financeiras.

O conselho de administração é a ligação mais íntima entre os acionistas e a direção executiva, estabelecido como um órgão de caráter nuclear guardião dos interesses dos proprietários e dotado de poderes emanados da assembleia geral. É responsável ainda pelo monitoramento de riscos, conflitos e custos na relação de agência.

A direção executiva tem como responsabilidade realizar a gestão executiva da corporação, objetivando a busca de eficácia estratégica, excelência operacional, criação de valor e otimização do retorno dos investimentos.



Observação

As estruturas de governança corporativa variam muito de acordo com o modelo implementado, de modo que alguns órgãos, como o conselho de administração, existem em todos os modelos (o que não é o caso do conselho fiscal).

7.1.4 Marcos da governança corporativa

Vejamos o que dizem Polizel e Steinberg sobre os marcos da governança corporativa.

Analizando especificamente o termo governança corporativa, quatro pessoas/instituições vinculam seu desenvolvimento: em primeiro lugar, o pioneirismo de Robert Monks, que desde 1991 escreve sobre o monitoramento das empresas pelos acionistas e, posteriormente, em 1995, publicou o livro *Corporate Governance*, que aborda vários exemplos práticos de governança em empresas norte-americanas; em segundo, Adrian Cadbury, que, em 1992, coordenou o comitê estabelecido pelo Banco da Inglaterra para elaborar o primeiro código de governança do mundo, denominado Relatório Cadbury. É possível verificar, em 1999, o terceiro marco estabelecido pela Organização de Cooperação e Desenvolvimento Econômico (OCDE), que objetiva o funcionamento adequado das organizações e dos mercados de capitais com a publicação de *Principles of Corporate Governance*. Em quarto lugar, vale destacar, passados mais de dez anos de sua promulgação, em 2002, a Lei Sarbanes Oxley, também conhecido como Lei SOX (POLIZEL; STEINBERG, 2013, p. 32).

Nas décadas mais recentes, quatro grandes marcos provocaram cada vez mais a necessidade de se ter governança corporativa nas empresas. Esses marcos davam uma ênfase especial nos oito Ps da governança corporativa: propriedade, princípios, poder, propósitos, papéis, práticas, perenidade e pessoa.

O primeiro grande marco foi o ativismo pioneiro de Robert Monks. Nascido em 1933, formou-se em Direito pela Universidade de Harvard e foi um empresário e executivo bem-sucedido. Em sua visão, existia uma série de distorções no governo das companhias, algo traçado pelos executivos, e não pelos proprietários.

No entender de Monks, a empresa que possui um monitoramento eficaz dos proprietários aumenta o seu valor e gera mais riqueza em comparação com outras que não gozam de tal benefício. A ideia de Monks era proporcionar uma aproximação efetiva da tríade acionistas-conselhos-direção.

O segundo marco é o Relatório Cadbury, divulgado em 1992 no Reino Unido, com base no trabalho de um comitê instituído pelo Banco da Inglaterra. Esse comitê foi coordenado por Adrian Cadbury e tinha por objetivo estabelecer e ressaltar a importância de dois princípios da governança: a prestação de contas e a transparência.

O relatório trazia um conjunto de práticas de governança corporativa dividido em quatro partes, destinadas a: conselho de administração, conselheiros não executivos e conselheiros executivos, além da área de relatórios e controles.

Como terceiro grande marco tem-se o estabelecimento dos princípios da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), organização que reúne os 34 países mais

industrializados do mundo. A OCDE percebeu, por volta da década de 1990, que a governança corporativa é o elo de desenvolvimento da tríade mercados-corporações-nações. Seus princípios são: enquadramento das empresas, direito e tratamento equânime dos shareholders, direito dos outros stakeholders, divulgação e transparência, responsabilidade dos conselhos de administração, gestão de riscos e avaliação da governança.

O quarto grande marco foi a Lei Sarbanes-Oxley (SOX), que causou uma ampla regulação da vida corporativa, fundamentada nas boas práticas de governança corporativa. O contexto em que a SOX foi criada engloba uma série de escândalos envolvendo grandes empresas no mercado de capitais americano.

As principais fraudes em balanços financeiros de companhias de capital aberto, que minaram a confiança dos investidores no mercado de capitais americano, envolviam a empresa do ramo energético Enron e a empresa de auditoria Arthur Andersen (empresa responsável por auditar as demonstrações e os balanços financeiros da Enron).

Essa situação levou à criação de uma lei para a proteção de investidores do mercado de capitais americano contra fraudes contábeis e financeiras. Ela foi publicada em agosto de 2002 como uma lei federal criada pelo senador americano Paul Sarbanes e pelo congressista Michael Oxley.

Entre tantas características da SOX, é possível citar:

- responsabilização civil e criminal do presidente e do diretor financeiro;
- obrigatoriedade de aderência à SOX por qualquer empresa com capital aberto na bolsa americana;
- ênfase na transparência dos dados;
- ênfase no uso de um framework de controle para avaliação de controles internos (Coso);
- adoção de penalidades mais rígidas;
- conferência de grande importância e poder a Comissão de Títulos e Câmbio dos Estados Unidos, a SEC (autoridade que regula o mercado de capitais norte-americano).

A própria estrutura da SOX e seu estabelecimento definem regras que impactam a gestão da informação das empresas e, consequentemente, a área de TI. A SOX coloca para as organizações que:

- o conteúdo da informação deve ser adequado, de modo a facilitar a transparência inerente a todas as organizações que prezam pela governança corporativa;
- a informação deve estar disponível no momento em que é necessária, facilitando auditorias e eventuais checagens;

- a informação deve ser atual (ou pelo menos a última disponível), a fim de evitar inconsistências frutos de informações que não retratem a realidade;
- os dados e as informações devem ser sempre corretos;
- a informação deve estar acessível aos usuários interessados;
- deve existir um sistema de controle interno sobre relatórios financeiros.

Como consequência dessas menções da SOX, é possível verificar alguns impactos gerados na área de TI. Isso porque as informações organizacionais (inclusive financeiras) utilizadas pelos processos de negócios são processadas, armazenadas e tratadas por sistemas de informação (SI). Esses SI operam sobre toda uma infraestrutura tecnológica que precisa operar com disponibilidade, continuidade e integridade.

7.1.5 Modelos de governança corporativa

O modelo de governança corporativa a ser adotado pelas organizações dependerá do ambiente institucional no qual as empresas encontram-se situadas. Desse modo, o Estado, ao estabelecer regulamentações influencia, em certo grau, o mercado de capitais e a proteção do patrimônio dos investidores. Assim, segundo as diversidades encontradas em cada país, os modelos de governança possuirão diferenças significativas entre si.

A saber, os cinco modelos de governança corporativa que mais se destacam são o anglo-saxão, o alemão, o japonês, o latino-europeu e o latino-americano.

O modelo anglo-saxão refere-se às práticas de governança corporativa da Inglaterra e dos Estados Unidos, apresentando como principal foco a dispersão do controle acionário e o divórcio bem definido entre propriedade e gestão. Desse modo, as corporações são financiadas por mercado de capitais, existindo intensa atuação de forças externas. Essas forças exercem papel preponderante e são representadas, por exemplo, pelos fundos de pensão, que mobilizaram outras instituições, criando-se, assim, um conselho de investidores institucionais.

O modelo anglo-saxão tem sua orientação baseada no mercado e no seu monitoramento. Isso se dá pela influência da SOX e das estruturas regulatórias estabelecidas pelo Estado, que têm em vista a segurança dos acionistas, como destacam os autores Rossetti e Andrade.

Sua fonte é o Direito Comum e entre os últimos institutos legais destacam-se a Sarbanes-Oxley Act, nos Estados Unidos; o Combined Code no Reino Unido, The Governance Policy, no Canadá, sob grande influência da lei americana; e The Corporation Act, na Austrália. Como contrapartida da pulverização do controle, os acionistas são protegidos por exigências que vão da adoção de padrões contábeis certificados à responsabilização legal dos gestores pelos números apresentados, com multas pesadas e penas de prisão nos casos de demonstrações fraudulentas (ROSSETTI; ANDRADE, 2012, p. 345).

O modelo de governança alemão denota as técnicas de governança corporativa praticadas na Alemanha, com grande e clara influência do processo de reconstrução de sua economia. Esse é um dos motivos de o capital de controle das companhias ser fortemente concentrado. O sistema alemão é claramente orientado a todos os stakeholders, ou seja, não tem como objetivo apenas os interesses dos proprietários, mas de todos os envolvidos (acionistas, credores, empregados e outras partes externas interessadas).

O modelo de governança corporativa japonês tem suas origens no processo da economia japonesa pós-Segunda Guerra Mundial, tendo interessantes semelhanças com o modelo praticado na Alemanha. Por esse motivo, é comum uma associação entre os dois modelos, chamada pela literatura da área de modelo nipo-germânico.

As semelhanças entre o modelo alemão e o japonês estão relacionadas com a importância dos bancos na estrutura de capital, no monitoramento e no controle das corporações; com a prática do consenso no processo de gestão; e com a consideração de múltiplos interesses. Já as diferenças prevalecem na estrutura de propriedade, na constituição e na efetividade dos Conselhos de Administração, nas questões centrais de governança (ANDRADE; ROSSETTI, 2012, p. 364).

O modelo de governança asiático tem características-chave de processos de governança mais próximos dos europeus. Isso se dá por conta das influências culturais e institucionais que colonizadores europeus trouxeram ao longo da formação histórica ou no processo mais recente de desenvolvimento industrial de países como Índia, Coreia do Sul, Malásia e Indonésia, entre outros.



Observação

Entre os países asiáticos, a China pode ser considerada a mais afastada das práticas de governança corporativa, pois ainda experimenta um tipo de transição para o sistema capitalista.

O modelo de governança latino-europeu engloba as técnicas e métodos de governança em países como Itália, França, Espanha e Portugal, onde a principal característica é a falta de definição de fonte de financiamento com propriedade concentrada. Dessa forma, há uma expressiva quantidade de empresas controladas por famílias e consórcios.

[...] são bastante semelhantes as características dominantes dos modelos de governança latino-europeu e latino-americano. Esses modelos distanciam-se dos padrões anglo-saxão e nipo-germânico. Do primeiro, pelo tipo mais comum de conflito de agência, que, no caso, é de expropriação, envolvendo acionistas majoritários e minoritários. Do segundo, pela ênfase atribuída a interesses múltiplos, que, no caso, não está ainda estabelecida, mas em transição (ROSSETTI; ANDRADE, 2012, p. 374).

Presente em países como Brasil, Argentina, Chile, Colômbia, México e Peru, o modelo latino-americano apresenta grande concentração patrimonial, grandes grupos privados familiares, tímida expressão do mercado de capitais e tradição jurídica do código civil latino-europeu. Além dessas características, alguns desses países têm passado por mudanças em seus sistemas econômicos, com aumento da ênfase nas privatizações e uma abertura cada vez maior do mercado.

7.1.6 Governança corporativa no Brasil

Ao observar a situação brasileira, percebe-se grande influência de dois fatores na governança corporativa. A primeira é a cultura nacional e a segunda, o contexto econômico (que ao longo da história demonstra sinais de certa constância). Esses fatores impactam fortemente os princípios e as estruturas de poder das corporações.

Segundo Rossetti e Andrade (2012), megamudanças globais agiram como forças modeladoras da governança corporativa no Brasil, interferindo em princípios, propósitos, processos e práticas de governança corporativa adotadas no país, envolvendo condições que prevalecem no macroambiente global e que impactam os mercados reais e financeiros. As principais megamudanças são descritas a seguir.

- Concepções político-ideológicas dominantes: existência de uma radicalização político-ideológica, marcada por dois sistemas claramente adversos (capitalismo liberal e o coletivismo de estado).
- Ordem geopolítica global: existência de um novo processo de macroalianças continentais caminhando de modo oposto a movimentos antiglobalização.
- Ordem econômica global: existência de ações no caminho da desregulamentação e liberalização das economias.



Observação

No Brasil é comum a intensa concentração da propriedade em acionistas majoritários, existindo uma sobreposição entre propriedade e direção executiva. Normalmente, os membros do conselho de administração só representam os interesses dos acionistas controladores ou majoritários, e os acionistas minoritários têm pouca ou nenhuma influência.

A criação do Instituto Brasileiro de Governança Corporativa (IBGC), antigo Instituto Brasileiro de Conselhos de Administração (IBCA), foi um dos maiores propulsores da disseminação das boas práticas de governança corporativa em empresas brasileiras. O IBGC lançou o primeiro Código Brasileiro das Melhores Práticas de Governança Corporativa em um período de estabilização na economia que fomentou o crescimento do país.

