Levantamento de Governança de TI 2012 - Glossário

Acordo de Nível de Serviço (ANS) ou “Service Level Agreement” (SLA)

Define um acordo que, para fins desse levantamento, deve ser necessariamente documentado, entre um prestador de serviço interno (no caso, a área de TI) e o cliente/usuário interno, no qual se define o “nível” de prestação do serviço necessário para sustentar adequadamente as operações do negócio. O acordo pode especificar níveis para quaisquer atributos do serviço. São comuns critérios relacionados à operação e suporte, tais como: disponibilidade, manutenibilidade, “performance”, incidência de erros, prioridades, etc. Um acordo de nível de serviço típico geralmente contém: a definição dos serviços, objetivos, indicadores e métricas, responsabilidades de ambas as partes (inclusive penalidades), garantias, medidas emergenciais, planos alternativos, definições sobre relatórios de monitoramento, dentre outras informações. [1]

Alta Administração

Equivale ao conceito de “dirigente” do setor privado. No setor público, compõem a “Alta Administração” os principais dirigentes da organização. Como exemplos mais conhecidos, temos Ministros e Secretários de Estado, titulares de cargos de natureza especial, secretários-executivos, secretários ou autoridades equivalentes ocupantes de cargo do Grupo-Direção e Assessoramento Superiores - DAS, nível seis, presidentes de tribunais, presidentes e diretores de agências nacionais, autarquias, fundações mantidas pelo Poder Público, presidentes de empresas públicas e sociedades de economia mista, bem como a diretoria executiva. [2]

Confidencialidade

Propriedade de que a informação não esteja disponível nem seja revelada a pessoas, entidades ou processos não autorizados, conforme definido pelo seu proprietário. [3]

Disponibilidade

Propriedade de que a informação esteja acessível e pronta para ser utilizada por pessoas, processos ou entidades autorizadas, sempre que necessário, conforme definido pelo seu proprietário. [4]

Governança corporativa

É o sistema pelo qual as organizações são dirigidas e controladas. Pode ser entendido como o conjunto de ações e responsabilidades exercidas pela alta administração da empresa, órgão ou entidade, com o objetivo de oferecer orientação estratégica e garantir que os objetivos sejam alcançados, com simultânea gerência de riscos e verificação de que os recursos são utilizados de forma responsável. [5]

Governança de TI ou Governança corporativa de TI

É o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização. A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore as estratégias e objetivos da organização. [6]

Incidente de segurança da informação

Um evento ou uma série de eventos indesejados ou inesperados e que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [7]

Indicador de desempenho

Métrica para medir e monitorar o desempenho havido e compará-lo com o desempenho desejado. Define como será medido e acompanhado o sucesso do alcance de um objetivo. Normalmente é utilizado para avaliar o desempenho de processos, atividades ou serviços relacionados a objetivos estabelecidos. Ressalte-se que o termo “desempenho” aqui utilizado não se limita apenas a “velocidade” ou “produtividade”, tendo alcance bastante amplo, podendo incluir metas de qualidade ou o alcance de objetivos de negócio, além de outras possibilidades. Alguns exemplos de indicadores: satisfação dos usuários com o atendimento do serviço de suporte remoto; quantidade de estações de trabalho com proteção antivírus atualizada; quantidade de casos de uso do sistema “XYZ” implementados; disponibilidade do acesso à Internet em horário normal de expediente; disponibilidade da infraestrutura de aplicações e do portal corporativo, em horário normal de

expediente. Há também indicadores de desempenho que ligam diretamente uma solução de TI à razão negocial para sua existência, tais como: número de usuários atendidos; número de transações eletrônicas corretamente finalizadas dentro do tempo de resposta esperado; retorno sobre o investimento da solução de TI. [8]

Indicadores de benefício

Métrica para medir quantitativamente o resultado de determinado processo em termos dos objetivos de negócio da organização. Relaciona-se diretamente com a dimensão EFETIVIDADE e é usado na avaliação da ECONOMICIDADE.