Além das ações desenvolvidas pelo IBGC, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) criou em outubro de 2000 o Programa de Apoio às Novas Sociedades Anônimas. O objetivo

desse programa era apoiar pequenas e médias empresas, mediante operações de capital de risco, a adotar práticas adequadas de governança corporativa. Desse modo, o BNDES teria uma participação nessas companhias pela subscrição de ações ou debêntures conversíveis em ações no percentual máximo de 35% no capital futuro da companhia.

Ainda por parte do governo, a cartilha de governança corporativa (CVM) aumentou a capacidade de intervir, de forma transparente e ativa, defendendo a adoção de melhores práticas de governança com o intuito de afastar a desconfiança da sociedade e dos investidores, desestimulando práticas predatórias. Por isso, em junho de 2002, a CVM divulgou amplamente no mercado a cartilha Recomendações da CVM sobre Governança Corporativa.

7.1.7 Desdobramentos da governança corporativa

O entendimento sobre governança corporativa pode e deve ser desdobrado em práticas que tornem mais transparentes, organizadas e legítimas as ações de direção e monitoramento das diversas áreas das corporações. Também é importante perceber que seus métodos não são limitados a uma visão macro das corporações, restritas apenas à alta direção, mas para todas as outras áreas do ambiente organizacional.

Desse modo, tais mecanismos habilitam a governo de cada ativo em particular da empresa no que tange a gerenciamento, controle e utilização que passa pelas áreas financeira, comercial, de TI, de recursos humanos e de departamento pessoal, entre todas as outras.

Daí brota a ideia de que assim como existe uma governança corporativa, é necessário que exista um desdobramento em governanças financeira, comercial, de TI, de recursos humanos, de departamento pessoal e tantas quantas forem necessárias para que haja a efetiva conversão da estratégia e dos comportamentos desejáveis em práticas disseminadas em toda a empresa.

7.2 Frameworks de governança de TI

7.2.1 Motivadores da governança de TI

Vejamos o que dizem Weill e Ross sobre os motivadores da governança de TI.

As empresas de melhor desempenho têm sucesso onde as outras fracassam porque implementam uma Governança de TI eficiente para sustentar suas estratégias. Por exemplo, firmas com uma Governança de TI acima da média que seguiam uma estratégia específica (a intimidade com o cliente, por exemplo) tiveram lucros mais de 20% superiores aos de firmas com má governança que seguiam a mesma estratégia. Definimos a Governança de TI como a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização da TI. A Governança de TI não consiste na tomada de decisões específicas sobre Tecnologia da Informação – a administração já faz isso –,

mas determina quem sistematicamente toma tais decisões e contribui para elas. Reflete princípios mais amplos da governança corporativa, ao mesmo tempo em que se concentra na administração e utilização da TI para concretizar metas de desempenho corporativo. A Governança de TI eficaz estimula e amplifica a engenhosidade dos funcionários no emprego da TI e assegura a observância da visão e dos valores gerais da empresa (WEILL; ROSS, 2006, p. 2).

Com o seu surgimento motivado não somente por questões financeiras, a governança de TI desponta como uma das áreas mais importantes que tem relação com a gestão de TI e com a gestão de SI. Lunardi, Becker e Macada (2012) pontuam em seu artigo intitulado "Um estudo empírico do impacto da governança de TI no desempenho organizacional" que a performance das empresas que adotam práticas de governança de TI é muito superior à performance daquelas que não adotam.

Com uma visão um pouco mais abrangente, Fernandes e Abreu (2012) estabelecem alguns motivadores da governança de TI. A figura a seguir reproduz esses motivadores.

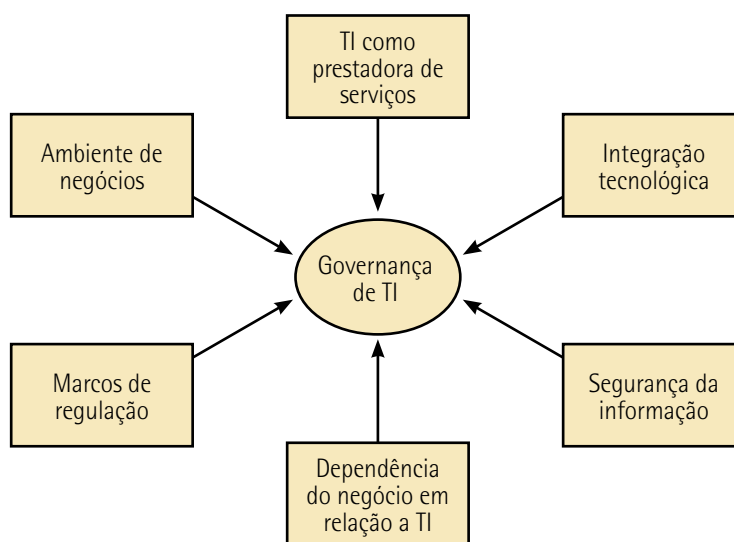


Figura 20 – Motivadores da governança de TI

Considerando esses motivadores e observando a evolução da área de TI, percebe-se a perda da imagem de uma simples provedora de infraestrutura para se tornar uma provedora de serviços. Isso, inevitavelmente, resulta na consciência de que as áreas de negócio não mais dependem do ferramental que a TI provê, mas do valor agregado de seus serviços entregues. Contudo, se os seus serviços não forem bem gerenciados e governados, impactos negativos incidirão sobre as estratégias dos negócios.

Também a utilização contínua e sistemática de ferramentas tecnológicas integradoras nas áreas de negócios tem contribuído decisivamente para a extinção de aplicativos legados motivadores da existência de verdadeiras ilhas de informação, gerando integração entre funções administrativas, fornecedores e clientes, entre outros stakeholders. Não obstante, não

se associando o uso dessas ferramentas a mecanismos eficazes de governança de TI, essa integração tecnológica poderá aumentar consideravelmente os riscos que a TI representa para a disponibilidade dos negócios.

Voltando à perspectiva financeira, Lunardi, Becker e Macada (2012) mencionam a percepção de que o ferramental da governança de TI aumenta de modo marcante a eficiência das organizações por meio de redução de custos ou da melhor utilização dos ativos. No entanto, ainda na mesma pesquisa de Lunardi, Becker e Macada (2012), uma comparação entre executivos brasileiros e de outros países aponta que os oriundos de organizações brasileiras ainda veem benefícios da TI mais ligados a processos operacionais do que estratégicos.

Ainda sobre motivadores que justificam a importância da governança de TI para as corporações, Weill e Ross (2006) mencionam algumas razões que justificam a necessidade de sua implementação, descritas a seguir.

- Compensações financeiras altas: há consideráveis diferenças nos resultados financeiros entre as empresas que têm e as que não têm governança de TI implementada. Aquelas que possuem governança têm um incremento no retorno de seus investimentos de até 20%.
- Altos custos relacionados a TI: os investimentos em TI das empresas caminham, nos dias de hoje, em torno de 6% a 7% da receita anual, requisitando, naturalmente, grande atenção da alta direção e gerando a necessidade de se governar bem a TI.
- TI oportunidade e ameaça: quando a TI não é considerada e dela não são extraídas as oportunidades, é possível que ela se torne uma ameaça. Isso porque, ao ignorar os ganhos com TI, desperdiça-se uma oportunidade, entregando à concorrência esse ganho e, conseqüentemente, transformando a oportunidade em ameaça. Esse também é um motivo para se governar a TI, para que ela seja melhor utilizada.
- Capacidade limitada da alta gerência: a alta gerência das corporações não consegue, eficientemente, atender todas as necessidades de gestão das mais diversas áreas do ambiente organizacional, inclusive da TI, gerando gargalos indesejáveis. Por isso, estabelecer governança de TI proporciona um processo decisório de gestão mais claro e transparente.

7.2.2 Conceito de governança de TI

Os principais conceitos mais aceitos de governança de TI apresentam-na como um sistema composto de aspectos de liderança, estruturas organizacionais e de processos que garantam que a área de TI apoie e desdobre os objetivos da organização (ITGI, 2007).

Assim como a governança corporativa, a governança de TI é de responsabilidade da alta direção e dos executivos, além de precisar de sua total adesão no processo de implementação. Isso se dá porque ter governança é necessariamente ter direção e controle para controlar o uso futuro e atual da TI (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).



Lembrete

A estratégia sempre nos remete para o futuro, e a governança também.

Ainda segundo Weill e Ross (2006), a governança de TI é a especificação de direitos de decisão e determinação de responsabilidades no estímulo de comportamentos desejáveis na utilização da TI. Esses comportamentos desejáveis, que geram valor para as empresas, associados às estratégias, interligam a governança corporativa à de TI.

O alinhamento estratégico da TI é o principal objetivo da governança de TI, porque ele contribui para o desdobramento dos objetivos de negócios em objetivos de TI. No entanto, é possível encontrar outros objetivos, não menos importantes: posicionamento esclarecido da TI em relação às outras áreas das organizações, estabelecimento de responsabilidades relacionadas às decisões críticas da TI, implementação de um conjunto de processos e controles que habilite a gestão de riscos e compliance, alinhamento de iniciativas de infraestrutura, arquitetura, aplicações e investimentos de TI com as estratégias empresariais.

Weill e Ross (2006) afirmam que a eficácia na governança de TI é alcançada quando três questões específicas são tratadas: decisões inter-relacionadas de TI, arquétipos decisórios e mecanismos para a tomada de decisão.

As decisões inter-relacionadas de TI são compostas de princípios de TI, arquitetura da TI, infraestrutura de TI, necessidades de aplicações de negócios e investimentos e priorização da TI. Os arquétipos decisórios são definidos como os tomadores dessa decisão e podem ser enquadrados como monarquia de negócios, monarquia de TI, feudalismo, duopólio de TI ou anarquia. Os mecanismos para a tomada de decisão tratam do modo e da forma como (com quais mecanismos) essas decisões devem ser tomadas e monitoradas. São eles: estruturas e comitês de tomada de decisão, processos de alinhamento e abordagens de comunicação.



Saiba mais

Para conhecer um pouco mais sobre tomada de decisão em TI, leia a obra indicada a seguir:

WEILL, P.; ROSS, J. W. *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores*. São Paulo: M. Books, 2006.

7.2.3 Modelos de governança de TI

Existem diversos requisitos para se implementar adequadamente a governança de TI: liderança para executar mudanças, envolvimento da alta direção, equipe qualificada e a adoção de um modelo de governança de TI.

A adoção de um modelo de governança de TI é fundamental para o alcance dos objetivos de TI alinhados aos negócios. Entre os modelos e frameworks de TI, aqueles com foco exclusivo na governança são o modelo Cobit e a norma da ISO 38500.

Weill e Ross (2006) propõe também um framework para governança de TI, o qual dispõe de uma harmonização entre as estratégias organizacionais, os arranjos de governança de TI e as métricas de desempenho do negócio. Tudo é colocado por meio de práticas de organização da TI e de comportamentos desejáveis.



Saiba mais

Para conhecer um pouco mais sobre esse modelo de governança de TI, você pode ler a obra indicada a seguir:

WEILL, P.; ROSS, J. W. *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores*. São Paulo: M. Books, 2006.

Fernandes e Abreu (2012) apresentam também um modelo de governança de TI genérico que pode ser aplicado em qualquer organização. Trata-se de um framework formado por componentes que podem ser encaixados como no clássico jogo de crianças Lego. A ideia desse modelo é que ele possa ser implementado de acordo com as necessidades, as prioridades e as disponibilidades da organização.



Saiba mais

Para conhecer um pouco mais sobre esse modelo de governança de TI, leia a obra indicada a seguir:

FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012.

7.2.4 Modelos de suporte à governança de TI

A área de TI pode ser concebida como um ambiente com diversas subdivisões, como: projetos de TI, processos de TI, operações de TI, negócios de TI, riscos de TI, qualidade de TI, desenvolvimento de software, terceirizações em TI, arquitetura de TI, infraestrutura de TI e serviços de TI.

Quando se defende a ideia de que a governança de TI é um desdobramento da governança corporativa, pode-se concluir que é necessário um desdobramento também da governança de TI para as outras subáreas da TI.

Então, da mesma forma que é crítico para o sucesso da governança de TI a implementação de um framework, também assim o é a implementação de frameworks e modelos que suportem a governança de TI especificamente nessa subárea.

Ao pensar, por exemplo, na subárea de projeto de TI, encontram-se pelo menos três modelos que podem suportá-la. Os mais conhecidos são: Project Management Body of Knowledge (PMBOK), Prince2 e Scrum.

O quadro a seguir mostra algumas das subáreas de TI e alguns dos modelos que suportam a governança de TI em cada uma dessas subáreas.

Quadro 7 – Modelos de gestão de TI

Subárea de TI	Modelos de suporte a governança de TI
Projetos de TI	Project Management Body of Knowledge (PMBOK). Prince2. Scrum.
Processos de TI	Guia para o Gerenciamento de Processos de Negócio - Corpo Comum de Conhecimento (BPM CBOK).
Operações de TI	Information Technology Infrastructure Library (Itil).
Negócios de TI	Business Analysis Body of Knowledge (Babok).
Riscos de TI	Risk IT.
Qualidade de software	Capability Maturity Model – Integration (CMMI).
Serviços de TI	Information Technology Infrastructure Library (Itil).
Arquitetura de TI	The Open Group Architecture Framework (Togaf).
Terceirizações em TI	eSourcing Capability Model (eSCM).

7.3 Modelo Cobit

7.3.1 Histórico do modelo Cobit

Vejamos o que diz o IT Governance Institute sobre o histórico do modelo Cobit.

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 (Committee of Sponsoring Organizations 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, infraestrutura 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 (ITGI, 2007, p. 7).

O modelo de governança de TI chamado Cobit foi criado em 1994 para a Information Systems Audit and Control Association (Isaca). A ideia inicial, já reformulada nos dias de hoje, foi desenvolver um conjunto de práticas e controles para a área de TI tendo em vista uma maior aderência às necessidades de negócio.

O modelo foi constituído a partir do framework Coso, utilizado em controles de governança corporativa, mas também recebeu incrementos originados de vários padrões internacionais e práticas de gestão de TI oriundas de diversas instituições que trabalham padronizações em gestão.

Hoje, o Cobit é mantido pelo Instituto de Governança de TI (ITGI), que nada mais é que um "braço" criado pela Isaca para manter o modelo, preservar sua missão e trabalhar um processo de melhoria contínua e atualização com base nas novas necessidades e requisitos existentes e demandados pelas áreas de negócios.

Segundo o ITGI, a missão do Cobit é:

pesquisar, desenvolver, publicar e promover um framework de controle para Governança de TI que seja embasado, atualizado, internacionalmente aceito para a adoção pelas organizações e usado no dia-a-dia pelos gerentes de negócio, profissionais de TI e profissionais de auditoria (ITGI, 2007, p. 5).

Com base na missão estabelecida, o modelo é destinado à governança de TI e precisa auxiliar a alta direção das organizações que estão relacionadas a riscos, valor e controle, estabelecendo uma metodologia segura para o alinhamento estratégico entre TI e negócio, maximizando os benefícios alcançados por meio dos recursos de TI.

Baseado nesse entendimento, o Cobit evoluiu decisivamente, conforme é possível verificar no quadro a seguir.

Quadro 8 – Evolução do Cobit

Ano	Versão	Foco
1996	1	Auditoria
1998	2	Controle
2000	3	Gerenciamento
2005	4	Governança
2007	4.1	Governança
2012	5	Governança e gestão

7.3.2 Características do modelo Cobit

As mais importantes características do modelo Cobit são: foco voltado para o negócio, orientação clara a processos, gerenciado por métricas e fundado em controles.

O foco voltado para o negócio é considerado a principal característica. Isso se dá porque a TI precisa ser percebida e concebida na perspectiva do negócio, ou seja, as expectativas e os objetivos empresariais precisam ser traduzidos em ações concretas na área de TI, de modo que haja alinhamento entre TI e negócio.

A característica do foco voltado para os negócios do Cobit estabelece fundamentações básicas para o uso do framework nas empresas. Assim, o modelo Cobit tem como fundamento que os requisitos de negócios direcionam investimentos de TI, mais especificamente em recursos, que são utilizados pelos processos de TI tendo em vista gerar a informação organizacional necessária para o negócio. A figura a seguir apresenta essa ideia.

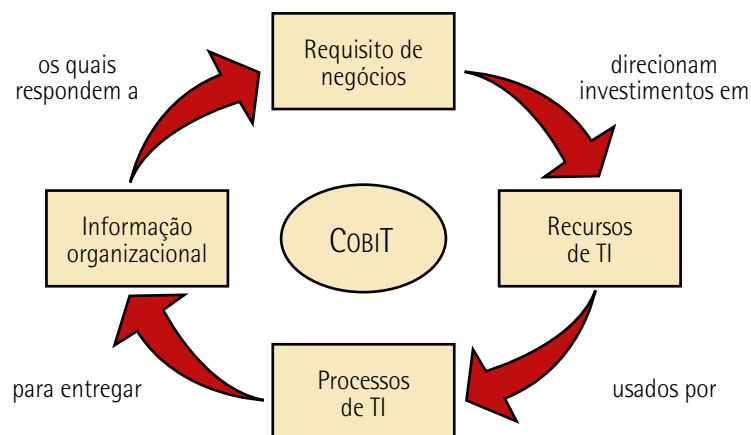


Figura 21 – Características do Cobit

A orientação clara a processos é colocada como característica, porque o Cobit tem as suas atividades baseadas completamente em processos e com uma linguagem comum, de modo que a organização visualize e gerencie a área de TI. Os processos dividem-se em quatro domínios e permeiam as áreas de responsabilidade da TI: planejamento, construção, processamento e monitoramento.

O Cobit também é um modelo gerenciado por métricas. Essa característica traduz o nível de performance da área de TI, avaliando sua maturidade e a performance dos processos e das atividades.

O Cobit também é fundado em controles. Há controles em vista do uso de qualquer um dos seus processos e atividades da TI. Por meio deles, são definidas políticas, procedimentos, práticas e estruturas organizacionais, garantindo que metas de negócios sejam atingidas ou, de certo modo, evitando ou corrigindo situações não desejadas.

7.3.3 Cobit 4.1

Ainda muito utilizado pelas organizações, o Cobit 4.1 é composto de três elementos fundamentais: processos, requisitos de negócios e recursos de TI. A figura a seguir apresenta esses componentes.

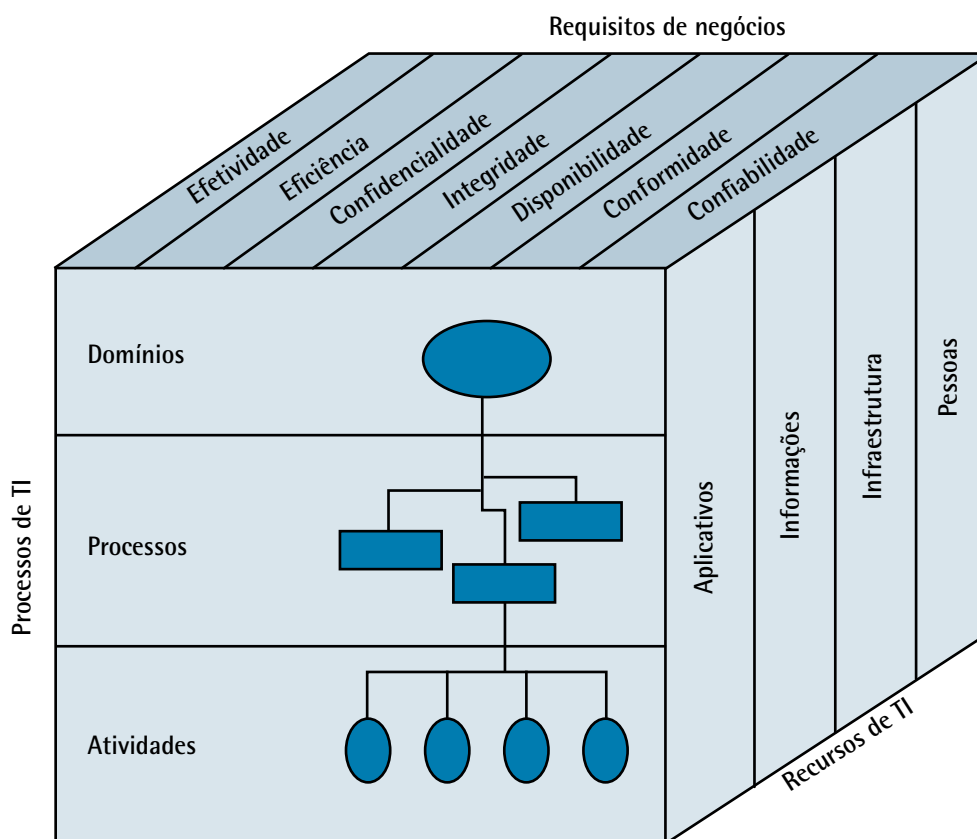


Figura 22 – Componentes do Cobit

Considerado o componente básico do modelo, os processos trazem praticamente todas as atividades-padrão de uma área de TI. Eles são em número de 34, divididos em quatro domínios: planejar e organizar (PO), adquirir e implementar (AI), entregar e suportar (ES) e monitorar e avaliar (MA).

Os requisitos de negócios também são conhecidos como critérios de informação. São critérios de controle que objetivam adequar as informações ao atendimento dos objetivos de negócios.

O quadro a seguir apresenta os conceitos de cada requisito de negócio.

Quadro 9 – Critérios da informação

Critério de informação	Descrição
Efetividade	Remete a informação importante para os processos de negócio entregue no tempo e modo correto, consistente e utilizável.
Eficiência	Define a entrega da informação com o uso mais produtivo possível dos recursos.
Confidencialidade	Relaciona-se a segurança de informações, no que tange ao aspecto confidencialidade para evitar a divulgação indevida.
Integridade	Remete a fidedignidade, inteireza e totalidade da informação, além da sua validade quando comparada aos requisitos de negócios solicitados.
Disponibilidade	Trata-se da disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro.
Conformidade	Está relacionado ao cumprimento de questões de compliance a que os processos de negócios estão sujeitos.
Confiabilidade	Remete a entrega da informação apropriada solicitada pelo negócio.

Fonte: IT Governance Institute (2007, p. 28).

Os recursos de TI representam o suporte para os processos e as atividades de TI, de modo a entregar o valor que o negócio necessita. Segundo o ITGI (2007), os recursos de TI são: aplicativos, informações, infraestrutura e pessoas.

Os aplicativos são sistemas de software destinados a usuários e processos. As informações representam o conjunto de dados relacionados usados em qualquer formato a ser utilizado pelos negócios. A infraestrutura é composta de recursos tecnológicos como hardware, sistemas operacionais, bancos de dados, redes de computadores e os ambientes que os abrigam, a fim de possibilitar o processamento dos aplicativos. As pessoas são aquelas que planejam, organizam, adquirem, implementam, entregam, suportam, monitoram e avaliam os sistemas de informação e serviços de TI, podendo ser internos, terceirizados ou contratados, conforme a necessidade.

Os processos representam a base do modelo Cobit. Eles cobrem praticamente todas as tarefas-padrão da área de TI e se apresentam em número de 34, divididos em quatro domínios: planejar e organizar (PO), adquirir e implementar (AI), entregar e suportar (ES) e monitorar e avaliar (MA).

O domínio planejar e organizar abrange as estratégias e táticas da corporação relacionadas à TI, preocupando-se na forma como o valor pode ser entregue por meio de recursos tecnológicos. O domínio adquirir e implementar cobre a identificação, o desenvolvimento e/ou a aquisição de soluções de TI para executar a estratégia de TI estabelecida. O domínio entregar e suportar refere-se à entrega dos serviços solicitados, ao gerenciamento da segurança e continuidade, ao gerenciamento de dados e aos recursos operacionais. O domínio monitorar e avaliar refere-se ao gerenciamento do desempenho, ao monitoramento do controle interno, à aderência regulatória e à governança.

Os processos do Cobit e seus respectivos códigos podem ser vistos no quadro a seguir.