Integridade

Propriedade de que a informação esteja exata e completa para os propósitos definidos pelo seu proprietário. A informação pode não ser íntegra desde sua origem, ou pode haver perda da integridade durante o uso, ou ainda pela comunicação (de maneira fortuita ou intencional).[9]

Nível de maturidade/capacidade

Medida da capacidade de um processo (ou de um macroprocesso) para atingir seu propósito, de acordo com uma escala definida em um “modelo de maturidade”. Um modelo normalmente define os processos e os atributos que serão medidos, bem como a escala de maturidade. Como exemplos de modelos de maturidade, podem ser citados: CMM, CMMI, MPS.BR, NBR ISO/IEC 15504, Cobit Generic Maturity Model e ITIL Process Maturity Framework. Os Modelos de maturidade podem ser voltados a um domínio específico de atuação, como a engenharia de software (caso do CMM) ou suportar diferentes domínios (caso do CMMI). No caso dos modelos CMM, CMMI E MPS.BR, quando a avaliação destina-se a medir a capacidade de uma organização (ou de um departamento ou de um projeto) em executar um macroprocesso, a medida resultante denomina-se “Nível de Maturidade”. Já quando se utilizam tais modelos para avaliar a eficácia de um processo particular que compõe um macroprocesso, o resultado denomina-se “Nível de Capacidade” do processo. Diferentemente, o modelo de maturidade genérico previsto no COBIT nomeia a avaliação de um processo particular como “Nível de Maturidade” do processo. Para o “Process Maturity Framework”, da biblioteca ITIL, tanto o macroprocesso de gestão de serviços de TI quanto os processos particulares podem ser avaliados por um “Nível de Maturidade”. [10]

Planejamento estratégico institucional

Processo que trata da formulação de objetivos de longo prazo e seleção de programas de ação e para sua execução, levando em conta as condições internas e externas à organização e sua evolução esperada. Observe-se que **não** se trata do documento elaborado ao fim do processo, o qual pode ser chamado, por exemplo, de plano estratégico institucional (PEI). O PEI é um exemplo de **produto** resultante do processo de Planejamento Estratégico. [11]

Planejamento Estratégico de TI

É a parte do processo de planejamento estratégico institucional que enfoca como a gestão e o uso da tecnologia de informação podem gerar valor para a organização. Observe-se que **não** se trata do documento elaborado ao fim do processo, o qual pode ser chamado, por exemplo, de plano diretor de tecnologia da informaçao institucional (PDTI). O PDTI é um exemplo de **produto** resultante do processo de Planejamento Estratégico de TI. [12]

Política

Instruções claras e mensuráveis de direção e comportamento desejado que condicionem as decisões tomadas dentro de uma organização. [13]

Política corporativa de segurança da informação

É um documento que declara o comprometimento da alta administração e seu apoio aos princípios e metas da segurança da informação. Estabelece o enfoque da organização e as diretrizes para gerenciar a segurança da informação. Esse documento deve conter declarações relativas a uma definição de segurança da informação, suas metas globais, princípios, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação. [14]

Portfólio de Serviços

É o conjunto de programas, projetos, serviços e ativos de TI selecionados para serem gerenciados e monitorados com vistas a apoiar ou viabilizar a geração dos resultados e a alcançar os objetivos estratégicos da organização. [15]

Processo de Software

Processo de trabalho usado por uma organização na produção/aquisição de software e na gestão de seu ciclo de vida. Inclui atividades realizadas nas fases de definição, desenvolvimento, operação e retirada do software.

TI (Tecnologia da Informação)

Engloba todos os recursos necessários para adquirir, processar, armazenar e disseminar informações. Inclui “Tecnologia da Comunicação (TC)” e é sinônimo de “Tecnologia da Informação e Comunicação (TIC)”. [16]

Referências:

1

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.197. SLA – Acordo de nível de serviços (Service level agreement) – Um acordo preferencialmente documentado entre o provedor do serviço e o cliente/usuário que define as metas mínimas de performance de um serviço e como elas serão mensuradas.