Quadro 10 – Processos do Cobit

Domínio	Código	Processo
Planejar e organizar	P01	Definir um plano estratégico de TI.
	P02	Definir a arquitetura da informação.
	P03	Determinar o direcionamento tecnológico.
	P04	Definir processos, organização e relacionamentos de TI.
	P05	Gerenciar o investimento de TI.
	P06	Comunicar as diretrizes e expectativas da diretoria.
	P07	Gerenciar os recursos humanos de TI.
	P08	Gerenciar a qualidade.
	P09	Avaliar e gerenciar os riscos de TI.
	P010	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	ES1	Definir e gerenciar níveis de serviços.
	ES2	Gerenciar serviços terceirizados.
	ES3	Gerenciar o desempenho e a capacidade.
	ES4	Assegurar a continuidade dos serviços.
	ES5	Assegurar a segurança dos sistemas.
	ES6	Identificar e alocar custos.
	ES7	Educar e treinar os usuários.
	ES8	Gerenciar a central de serviço e os incidentes.
	ES9	Gerenciar a configuração.
	ES10	Gerenciar problemas.
	ES11	Gerenciar os dados.
	ES12	Gerenciar o ambiente físico.
	ES13	Gerenciar as operações.
Monitorar e avaliar	MA1	Monitorar e avaliar o desempenho de TI.
	MA2	Monitorar e avaliar os controles internos.
	MA3	Assegurar a conformidade com requisitos externos.
	MA4	Prover governança de TI.

Adaptado de: IT Governance Institute (2007, p. 30).

A implementação de melhorias no ambiente organizacional pressupõe uma análise de sua situação inicial, a fim de saber qual é o caminho a ser tomado. Essa é justamente a análise conhecida como de maturidade. Especificamente para a área de TI, a ideia é descobrir o quão madura ela é em matéria de processos do Cobit.

O modelo de maturidade para o gerenciamento e o controle dos processos de TI, segundo o Cobit, baseia-se em uma metodologia de avaliação originada do Software Engineering Institute (SEI). Essa metodologia avalia a maturidade de cada processo do Cobit dentro de uma escala que vai de zero a cinco.

- Nível 0: inexistente. Completa falta de um processo reconhecido, além de a corporação não reconhecer a necessidade de processos.
- Nível 1: inicial. Existem evidências de que a empresa reconheceu a existência de questões a serem trabalhadas. Nesse nível não há processo padronizado.
- Nível 2: repetível, porém intuitivo. Processos sofreram uma evolução para procedimentos seguidos por diferentes pessoas. No entanto, não há treinamento e comunicação formal, sendo a responsabilidade atribuída a cada indivíduo.
- Nível 3: processo definido. Procedimentos não são sofisticados, mas foram padronizados, documentados e comunicados por meio de treinamento. Processos são seguidos, no entanto, desvios não são detectados.
- Nível 4: gerenciado e mensurável. Há aderência a procedimentos, e ações corretivas são tomadas quando necessário, fornecendo boas práticas e constantes aprimoramentos.
- Nível 5: otimizado. Processos encontram-se refinados pareados com as melhores práticas, baseados em um resultado de contínuo aprimoramento e modelagem da maturidade com outras organizações.

Exemplo de aplicação

Escolha um processo do Cobit para a empresa em que você trabalha (ou outra a que você tenha acesso) e tente descobrir o nível de maturidade nesse processo.

7.3.4 Cobit 5

Por ser um modelo bem estruturado, o Cobit na versão 5 agrega valores e benefícios para a organização na qual ele foi implantado. Porém esses benefícios só serão possíveis se todo o processo de implementação for realizado corretamente e possuir, posteriormente, um acompanhamento diário. Todo processo que visa à qualidade necessita de atenção e dedicação constante e é passível de ajustes, a fim de se obter uma melhoria continuada.

Com a utilização contínua do Cobit 5 como modelo de governança de TI, os benefícios são inúmeros. Observe alguns exemplos listados a seguir.

- Apresentar uma visão clara dos facilitadores da TI e suas vulnerabilidades.
- Maior assertividade na tomada de decisão (uma vez que há processos definidos, estruturados e controlados, tem-se mais transparência nas informações e melhor visibilidade do negócio).
- Gerenciar informações de alta qualidade para suportar as decisões de negócios.
- Atingir metas estratégicas e entregar benefícios de negócio por meio do efetivo uso da TI, gerando, assim, ganho de valor dos investimentos em TI.
- Tangenciar a excelência operacional por intermédio da aplicação confiável e eficiente da TI.
- Reduzir a exposição a riscos relacionados com a TI.
- Aperfeiçoar e equilibrar os custos de serviços de TI.
- Manter a conformidade com leis, regulamentos, acordos contratuais e políticas.
- Redução dos custos operacionais e do acervo de TI.
- Aumento significativo da visibilidade a todos os níveis da organização (em decorrência dos esforços de melhoria implantados pelos processos).
- Maior solidez no planejamento estratégico, pois possuem dados mais confiáveis e íntegros.

A família de produtos Cobit 5 é composta dos itens listados a seguir.

- Cobit 5: o modelo, que contempla uma visão geral entre a área de negócios e a gestão e governança de TI, apresentando os princípios do Cobit 5, seus passos e diretrizes, também descreve de forma resumida o guia de implementação e expõe os modelos de mapeamentos para objetivos corporativos e de TI.
- Guia habilitador de processos (Cobit 5 Enabling Process): um guia de referência detalhado de cada processo a ser definido, também inclui modelo cascata, objetivos e referências.
- Guia habilitador de informações (Cobit 5 Enabling Information): um guia que explica detalhadamente o modelo de informação e fornece exemplos de entidades de informação totalmente elaboradas. É complemento para o guia de processos.
- Guia profissional de implementação (Cobit 5 Implementation): fornece uma abordagem de boas práticas para a implementação da governança de TI com base no ciclo de vida de melhoria contínua (devendo ser adaptado às necessidades específicas da empresa).

- Guia profissional para segurança da informação (Cobit 5 for Information Security): a segurança da informação é essencial nas operações diárias das empresas, portanto, deve ser assegurada a fim de manter a confidencialidade e a integridade das suas informações (proporcionando, simultaneamente, sua disponibilidade às pessoas que devem ter acesso a elas).
- Guia profissional para risco (Cobit 5 for Risk): tem como objetivo orientar de forma específica sobre os riscos de informação em relação ao Cobit para os componentes de risco de informação da Isaca. Trata-se de um complemento do guia de segurança da informação.
- Guia profissional para garantia (Cobit 5 for Assurance): tendo como base o quadro Cobit 5, esse guia centra-se na garantia e fornece orientações mais detalhadas e práticas para os profissionais de certificação (e outras partes interessadas em todos os níveis da empresa) sobre como utilizar o Cobit 5 para suportar as atividades de garantia de TI.
- Guia profissional de programa de avaliação (Cobit 5 Assessment Programme): é base para a avaliação dos processos de uma empresa para a governança e a gestão de tecnologia da informação e serviços relacionados. Conforme descrito no Cobit 5, possui guias relacionados, como o guia de autoavaliação, o guia do avaliador e o modelo de avaliação de processos.

8 ESTRUTURAS DE GERENCIAMENTO DE REDES

8.1 Administração de redes

8.1.1 Conceitos de administração de rede

Vejamos o que diz Burgess sobre os conceitos de administração de rede.

A administração de redes e sistemas é uma ramificação da engenharia relacionada ao gerenciamento de sistemas homem-computador. É incomum uma disciplina de engenharia abordar igualmente tanto a tecnologia de sistemas de computador quanto os usuários dessa tecnologia. Trata-se de reunir uma rede de computadores (estações de trabalho, PCs e supercomputadores), colocá-los em execução e mantê-los em execução apesar das atividades dos usuários que tendem a fazer os sistemas falharem. O administrador de sistemas trabalha para os usuários, para que eles possam usar o sistema e produzir trabalho. No entanto, ele não deve satisfazer apenas uma ou duas necessidades individuais, mas trabalhar também para o benefício de toda a comunidade. Atualmente, essa é uma comunidade global de máquinas e empresas, que se estende a todo nicho da sociedade e cultura humanas, graças à Internet. Geralmente é um ato de equilíbrio difícil determinar a melhor política, que abranja as diferentes necessidades de todas as pessoas com base em um sistema. Quando um computador é conectado à Internet, temos que considerar as consequências de estar diretamente conectado com todos os outros

computadores do mundo. No futuro, os aperfeiçoamentos na tecnologia podem tornar a administração de sistemas uma tarefa um pouco mais fácil – que lide apenas com a administração de recursos – mas, atualmente, ela não é apenas um trabalho administrativo, é um trabalho de engenharia extremamente exigente. Envolve hardware, software, suporte ao usuário, diagnóstico, reparo e prevenção. Os administradores de sistema têm que saber um pouco de tudo: as habilidades são técnicas, administrativas e sociopsicológicas. Os termos administração de redes e administração de sistemas existem separadamente e são usados de maneira variável e inconsistente pela indústria e por acadêmicos. Administração de sistemas é o termo usado tradicionalmente por engenheiros de mainframe e Unix para descrever o gerenciamento de computadores, estando eles conectados ou não a uma rede. Para essa comunidade, administração de rede significa o gerenciamento de dispositivos de infraestrutura de rede (roteadores e switches). O universo dos computadores pessoais (PCs) não tem como tradição o gerenciamento de computadores individuais e seus subsistemas, e, portanto, não fala de administração de sistemas. Para essa comunidade, a administração de redes é o gerenciamento de PCs em uma rede. A administração de redes e sistemas é cada vez mais desafiadora. A complexidade dos sistemas de computador está sempre aumentando. Atualmente, mesmo um simples PC, executando o Windows NT e conectado a uma rede, se aproxima do nível de complexidade que computadores mainframe tinham há dez anos. Agora somos forçados a considerar sistemas e não só computadores (BURGESS, 2006, p. 2).

Adentrando agora especificamente no recurso redes de computadores e telecomunicações, pode-se definir administração de redes como um conjunto de tarefas com o intuito de planejar, operar, controlar e monitorar as redes de computadores.

A gestão de uma rede sempre precisa ter em vista a entrega de valor para negócio, ou seja, criar diferenciais competitivos para as organizações. Por isso, a administração das redes pode ser dividida em seis funções básicas: administração da configuração, administração do desempenho, administração da falha, suporte ao usuário final, administração de custos e gerenciamento da segurança.

Na prática, torna-se difícil dividir literalmente o trabalho do administrador de redes nessas funções, mas é possível segmentar as tarefas.

Assim, os administradores de redes devem fazer a gestão de atividades cotidianas, fornecendo suporte ao usuário e assegurando o funcionamento da rede de forma confiável. Não menos importante, o administrador de rede também precisa fazer a gestão dos recursos humanos técnicos, bem como ter um plano estratégico para atender as demandas e as expectativas do negócio.

É importante destacar também, que a administração e gestão de uma rede pode, em diversas organizações, ser executada por um gestor de Tecnologia da Informação que administra recursos

tecnológicos de forma geral, considerando não somente as redes, mas o hardware, o software e os bancos de dados.

É comum também, no gerenciamento de redes, a utilização do modelo Fault Configuration Accounting Performance Security (FCAPS) na definição do escopo das ações de gestão. Esse acrônimo nos remete a cinco aspectos muito importantes na administração de redes, descritos a seguir.

- Detecção e correção de falhas: relacionado a aspectos da operação do gerenciamento de redes.
- Configuração e operação: relacionado a configuração e implementação de hardware, software e contas de usuários.
- Contabilidade e faturamento: relacionado a custos na operação das redes.
- Avaliação de desempenho e otimização: relacionado a avaliações diagnósticas e de tendências.
- Garantia de segurança e proteção: relacionado a pilares da segurança da informação que trafega nas redes.

8.1.2 Administração da configuração

Administrar a configuração é uma das atividades do gerenciamento de redes que consiste na documentação e na gestão da configuração do hardware e software de redes, objetivando a contínua atualização das informações sobre os itens da infraestrutura de redes.

Entre as atividades mais comuns, encontra-se a gestão de contas de usuários que são acrescentados nas redes de computadores. Esses usuários são, normalmente, membros de algum grupo com privilégios distintos para acessar recursos específicos (como servidores de arquivos, diretórios e até mesmo o próprio login de acesso às redes de computadores).

Outra atividade corriqueira da administração de configuração é a atualização dos softwares dos computadores clientes. Essa ação ocorre quando há uma atualização de softwares ou sistemas utilizados pelo usuário. Claro que essa ação pode parecer simples ao considerar uma rede com poucas estações, não obstante, o trabalho torna-se penoso quando falamos em muitas máquinas.

A documentação da configuração é mais uma ação importantíssima porque consiste na coleta e na gestão das informações sobre: hardware de rede, software de rede, perfis de usuários e perfis de aplicações, entre outros.

Entre essas informações, considera-se o hardware de rede mais básica, por consistir em conjunto de diagramas de configuração de rede com detalhes sobre números, tipos e localização dos circuitos de rede, dos servidores, dos computadores clientes e de demais dispositivos (como roteadores, hubs, switches e access point, entre outros).

Os detalhes individuais de cada componente integram juntos aos diagramas as documentações individuais acrescidas de informações sobre falhas, reparos, número de telefone para reparos e quaisquer outras informações adicionais.

A figura a seguir apresenta detalhes de um diagrama utilizado na gerência de configuração.

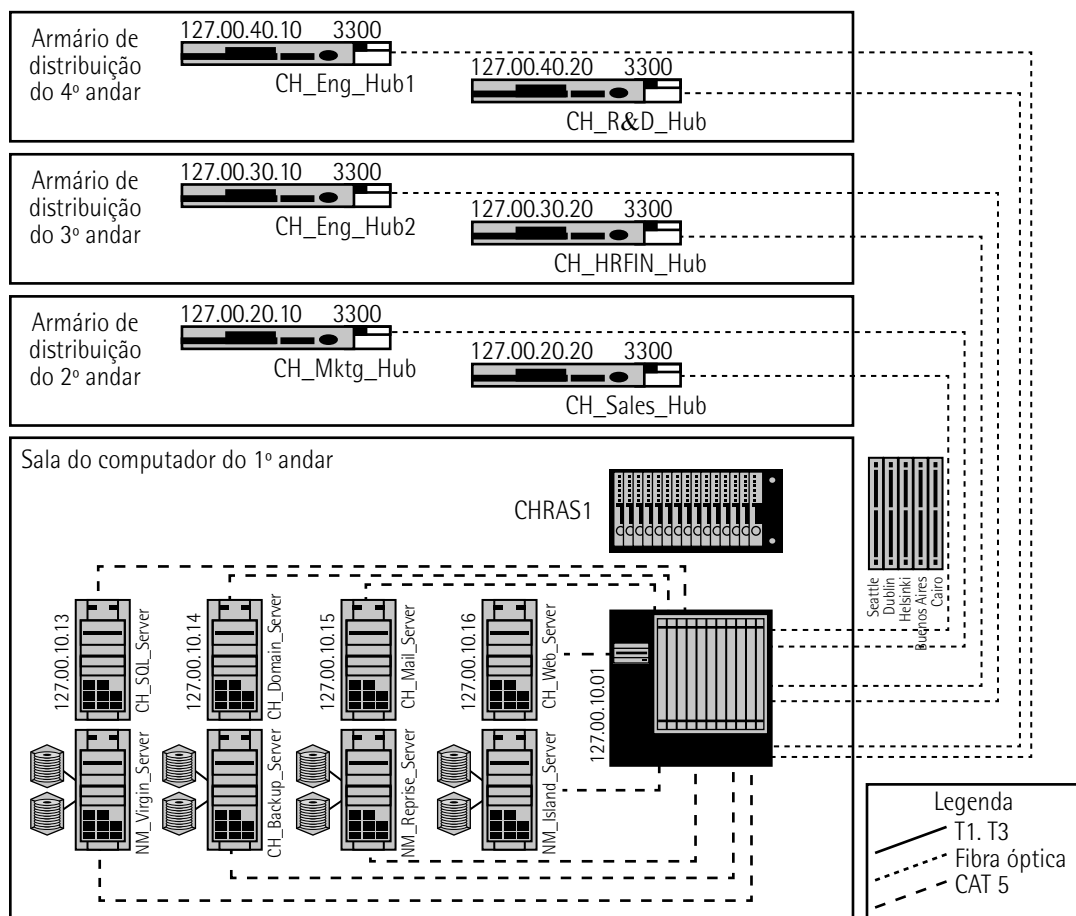


Figura 23 – Diagrama de rede

Pensando no software de rede, a gerência de configuração documenta detalhes sobre o sistema operacional de rede e todos os outros softwares específicos utilizados em rede. Estão incluídos também detalhes sobre licenças locais, pagamentos e usuários que utilizam, entre outras informações.

Dessa forma, pode-se dividir a documentação da administração da configuração em três partes, enunciadas a seguir.

- Documentação de hardware: envolvendo mapas e especificações.
- Documentação de software: envolvendo software, versão, instalação e licença.
- Documentação de conta de usuário: envolvendo informações do usuário.

8.1.3 Administração da falha

A administração de falhas remete a detecção, correção e prevenção de falhas nos recursos de redes disponíveis para o usuário. A administração de falhas, especificamente, pode ser dividida em: administração de falhas reativa e administração de falhas proativa.

Na administração de falhas reativa detecta-se, isola-se, corrige-se e registra-se a falha, com um foco na solução de curto prazo. A detecção de falhas figura como a primeira ação, tendo o intuito de promover ações de curto prazo para resolução e/ou contorno da situação encontrada. O isolamento da falha ocorre em seguida, de forma a reduzir os eventuais impactos a outros usuários. A correção de falhas promove a substituição ou o reparo do componente defeituoso, e o registro de falha consiste na documentação da situação e da solução empregada.



A documentação é de grande importância porque a resposta precisa ser imediata caso o mesmo problema ocorra novamente.

Na administração de falhas proativa a ideia é se antecipar às situações em que ocorrem as falhas (embora nem sempre isso seja possível). As ações proativas decorrem da observação feita dos recursos tecnológicos de redes.

8.1.4 Administração de desempenho

Administrar o desempenho está relacionado à garantia de que a rede funcione de forma adequada, eficiente e conforme planejado no desenho original do projeto.

A administração de desempenho e a de falhas estão intrinsicamente ligadas pelas ações de monitoramento que visam, de forma proativa, acompanhar o funcionamento e a operação das redes de computadores tendo em vista garantir a disponibilidade e a continuidade dos negócios de uma organização.

O monitoramento das redes de computadores normalmente é executado por softwares de gerenciamento de redes, os quais, por meio de protocolos estruturados, observam todo o ambiente e os recursos utilizados. No entanto, é possível perceber que, em redes pequenas, todo o trabalho de monitoramento é feito por um técnico, ao passo que, em redes maiores, os técnicos trabalham em conjunto em um centro de operações de redes, conhecido pelo seu acrônimo em inglês NOC (Network Operations Center).



O NOC é responsável pelo monitoramento e solução dos problemas de redes, diagnosticando e resolvendo problemas críticos.

A administração do desempenho monitora e busca transformar em números os aspectos de: capacidade (medindo taxas de transferências), tráfego (interno e externo baseado em pacotes), vazão (individual por equipamento ou em todo conjunto da rede) e tempo de resposta (tendo em vista descobrir a qualidade no tempo de requisição de um serviço de rede).

Tanto na avaliação de desempenho quanto na de falhas, é necessário conservar a boa prática de utilização de relatórios técnicos, úteis no fornecimento de informações que visam ao aprimoramento das redes de computadores. Os principais detalhes técnicos que devem ser incluídos em um relatório são:

- detalhamento e utilização do circuito de comunicação;
- taxa de utilização de hardwares de redes (incluindo servidores, roteadores e switches, entre outros);
- taxas de atividades de arquivos envolvendo bancos de dados em rede;
- utilização de links de comunicação de dados por parte dos computadores clientes;
- verificações do tempo de resposta de solicitações;
- relação do uso de voz e dados em um circuito;
- análise e descrição dos comprimentos de fila na transmissão de dados;
- taxas de falhas envolvendo links de dados, hardware e software de redes;
- quaisquer outros detalhes relacionados a falhas e desempenho da rede.

Com base no uso dos relatórios técnicos e com a detecção de falhas, é possível apontar os principais problemas de uma rede. Assim, é necessária também a criação de um relatório de problemas, incluindo alguns registros importantes, como:

- data e hora do relatório;
- dados relativos ao usuário que relatou o problema;
- data e hora do problema;
- localização do problema;
- natureza do problema;
- momento em que o problema foi identificado;
- por que e como ocorreu o problema.

Por meio dessas rotinas e boas práticas, é possível colher e trabalhar com as estatísticas de desempenho e de falhas, que devem ser constantemente coletadas. Essas estatísticas formam a base de conhecimento sobre problemas relacionados, favorecendo o encaminhamento de soluções rápidas e com impacto reduzido para os usuários.

A principal dessas estatísticas é a disponibilidade, que é definida como o percentual de tempo em que o recurso de redes está disponível ao usuário. Pode ser calculada como o número de horas disponíveis dividido pelo número de horas totais do mês.



Observação

A disponibilidade é calculada considerando um dia com 24 horas e um mês com 30 dias.

Outra interessante estatística é o tempo de manutenção que expressa o tempo de indisponibilidade do recurso de redes, em razão de falhas que geraram uma manutenção ou atualização. Completam ainda as estatísticas os cinco tempos enunciados a seguir.

- Tempo médio entre falhas (mean time between failures ou MTBF): número de horas ou dias de operação contínua antes da falha do componente.
- Tempo médio de reparo (mean time to repair ou MTTR): média de minutos ou horas até que o dispositivo ou circuito que falhou esteja novamente operacional.
- Tempo médio de diagnóstico (mean time to diagnose ou MTTD): média de minutos até que a raiz da causa da falha seja diagnosticada corretamente.
- Tempo médio de resposta (mean time to respond ou MTTRsp): média de minutos ou horas até que o pessoal de serviço chegue ao local do problema para começar a trabalhar nele.
- Tempo médio de conserto (mean time to fix ou MTTF): mostra a rapidez com que o pessoal de manutenção pode corrigir o problema após chegar.

Ainda nesse contexto de administração de desempenho e falhas, é importante o trabalho com relatórios de gerenciamento. Esses são de grande importância no fornecimento de informações úteis para prover uma visão global para os administradores. Devem constar nesses relatórios:

- gráficos semanais, diários e mensais, mencionando erros e demais situações pertinentes nas redes;
- disponibilidade da rede, incluindo tempo de funcionamento com histórico específico;
- percentual de horas semanais de indisponibilidade das redes;

- diagnóstico de erros;
- tempos de respostas iguais ou superiores a três segundos;
- volumes de pico no uso dos recursos de rede;
- comparação de atividade entre o dia de hoje e qualquer período prévio semelhante.

A figura a seguir apresenta um gráfico de controle de qualidade para circuitos.

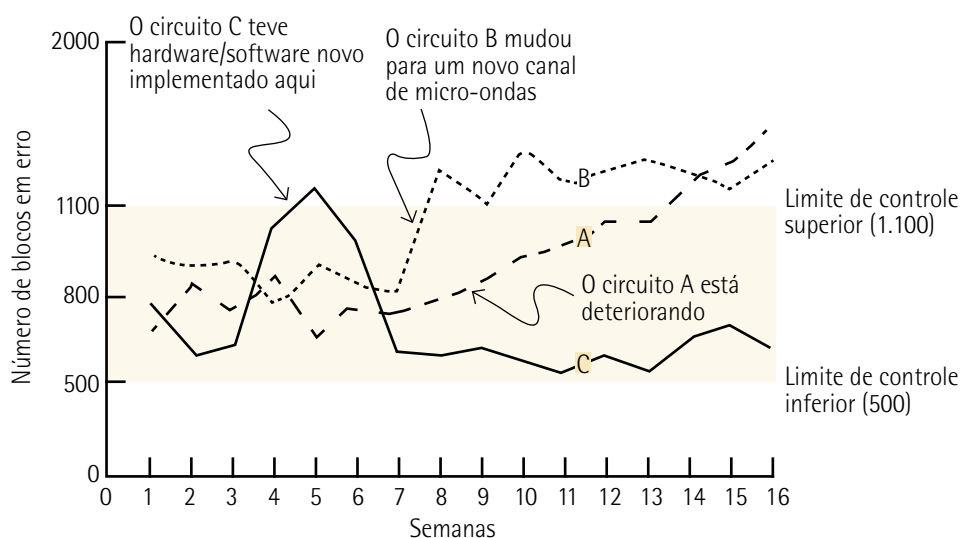


Figura 24 – Gráfico de controle de qualidade para circuitos

8.1.5 Suporte ao usuário final

O suporte ao usuário final estabelece-se como uma das ações também importantes no gerenciamento e administração das redes de computadores. As ações nesse pilar tem como objetivo manter uma boa relação com o usuário, principalmente no momento em que ocorrem as falhas, as quedas no desempenho e os problemas.

Os principais problemas que o usuário encontra na utilização dos recursos tecnológicos de redes e telecomunicações são: falhas no hardware de rede, ausência de conhecimento do usuário e problemas com software de redes.

As ações eficazes de suporte ao usuário final decorrem de uma boa administração das falhas e do desempenho da rede no que tange aos problemas que normalmente ocorrem no dia a dia do uso das redes de computadores. Não obstante, os problemas de conhecimento por parte do usuário não são poucos e podem ser resolvidos com treinamentos aplicados pela área técnica.