2

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.**
p.3. Dirigente - Membro da mais alta direção de uma organização. Incluem proprietários, membros de conselho de administração, parceiros, executivos seniores ou similares e funcionários autorizados pela legislação ou regulamentação.

BRASIL. Código de Conduta da Alta Administração Federal.
Art. 2o As normas deste Código aplicam-se às seguintes autoridades públicas: I - Ministros e Secretários de Estado; II - titulares de cargos de natureza especial, secretários-executivos, secretários ou autoridades equivalentes ocupantes de cargo do Grupo-Direção e Assessoramento Superiores - DAS, nível seis; III - presidentes e diretores de agências nacionais, autarquias, inclusive as especiais, fundações mantidas pelo Poder Público, empresas públicas e sociedades de economia mista.

3

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**
p.2 e 3. Confidencialidade - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

4

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**
p.2 e 3. Disponibilidade - propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada

5

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.**
p.3. Governança corporativa - O sistema pelo qual as organizações são dirigidas e controladas. (adaptado do Cadbury 1992 e OECD 1999).

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.195. Governança corporativa (Enterprise governance) – Conjunto de responsabilidades e práticas exercidas pela Alta Direção e Executivos com o objetivo de prover direção estratégica, assegurando que os objetivos sejam atingidos, assegurando que os riscos sejam gerenciados apropriadamente e verificando se os recursos da organização são utilizados com responsabilidade.

6

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação**.

p.3. Governança corporativa de TI- O sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Governança corporativa de TI significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**

p.7. A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização.

7

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**

p.2. incidente de segurança da informação - um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação
[ISO/IEC TR 18044:2004]

8

WIKIPEDIA. **Performance Indicator.**

A performance indicator or key performance indicator (KPI) is a measure of performance. Such measures are commonly used to help an organization define and evaluate how successful it is, typically in terms of making progress towards its long-term organizational goals... The KPIs differ depending on the nature of the organization and the organization's strategy. They help to evaluate the progress of an organization towards its vision and long-term goals (...)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**

p.195. KPI – Indicador-chave de performance (Key performance indicator) – Mensurações que determinam o andamento de um processo para permitir que um objetivo seja atingido. Eles são indicativos de tendências futuras quanto a se um objetivo será provavelmente atingido; são bons indicadores de capacidades, práticas e especialização. Medem os objetivos de atividades que são as medidas que os proprietários de processos precisam tomar para um efetivo desempenho do processo.

9

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**

p.3. integridade - propriedade de salvaguarda da exatidão e completeza de ativos.

10

WIKIPEDIA.**CMM - Capability Maturity Model.**
The Capability Maturity Model (CMM) was originally developed as a tool for objectively assessing the ability of government contractors' processes to perform a contracted software project. (…) There are five levels defined along the continuum of the CMM (…) 1. Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new process. 2. Managed - the process is managed according to the metrics described in the Defined stage. 3. Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the latter being Work Instructions). 4. Quantitatively managed. 5. Optimized - process management includes deliberate process optimization/improvement.

BRASIL. Softex. MPS.BR - **Melhoria de Processo do Software Brasileiro - Guia Geral**. 2009.
p.6. O modelo MPS baseia-se nos conceitos de maturidade e capacidade de processo para a avaliação e melhoria da qualidade e produtividade de produtos de software e serviços correlatos.
p.16. Os níveis de maturidade estabelecem patamares de evolução de processos, caracterizando estágios de melhoria da implementação de processos na organização. O nível de maturidade em que se encontra uma organização permite prever o seu desempenho futuro ao executar um ou mais processos. O MR-MPS define sete níveis de maturidade: A (Em Otimização), B (Gerenciado Quantitativamente), C (Definido), D (Largamente Definido), E (Parcialmente Definido), F (Gerenciado) e G (Parcialmente Gerenciado). A escala de maturidade se inicia no nível G e progride até o nível A.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.19. No CobiT, uma definição genérica é provida para as escalas de maturidade do CobiT as quais são similares às do CMM mas interpretadas de acordo com a natureza dos processos de gerenciamento de TI do CobiT. Um modelo específico é fornecido derivando dessa escala genérica para cada um dos 34 processos CobiT.
p.21. Modelo de Maturidade Genérico- 0 Inexistente – Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada. 1 Inicial / Ad hoc – Existem evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem enfoques Ad Hoc que tendem a ser aplicados individualmente ou caso-a-caso. O enfoque geral de gerenciamento é desorganizado. 2 Repetível, porém Intuitivo – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixado com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e conseqüentemente erros podem ocorrer. 3 Processo Definido – Procedimentos foram padronizados, documentados e comunicados através de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados mas existe a formalização das práticas existentes. 4 Gerenciado e Mensurável – A gerencia monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão debaixo de um constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada. 5 Otimizado – Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida em adaptar-se.