8.1.6 Administração de custos

Como fruto da própria visão das áreas de negócios sobre o que é a área de TI, mais do que nunca tem sido importante a administração adequada dos custos com os recursos tecnológicos, principalmente o de redes, mesmo considerando que a TI representa muito mais investimento que custo.

Esses custos normalmente crescem com o aumento do tráfego nos circuitos de comunicação. A figura a seguir apresenta essa ideia.

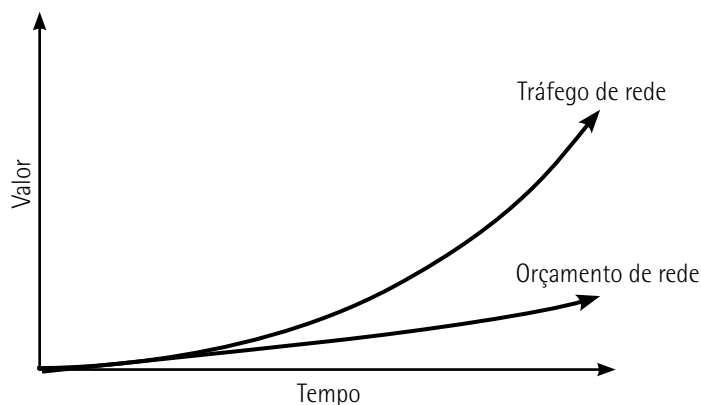


Figura 25 – Gráfico sobre o valor e o tempo



Lembrete

Nos recursos tecnológicos, é necessário contabilizar, além do custo com a aquisição (seja ele hardware, software, redes ou bancos de dados), o custo total de propriedade (conhecido pela sigla TCO, que se refere ao termo em inglês *total cost ownership*).

Vejamos o que dizem Fitzgerald e Dennis.

Diversos estudos realizados ao longo dos últimos anos pelo Gartner Group, Inc., uma empresa líder em pesquisa na indústria, sugere que o TCO de um computador é espantosamente alto. A maioria dos estudos sugere que o TCO para computadores Windows comuns em uma rede seja de aproximadamente US\$ 7.000 ao ano por computador. Em outras palavras, custa quase cinco vezes mais a cada ano para operar um computador do que comprá-lo pela primeira vez. Outros estudos, realizados por empresas como a IBM e a Information Week, uma revista da indústria, produziram estimativas de TCO entre US\$ 5.000 e 10.000 ao ano, sugerindo que as estimativas do Gartner Group são razoáveis. Embora o TCO tenha sido aceito por muitas organizações, outras empresas argumentam contra a prática de incluir o custo indireto no cálculo. Por exemplo, utilizando a técnica de incluir o custo indireto o TCO de uma máquina de café é mais de US\$ 50.000 ao ano – sem contar o custo do café

ou dos suprimentos. Isso se baseia na suposição de que pegar café "desperdiça" 12 minutos por dia vezes cinco dias por semana, o que leva a uma hora por semana, ou aproximadamente 50 horas por ano de tempo desperdiçado. Se você considerar que a cafeteria serve 20 empregados que têm um custo médio de US\$ 50 a hora (o que não é um número extraordinariamente alto), você tem uma perda de US\$ 50.000 ao ano (FITZGERALD; DENNIS, 2010, p. 384).

Uma adaptação interessante do termo TCO pode ser utilizada para as redes de computadores e telecomunicações, conhecida como custo de propriedade de rede (network cost of ownership, daí NCO). O NCO está diretamente ligado ao cálculo de custos de propriedades de recursos tecnológicos de rede. A tabela a seguir apresenta um detalhamento de NCO.

Tabela 1

Operações de rede		US\$ 14.871.000
Administração de contas	275.000	
Serviços de autenticação	257.000	
Infraestrutura de serviços de diretório (incluindo DHCP e DNS)	746.000	
E-mail e messaging	1.434.000	
Operações de mainframe e cluster	633.000	
Armazenamento de dados em massa	1.424.000	
Administração de políticas	75.000	
Impressão	201.000	
Administração de segurança	1.270.000	
Operações WAN	7.410.000	
Serviços da web	1.146.000	
Suporte ao usuário final		US\$ 6.544.000
Suporte de tecnologia departamental	553.000	
Suporte de tecnologia de instrução	856.000	
Suporte à residência dos estudantes	279.000	
Suporte aos centros de tecnologia dos estudantes	1.288.000	
Centro de suporte (central de atendimento)	2.741.000	
Treinamento e educação	827.000	
Hardware-cliente		US\$ 3.901.000
Equipamentos e suprimentos de tecnologia de sala de aula	844.000	
Equipamentos e suprimentos da residência dos estudantes	601.000	
Equipamentos e suprimentos dos centros de tecnologia dos estudantes	2.456.000	
Software de aplicação		US\$ 3.729.000
Licenças de software	2.540.000	
Software da residência dos estudantes	146.000	
Software dos centros de tecnologia dos estudantes	1.043.000	
Total		US\$ 29.045.000

Fonte: Fitzgerald e Dennis (2010, p. 385).

Uma das ações mais desejadas pelas áreas de negócio é a redução de custos, a fim de reduzir também os grandes valores de NCO. Essa redução pode ocorrer por meio de cinco passos, descritos a seguir.

- Desenvolvimento de um padrão de configurações para hardwares e softwares de redes.
- Implementações de robustas ferramentas de administração e gerenciamento de redes permitindo a máxima automatização da função de gestão de redes.
- Opção por fabricantes que ofereçam soluções de melhor custo, sempre preservando as expectativas de usuário quanto à qualidade dos serviços prestados pelas redes de computadores e telecomunicações.
- Centralização das centrais de suporte e de atendimento aos usuários.
- Mudanças e enxugamentos nas arquiteturas de rede utilizadas.

8.1.7 Administração da segurança

A administração da segurança da informação é fundamental para prover o controle de acesso às redes de computadores com base em políticas de segurança de informação bem definidas.

O gerenciamento de segurança é uma ação que abrange não somente os recursos de tecnologias de redes e telecomunicações, mas também todas as outras áreas do ambiente tecnológico, incluindo hardware, software e banco de dados.

8.2 Ferramentas de gerenciamento de redes

8.2.1 Principais ferramentas de gerenciamento de redes

As ferramentas de gerenciamento de redes são componentes fundamentais na administração desse tipo de recurso. É possível citar diversas ferramentas, como: teste de camada física, acesso e conectividade, análise de pacotes, descoberta de redes, consulta de dispositivo, monitoramento de eventos, monitoramento de desempenho, análise de fluxo, engenharia de tráfego e roteamento, configuração, aplicação das políticas de segurança e planejamento da rede.

De forma geral, é possível classificar as ferramentas de gerenciamento de redes em ativas e passivas. As ferramentas ativas geram interferência no sistema com o objetivo de alcançar as informações necessárias e as ferramentas passivas coletam dados já existentes. Os principais tipos de ferramentas de gerenciamento são listados a seguir.

- Coletores: colhem e guardam diferentes tipos de informação de rede.
- Sistemas de detecção de invasão (IDS): detectam padrões suspeitos que são característicos de comportamento malicioso na rede.

- Sistemas de análise de performance: permitem a análise de dados de tráfego e de performance.
- Sistemas de gerenciamento de alarme: coletam e monitoram os alarmes da rede.
- Sistemas de tickets: rastreiam como os problemas estão sendo resolvidos.
- Ferramentas de acesso: permitem o uso de máquinas remotas, possibilitando a troca de informação entre a ferramenta de gerenciamento e os dispositivos.
- Ferramentas de depuração: verificam e depuram informações sobre problemas nas redes.
- Ferramentas de log: auxiliam na gestão dos arquivos log criados no sistema.
- Ferramentas de performance: medem ativamente a máxima banda possível e a vazão (ou throughput) na rede IP.
- Ferramentas de gerenciamento de configuração: executam configurações de forma manual ou automática.
- Gerenciamento de endereços: gerenciam endereços de hosts em uma rede.

8.2.2 Protocolo simples de gerenciamento de redes

Um dos protocolos desenvolvidos que foi padronizado para o gerenciamento de redes foi o protocolo simples de gerenciamento de rede. Conhecido pelo seu acrônimo SNMP, que significa Simple Network Management Protocol, ele foi criado em 1987 com o nome de SGMP, que significa Simple Gateway Monitoring Protocol. Foi designado como protocolo de gerenciamento de rede na versão que foi definida no *Request for comments: 1157* (RFC 1157) de maio de 1990.

Após a primeira versão de 1990, foi criada a versão 2 e, atualmente, encontra-se na versão 3, conhecido como SNMPv3, utilizando o padrão conhecido como ASN.1 para codificação de mensagens. A figura a seguir apresenta um exemplo de codificação ASN.1.

Tabela 2

Inteiro decimal	Equivalente hexa	Comprimento do byte	Bytes do valor (em hexa)
27	1B	01	1B
792	318	02	03 18
24.567	5FF7	02	5F F7
190.345	2E789	03	02 E7 89

Fonte: Comer (2016, p. 474).

A arquitetura desse protocolo consiste em uma solução para o problema de gerenciamento de redes (em termos da representação da informação de gerenciamento comunicada pelo protocolo), da forma e do significado das trocas entre entidades de gerenciamento, da definição dos relacionamentos administrativos entre entidades de gerenciamento, do escopo da informação de gerenciamento comunicada pelo protocolo e da forma e do significado das referências às informações de gerenciamento.

O RFC 1157 inclui ainda três objetivos a serem conseguidos pelo SNMP: ser independente da arquitetura e do mecanismo dos dispositivos gerenciados, minimizar o número e a complexidade das funções de gerenciamento e ser flexível o suficiente para permitir expansões futuras.

O SNMP é uma estrutura de dispositivos em uma pilha de protocolos TCP/IP e utiliza o conceito de gerente e agente. O gerente, normalmente, é uma estação que controla um conjunto de agentes, que podem ser roteadores ou servidores.

O gerenciador central e os equipamentos de rede utilizam o protocolo SNMP para a comunicação das informações de gerenciamento de redes. Nos elementos que se busca gerenciar, é instalado um software cliente, também conhecido como agente. Esse elemento manda dados ao gerenciador central da rede, o qual guarda esses dados e exibe alertas quando ocorre falha de algum equipamento ou do meio de comunicação utilizado. A figura a seguir apresenta a ideia utilizada no protocolo SNMP.

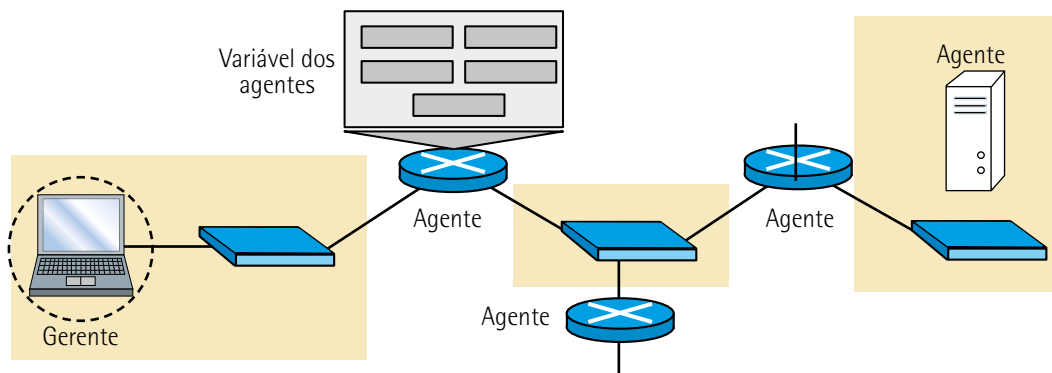


Figura 26 – Ideia do protocolo SNMP

O SNMP é um protocolo da camada de aplicação no qual poucas estações gerentes controlam um conjunto de agentes. O intuito de o protocolo ter sido desenvolvido nessa camada é possibilitar o monitoramento dos dispositivos produzidos por fornecedores variados e instalados em diferentes redes físicas. Assim, o protocolo SNMP permite que as atividades de gerenciamento ocorram independentemente das características físicas dos dispositivos ou da tecnologia da rede adotada.

Com o gerenciamento SNMP é possível implementar funções, como um gerente inspecionar um agente por meio de uma solicitação de informações que refletem no comportamento do agente. Outra função possível é um agente contribuir com o processo de gerenciamento por meio de alertas, avisando o gerente de uma situação incomum. Por fim, um gerente pode forçar um agente a executar uma tarefa por meio da reinicialização dos valores na base de dados desse agente.

O SNMP utiliza o protocolo User Datagram Protocol (UDP) para o envio de dados em uma rede TCP/IP na comunicação entre cliente e servidor. Para o cliente da rede, o SNMP executa as operações sobre os objetos de forma transparente, o que permite à interface do software de gerenciamento da rede criar comandos imperativos para executar operações sobre os objetos gerenciados. Essa é a grande diferença entre gerenciar uma rede usando o protocolo SNMP e gerenciar a mesma rede usando outros protocolos.



Resumo

Foram abordados os temas da governança corporativa e de TI, além do gerenciamento do recurso de redes. Foram vistos conceitos, princípios e definições de governança corporativa e governança de TI.

Destacou-se que o assunto governança corporativa, além carregar grande importância para as organizações, é premissa para o entendimento da governança de TI e, conseqüentemente, para a gestão das ferramentas tecnológicas utilizadas pelas empresas nos dias de hoje. Isso se dá porque os interesses de todas partes do negócio (acionistas, empregados, clientes e fornecedores, entre outros) influencia as estratégias organizacionais e determina grande parte das ações no dia a dia das empresas. É justamente nesse contexto que a governança corporativa é concebida.

Tratou-se ainda da ideia de estruturas de poder que governam as empresas, além dos principais modelos de governança no mundo (destacando especialmente o anglo-saxão, o alemão, o japonês, o latino-europeu e o latino-americano). Foram apresentados os marcos da governança corporativa, além do seu uso no Brasil e os seus desdobramentos para a área de TI das empresas.

Foram trazidos diversos conceitos de governança de TI. Explicou-se que a governança de TI é de responsabilidade da alta direção e dos executivos, além de precisar de sua total adesão no processo de implementação. Isso se dá porque ter governança é, necessariamente, ter direção e controle a fim de controlar o uso futuro e atual da TI.

Por fim, apresentou-se o modelo Cobit, o mais utilizado no mundo em matéria de governança de TI. O modelo foi criado em 1994 para a Information Systems Audit and Control Association (Isaca). A ideia inicial, já reformulada nos dias de hoje, foi desenvolver um conjunto de práticas e controles para a área de TI, tendo em vista uma maior aderência às necessidades de negócio. Posteriormente, tratou-se do gerenciamento das redes de computadores.



Exercícios

Questão 1. (FCC 2016) Para gerenciar os serviços de Tecnologia da Informação (TI) um analista do TRF3 deve adotar um modelo baseado nas melhores práticas de gerenciamento de serviços utilizadas com sucesso nas organizações. Já para a governança e gestão de TI deverá adotar um framework que traz boas práticas para a governança e gestão da TI. A escolha do analista deverá ser, respectivamente,

- A) Itil – Cobit.
- B) CMMI – MPS.BR.
- C) BSC – Prince2.
- D) Itil – CMMI.
- E) Spice – Cobit.

Resposta correta: alternativa A.

Análise das alternativas

A) Alternativa correta.

Justificativa: Itil é um esforço que reúne melhores práticas de gerenciamento de serviços de Tecnologia da Informação, com o intuito de melhoria na entrega e suporte aos serviços de TI. Cobit fornece um framework abrangente que auxilia as empresas a alcançar seus objetivos para a governança e o gerenciamento da TI em suas organizações. Em palavras simples, auxilia as empresas a criar valor a partir da TI por meio da ponderação entre os benefícios alcançáveis, riscos assumidos e recursos utilizados.

B) Alternativa incorreta.

Justificativa: o CMMI (Capability Maturity Model Integration ou Modelo Integrado de Maturidade em Capacitação) é um modelo de referência que contém práticas (genéricas ou específicas) necessárias à maturidade em disciplinas específicas. O MPS-BR, ou Melhoria de Processos do Software Brasileiro, é um modelo de qualidade de processo criado em 2003 pela Softex.

C) Alternativa incorreta.

Justificativa: BSC tem o objetivo de melhorar os métodos de medição de desempenho empresarial. A metodologia foi escolhida pela renomada revista Harvard Business Review como uma das práticas de gestão mais importantes e revolucionárias. Prince2® (Projects In Controlled Environments) é um padrão

desenvolvido e utilizado pelo Governo do Reino Unido, sendo amplamente reconhecido e utilizado no setor privado, tanto no Reino Unido quanto em outros países. Ele estabelece e comprovada as melhores práticas em gerenciamento de projetos.

D) Alternativa incorreta.

Justificativa: Itil é um esforço que reúne melhores práticas de gerenciamento de serviços de Tecnologia da Informação, com o intuito de melhoria na entrega e no suporte aos serviços de TI, mas o CMMI (Capability Maturity Model Integration ou Modelo Integrado de Maturidade em Capacitação) é um modelo de referência que não contém práticas (genéricas ou específicas) necessárias à maturidade em disciplinas específicas.

E) Alternativa incorreta.

Justificativa: a adoção do Cobit é correta, conforme explicado anteriormente, mas a da Spice não é correta.

Questão 2. A respeito do protocolo de gerenciamento de rede SNMP, analise as afirmativas a seguir.

I – É um protocolo da camada de Enlace.

II – É utilizado para trocar informações de gerenciamento entre os dispositivos da rede.

III – Consiste em nó gerenciado SNMP, agente SNMP e estação de gerenciamento de rede SNMP.

Está(ão) correta(s) apenas:

A) I.

B) II.

C) III.

D) I e II.

E) II e III.

Resolução desta questão na plataforma.

FIGURAS E ILUSTRAÇÕES

Figura 1

Adaptado de: LAURINDO, F. J. B. *Tecnologia da Informação: planejamento e gestão de estratégias*. São Paulo: Atlas, 2008. p. 35.

Figura 2

WEILL, P.; ROSS, J. W. *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores*. São Paulo: M. Books, 2006. p. 38.

Figura 3

REZENDE, D. A.; ABREU, A. F. de. *Tecnologia da Informação aplicada a sistemas de informação empresariais*. São Paulo: Atlas, 2013. p. 58.

Figura 4

Adaptado de: STALLINGS, W. *Organização e arquitetura de computadores*. São Paulo: Pearson Prentice Hall, 2010. p. 51.

Figura 5

Adaptado de: LAUDON, K. C.; LAUDON, J. P. *Sistemas de informação gerenciais*. 10. ed. São Paulo: Pearson, 2013. p. 117.

Figura 6

Adaptado de: MAGALHÃES, I. L.; PINHEIRO, W. B. *Gerenciamento de serviços de TI na prática*. São Paulo: Novatec, 2007. p. 46.

Figura 7

Adaptado de: FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012. p. 55.

Figura 8

MOLINARO, L. F. R.; RAMOS, K. H. C. *Gestão de Tecnologia da Informação*. Rio de Janeiro: LTC, 2011. p. 129.

Figura 9

Adaptado de: IT GOVERNANCE INSTITUTE. *Enterprisevalue: governance of it investments*. Rolling Meadows, 2008. p. 15.

Figura 11

Adaptado de: FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012. p. 25.

Figura 12

Adaptado de: FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012. p. 28.

Figura 13

Adaptado de: FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012. p. 26.

Figura 14

Adaptado de: FOINA, P. R. *Tecnologia da Informação: planejamento e gestão*. São Paulo: Atlas, 2009. p. 39.

Figura 15

Adaptado de: FREITAS, M. A. S. *Fundamentos do gerenciamento de serviços de TI*. 2. ed. Rio de Janeiro: Brasport, 2013. p. 184.

Figura 17

Adaptado de: FREITAS, M. A. S. *Fundamentos do gerenciamento de serviços de TI*. 2. ed. Rio de Janeiro: Brasport, 2013. p. 194.

Figura 18

FREITAS, M. A. S. *Fundamentos do gerenciamento de serviços de TI*. 2. ed. Rio de Janeiro: Brasport, 2013. p. 254.

Figura 19

Adaptado de: ROSSETTI, J. C.; ANDRADE, A. *Governança corporativa: fundamentos, desenvolvimento e tendências*. São Paulo: Atlas, 2012. p. 256.

Figura 20

FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012. p. 1.

Figura 21

IT GOVERNANCE INSTITUTE. *Cobit 4.1*. Rolling Meadows, 2007. p. 12.

Figura 22

IT GOVERNANCE INSTITUTE. *Cobit 4.1*. Rolling Meadows, 2007. p. 27.

Figura 23

FITZGERALD, J.; DENNIS, A. *Comunicação de dados empresariais e redes*. 10. ed. Rio de Janeiro: LTC, 2010. p. 374.

Figura 24

FITZGERALD, J.; DENNIS, A. *Comunicação de dados empresariais e redes*. 10. ed. Rio de Janeiro: LTC, 2010. p. 381.

Figura 25

FITZGERALD, J.; DENNIS, A. *Comunicação de dados empresariais e redes*. 10. ed. Rio de Janeiro: LTC, 2010. p. 383.

Figura 26

FOROUZAN, B. A.; MOSHARRAF, F. *Redes de computadores: uma abordagem top-down*. Porto Alegre: AMGH, 2013. p. 723.

REFERÊNCIAS

Textuais

AKABANE, G. K. *Gestão estratégica da Tecnologia da Informação: conceitos, metodologias, planejamento e avaliações*. São Paulo: Atlas, 2012.

ALBERTIN, A. L. Valor estratégico dos projetos de Tecnologia de Informação. *RAE: Revista de Administração de Empresas*, São Paulo, v. 41, n. 3, p. 42-50, 2001.

_____.; ALBERTIN, R. M. M. Dimensões do uso de tecnologia da informação: um instrumento de diagnóstico e análise. *RAP: Revista de Administração Pública*, São Paulo, v. 46, n. 1, p. 125-151, 2012.

ANSOFF, H. I. *A nova estratégia empresarial*. São Paulo: Atlas, 1991.

_____. *Estratégia empresarial*. McGraw-Hill: São Paulo, 1977.

_____.; McDONNELL, E. *Implantando a administração estratégica*. São Paulo: Atlas, 1993.

ARAÚJO, M. *A evolução dos departamentos de TI*. Disponível em: <<http://student.dei.uc.pt/~maraujo/csi/artigo2.htm>>. Acesso em: 7 jun. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 38500: Governança Corporativa de Tecnologia da Informação*. Rio de Janeiro, 2008.

BANZATO, E. *Tecnologia da Informação aplicada a logística*. São Paulo: Iman, 2005.

BATAGLIA, W.; YU, A. S. O. A sincronização da tomada de decisão estratégica com o planejamento estratégico formal. *Revista de Administração Mackenzie*, São Paulo, v. 9, n. 5, p. 82-111, 2008.

BATEMAN, T.; SNELL, S. *Administração: construindo vantagem competitiva*. São Paulo: Atlas, 1998.

BEAL, A. *Gestão estratégica da informação: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações*. São Paulo: Atlas, 2004.

BERNAL, P. S. M. *Voz sobre o protocolo IP: a nova realidade da telefonia*. São Paulo: Érica, 2007.

BORGES, M. E. N. A informação como recurso gerencial das organizações na sociedade de conhecimento. *Ciência da Informação*, Brasília, v. 24, n. 2, p. 31-45, 1995.

BORN, R. A. et al. *Construindo o plano estratégico*. Porto Alegre: Sulina, 2007.

BRITO, M. A. L. *Análise de desempenho do Sistema de Informação nos processos administrativos da UFPI*. 2011. Monografia (Bacharelado em Administração) – Universidade Federal do Piauí, Picos.

BRITO, M. J. *Tecnologia da informação e mercado futuro: o caso da BM&F, tecnologia da informação e estratégia empresarial*. São Paulo: FEA/USP, 1996.

BROCKA, B.; BROCKA, M. S. *Gerenciamento da qualidade*. São Paulo: Makron Books, 1995.

BURGESS, M. *Princípios de administração de redes e sistemas*. 2. ed. Rio de Janeiro: LTC, 2006.

CASE, J. et al. *Request for comments: 1157*. 1990. Disponível em: <<https://www.ietf.org/rfc/rfc1157.txt>>. Acesso em: 25 jul. 2018.

CICCARELLI, P. et al. *Princípios de redes*. Rio de Janeiro: LTC, 2009.

COMER, D. E. *Redes de computadores e internet*. São Paulo: Bookman, 2016.

COSTA, I. et al. *Qualidade em Tecnologia da Informação: conceitos de qualidade nos processos, produtos, normas, modelos e testes de software no apoio às estratégias empresariais*. São Paulo: Atlas, 2012.