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 15504-2:2008 - Tecnologia da Informação - Avaliação de Processo - Parte 2: Realização de uma Avaliação**
p.6 a 9. Uma Estrutura de Medição para a Capacidade de processo - Esta seção da ABNT NBR ISO/IEC 15504-2 define uma estrutura de medição para a avaliação da capacidade de processo. A capacidade de processo é definida em uma escala ordinal de seis pontos (...) Nível 0: Processo incompleto - O processo não está implementado ou não atinge o seu propósito. Nível 1: Processo executado - O processo implementado atinge o seu propósito. Nível 2: Processo gerenciado - O processo executado, descrito anteriormente, agora é implementado de forma gerenciada, monitorada e ajustada e seus produtos de trabalho são estabelecidos, controlados e mantidos apropriadamente. Nível 3: Processo estabelecido - O Processo Gerenciado, descrito anteriormente, agora é implementado utilizando um processo definido capaz de atingir seus resultados. Nível 4: Processo previsível - O processo estabelecido, descrito anteriormente, agora opera dentro de limites definidos para atingir seus resultados. Nível 5: Processo em otimização - O processo previsível, descrito anteriormente, é melhorado continuamente para atingir metas de negócio relevantes, atuais e projetadas.

11

WIKIPEDIA. **Planejamento Estratégico.**
O Planejamento estratégico é um processo gerencial que diz respeito à formulação de objetivos para a seleção de programas de ação e para sua execução, levando em conta as condições internas e externas à empresa e sua evolução

esperada. Também considera premissas básicas que a empresa deve respeitar para que todo o processo tenha coerência e sustentação. Para Bateman e Snell (1998), a administração estratégica é um processo envolvendo administradores de todos os níveis da organização, que formulam e implementam objetivos estratégicos. Já o Planejamento Estratégico seria o processo de elaboração da estratégia, na qual se definiria a relação entre a organização e o ambiente interno e externo, bem como os objetivos organizacionais, com a definição de estratégias alternativas.

12

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.196. Plano estratégico de TI (IT strategic plan) – Plano de longo prazo, ou seja, com horizonte de três a cinco anos, no qual as direções de negócios e de TI colaborativamente descrevem como os recursos de TI contribuirão com o objetivos estratégicos da organização.

13

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.**
p.4. Política - Instruções claras e mensuráveis de direção e comportamento desejado que condicionem as decisões tomadas dentro de uma organização.

14

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**
p.8. Política de Segurança da Informação - Documento que declara o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a segurança da informação.

15

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.196. Portfólio (Portfolio) – Um grupo de programas, projetos, serviços ou bens selecionados, gerenciados e monitorados para otimizar o retorno do negócio.

16

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.**
p.4. Tecnologia da Informação (TI) - Os recursos necessários para adquirir, processar, armazenar e disseminar informações. Este termo também inclui "Tecnologia da Comunicação (TC)" e o termo composto de "Tecnologia da Informação e Comunicação (TIC)".

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**

p.198. TI – Tecnologia da informação (IT – Information technology) – Refere-se ao hardware, software, comunicação e outras facilidades usadas para entrada de dados, armazenagem, processamento, transmissão e saída de dados de qualquer forma.