COSTA NETO, P. L. O.; CANUTO, S. A. *Administração com qualidade*. São Paulo: Blucher, 2010.

- ELEUTÉRIO, M. A. N. *Sistemas de informações gerenciais na atualidade*. Curitiba: Intersaberes, 2015.
- ERL, T. *SOA: princípios de design de serviços*. São Paulo: Pearson Prentice Hall, 2008.
- FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*. Rio de Janeiro: Brasport, 2012.
- FILIPPETTI, M. A. *CCNA 6.0: guia de estudo*. Florianópolis: Visual Books, 2017.
- FISCHMANN, A. A.; ALMEIDA, M. I. R. *Planejamento estratégico na prática*. São Paulo: Atlas, 2009.
- FITZGERALD, J.; DENNIS, A. *Comunicação de dados empresariais e redes*. 10. ed. Rio de Janeiro: LTC, 2010.
- FOINA, P. R. *Tecnologia da Informação: planejamento e gestão*. São Paulo: Atlas, 2009.
- FOROUZAN, B. A.; MOSHARRAF, F. *Redes de computadores: uma abordagem top-down*. Porto Alegre: AMGH, 2013.
- FREITAS, M. A. S. *Fundamentos do gerenciamento de serviços de TI*. 2. ed. Rio de Janeiro: Brasport, 2013.
- FRYE, C. *Microsoft Excel 2016: passo a passo*. Porto Alegre: Bookman, 2016.
- GAMA, F. A.; MARTINELLE, M. Análise do impacto do nível da Governança de Tecnologia da Informação em indicadores de performance de TI: estudo de caso no setor siderúrgico, 30º Encontro da Enanpad, 23 a 27 de setembro de 2006.
- GIL, A. de L. *Qualidade total em informática*. São Paulo: Atlas, 1999.
- ____; BIANCOLINO, C. A.; BORGES, T. N. *Sistemas de informações contábeis: uma abordagem gerencial*. São Paulo: Saraiva, 2010.
- GONÇALVES, R. C. M. G.; RICCIO, E. L. *Sistemas de informação: ênfase em controladoria e contabilidade*. São Paulo: Atlas, 2009.
- GORDON, S. R.; GORDON, J. R. *Sistemas de informação: uma abordagem gerencial*. 3. ed. Rio de Janeiro: LTC, 2006.
- HENDERSON, J. C.; VENKATRAMAN, N. Strategic alignment: leveraging information technology for transforming organizations. *IBM System Journal*, Riverton, v. 32, n. 1, p. 4-16, 1993.
- HURT, R. L. *Sistemas de informações contábeis: conceitos básicos e temas atuais*. 3. ed. Porto Alegre: AMGH, 2014.
- INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). *Sustentabilidade*. Rolling Meadows, 2011.

IT GOVERNANCE INSTITUTE. *Cobit 4.1*. Rolling Meadows, 2007.

____. *Enterprisevalue: governance of it investments*. Rolling Meadows, 2008.

KAPLAN, R. S.; NORTON, D. P. *A estratégia em ação: BSC, Balanced Scorecard*. Rio de Janeiro: Campus, 1997.

____. *Organização orientada para a estratégia: como as empresas que adotaram o Balanced Scorecard prosperam no novo ambiente de negócios*. Rio de Janeiro: Campus, 2001.

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*. 3. ed. São Paulo: Pearson, 2006.

LAUDON, K. C.; LAUDON, J. P. *Sistemas de informação gerenciais*. 10. ed. São Paulo: Pearson, 2013.

LAURINDO, F. J. B. *Tecnologia da Informação: planejamento e gestão de estratégias*. São Paulo: Atlas, 2008.

LUFTMAN, J. *Competing in the information age: strategic alignment in practice*. New York: Oxford University Press, 1996.

LUNARDI, G. L.; BECKER, J. L.; MACADA, A. C. G. Um estudo empírico do impacto da governança de TI no desempenho organizacional. *Produção*, São Paulo, v. 22, n. 3, p. 612-624, ago. 2012. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-65132012000300019&lng=en&nrm=iso>. Acesso em: 24 jul. 2018.

MAGALHÃES, I. L.; PINHEIRO, W. B. *Gerenciamento de serviços de TI na prática*. São Paulo: Novatec, 2007.

MANSUR, R. *Governança de TI verde: o ouro verde da nova TI*. Rio de Janeiro: Ciência Moderna, 2011.

MARÇULA, M.; BENINI FILHO, P. A. *Informática: conceitos e aplicações*. São Paulo: Erica, 2013.

MARQUES, F. T. *Projeto de Infraestrutura de TI pela perspectiva de negócio*. 2006. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Campina Grande, Paraíba.

MEDEIROS, J. C. O. *Princípios de telecomunicações: teoria e prática*. São Paulo: Erica, 2012.

MOLINARO, L. F. R.; RAMOS, K. H. C. *Gestão de Tecnologia da Informação*. Rio de Janeiro: LTC, 2011.

MORAES, A. J. M.; COSTA, I. Proposta de alinhamento das atividades de TI na produção de aplicações com as determinações geradas pelo planejamento estratégico da organização. In: XXIX ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO, 2009, Salvador, *Anais...*, Salvador, Abepro, 2009, p. 1-14.

O'BRIEN, J.; JAMES, A. *Sistemas de informação e as decisões gerenciais na era da internet*. São Paulo: Saraiva, 2002.

OLIVEIRA, D. P. R. *Planejamento estratégico: conceito, metodologia e práticas*. São Paulo: Atlas, 2001.

- ____. *Administração de processos: conceitos, metodologia, práticas*. 3. ed. São Paulo: Atlas, 2009.
- PADOVEZE, C. L. *Sistemas de informações contábeis: fundamentos e análise*. 7. ed. São Paulo: Atlas, 2015.
- PEREZ, C. C. S.; ANDRADE, D. F. *Excel 2016: conceito e prática*. Santa Cruz do Rio Pardo: Viena, 2016.
- POLIZEL, C.; STEINBERG, H. *Governança corporativa na educação superior: casos práticos de instituições privadas (com e sem fins lucrativos)*. São Paulo: Saraiva, 2013.
- PORTER, M. E. *Vantagem competitiva: criando e sustentando um desempenho superior*. Rio de Janeiro: Campus, 1989.
- ____; MILLAR, V. E. How information gives you competitive advantage. *Harvard Business Review*, Boston, v. 63, n. 4, jul./ago., p. 149-160, 1987.
- REINHARD, N. Evolução das ênfases gerenciais e de pesquisa na área de tecnologia de informática e de telecomunicações aplicada nas empresas. *RAUSP- Revista de Administração*, São Paulo, v. 31, n. 4, p. 5-6, 1996.
- REZENDE, D. A. *Evolução da Tecnologia da Informação nos últimos 45 anos*. Disponível em: <https://www.joinville.udesc.br/portal/professores/pfitscher/materiais/Evolu_o_da_TI.pdf>. Acesso em: 2008.
- ____; ABREU, A. F. de. *Tecnologia da Informação aplicada a sistemas de informação empresariais*. São Paulo: Atlas, 2013.
- RIBEIRO NETO, L. G. Os impactos da tecnologia de informação nas organizações: uma visão política. *Revista da Universidade de Alfenas*, Alfenas, v. 5, n. 3, p. 95-101, 1999.
- RODRIGUEZ, G. M.; BRANDÃO, M. M. *Visões da governança corporativa: a realidade das sociedades por ações e a sustentabilidade*. São Paulo: Saraiva, 2010.
- ROSSETTI, J. C.; ANDRADE, A. *Governança corporativa: fundamentos, desenvolvimento e tendências*. São Paulo: Atlas, 2012.
- STAIR, R. M.; REYNOLDS, G. W. *Princípios de sistemas de informação*. 9. ed. São Paulo: Cengage Learning, 2011.
- STALLINGS, W. *Arquitetura e organização de computadores*. São Paulo: Pearson, 2009.
- ____. *Organização e arquitetura de computadores*. São Paulo: Pearson Prentice Hall, 2010.
- ____. *Redes e sistemas de comunicação de dados*. Rio de Janeiro: Elsevier, 2005.
- SUPPI, G. M. et al. Uma visão geral sobre a internet das coisas. *Univap*, São José dos Campos, v. 22, n. 40, p. 586-599, 2016.

- TANENBAUM, A. S. *Organização estruturada de computadores*. São Paulo: Pearson, 2013.
- _____; WETHERALL, D. J. *Redes de computadores*. 5. ed. Rio de Janeiro: Pearson Prentice Hall, 2011.
- TAVARES, M. C. *Gestão estratégica*. São Paulo: Atlas, 2008.
- TIGRE, P. B. *Gestão da inovação: a economia da tecnologia do Brasil*. Rio de Janeiro: Elsevier, 2006.
- TORRES, G. *Redes de computadores: versão revisada e atualizada*. 2. ed. Rio de Janeiro: Novaterra, 2016.
- TZU, S. *A arte da guerra*. São Paulo: Geração Editorial, 2012.
- VAL IT framework for business technology management. *Isaca*, [s.d.]. Disponível em: <<http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx>>. Acesso em: 16 ago. 2018.
- VELOSO, R. *Tecnologias da informação e da comunicação: desafios e perspectivas*. São Paulo: Saraiva, 2011.
- WEILL, P; ROSS, J. W. *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores*. São Paulo: M. Books, 2006.

Sites

- <<http://www.computerhistory.org>>
- <www.top500.org>
- <<http://www.teleco.com.br/tutoriais.asp>>
- <www.telebrasil.org.br>
- <www.teleco.com.br>
- <<http://www.itsmf.com.br/portal/>>
- <www.itsmf.org>
- <<http://www.itil.org.uk/>>
- <<http://www.ibgc.org.br>>

Exercícios

Unidade I – Questão 1: TRIBUNAL REGIONAL DO TRABALHO 1ª REGIÃO. *Concurso Público para provimento de cargos de analista judiciário: área administrativa*. Questão 36. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/29472/fcc-2013-trt-1-regiao-rj-analista-judiciario-area-administrativa-prova.pdf>. Acesso em: 27 jul. 2018.

Unidade I – Questão 2: CÂMARA MUNICIPAL DE SÃO JOSÉ DOS CAMPOS. *Concurso público 2009: analista de sistemas*. Questão 34. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/976/fip-2009-camara-municipal-de-sao-jose-dos-campos-sp-analista-de-sistemas-prova.pdf>. Acesso em: 27 jul. 2018.

Unidade II – Questão 1: MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE. *Concurso público para provimento de cargos de analista do Ministério Público: área Informática I*. Questão 58. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/32802/fcc-2013-mpe-se-analista-informatica-gestao-e-analise-de-projeto-de-sistema-prova.pdf>. Acesso em: 27 jul. 2018.

Unidade II – Questão 2: TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO. *Concurso público para provimento de cargos de analista judiciário: área apoio especializado*. Questão 45. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/57057/fcc-2018-trt-6-regiao-pe-analista-judiciario-tecnologia-da-informacao-prova.pdf>. Acesso em: 27 jul. 2018.

Unidade III – Questão 1: TRIBUNAL DE CONTAS DO ESTADO DO PARÁ. *Assessor técnico de informática: analista de sistemas*. Questão 35. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/28820/aocp-2012-tce-pa-assessor-tecnico-de-informatica-analista-de-sistemas-prova.pdf>. Acesso em: 27 jul. 2018.

Unidade III – Questão 2: MINISTÉRIO PÚBLICO DO ESTADO DO MARANHÃO. *Concurso público para provimento de cargos de técnico ministerial: tecnologia da informação*. Questão 53. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/31886/fcc-2013-mpe-ma-tecnico-ministerial-tecnologia-da-informacao-prova.pdf>. Acesso em: 27 jul. 2018.

Unidade IV – Questão 1: TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO. *Concurso público para provimento de cargo de analista judiciário: área administrativa*. Questão 99. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/47748/fcc-2016-trf-3-regiao-analista-judiciario-area-administrativa-prova.pdf>. Acesso em: 27 jul. 2018.



A series of horizontal lines for writing, consisting of 30 evenly spaced lines across the page.



Handwriting practice lines consisting of 30 horizontal blue lines. Each line is preceded by a small blue dot, serving as a starting point for letter formation. The lines are evenly spaced and extend across the width of the page.



Handwriting practice lines consisting of 30 horizontal blue lines. Each line is preceded by a small blue dot, serving as a starting point for letter formation. The lines are evenly spaced and extend across the width of the page.



Interativa

Informações:
www.sepi.unip.br ou 0800 010 9000