POLÍTICAS E QUALIDADE EM T.I

(Gestão do Conhecimento)

Unidade 02

Prof. Daniel Caixeta

Atualizado em 2.2025

CONTEÚDO PROGRAMÁTICO

05 Governança em T.I: Conceitos e visões da T.I

5.1. O que Governança em T.I?

5.2. A visão da Governança.

- 5.2.1. Do alinhamento ao *compliance*.
- 5.2.2. Decisão, compromisso, priorização e alocação de recursos.
- 5.2.3. Estrutura, processo, operações e gestão.
- 5.2.4. Gestão de valor e desempenho.

5.3. Gestão *versus* Governança.

06 Políticas de Governança em T.I: Conceitos, abordagens, diretrizes.

6.1. O que são Políticas de Governança em T.I?

6.2. Qual abordagem adotar?

6.3. Quais tipos de organizações precisam de Políticas de T.I?

6.4. Definições aplicáveis à Governança em T.I.

6.5. Os objetivos [...].

6.6. Os princípios [...].

6.7. A governança dos dados.

6.8. Principais desafios da gestão de políticas em T.I.

CONTEÚDO PROGRAMÁTICO

07

Políticas em T.I: Estruturas funcionais, normas e regras.

7.1. Finalidades, áreas de aplicações [...].
7.2. Dos princípios básicos: Gerais e Obrigatórios.
7.3. Dos procedimentos gerais.
7.4. Segurança da Informação.
7.5. Auditoria e monitoração eletrônica.
7.6. Testes e homologação.
7.7. Documentação.
7.8. Arquitetura de segurança e integridade dos dados.
7.9. Conclusão.

Referências

5. GOVERNANÇA EM T.I

Conceitos e visões: Do alinhamento à gestão de valores [...]

5.1. O QUE É GOVERNANÇA EM T.I?

- De acordo com a ISO/IEC 38.500 (ABNT 2009), Governança de T.I é:

> O sistema pelo qual o uso atual e futuro da T.I são dirigidos e controlados. Significa avaliar e direcionar o uso da T.I para dar suporte à organização e monitorar seu uso para realizar planos. Inclui a estratégia e as políticas de uso da T.I dentro da organização. (grifo meu).

- Analisando a definição, conclui-se que a Governança de T.I, além de buscar o direcionamento para atender ao negócio, monitora e verifica a conformidade com a direção tomada pela gestão. Portanto, não é somente implantar modelos de melhores práticas, tais como CobiT, ITIL, CMMI, MPS.br, etc., mas também avaliar politicamente os cenários internos e externos.

- Então, diante dessa visão, entende-se que a Governança de T.I deverá promover:

1. O seu alinhamento ao negócio (suas estratégias e objetivos), tanto no que diz respeito às aplicações quanto à infraestrutura de serviços.
2. A implantação de mecanismos que garantam a continuidade do negócio contra interrupções e falhas (manter e gerir as aplicações e a infraestrutura de serviços).
3. E, juntamente com áreas de controle interno, *compliance* e gestão de riscos, o alinhamento da T.I a marcos de regulação internos e externos, além de outras normas.

5.2. A VISÃO DA GOVERNANÇA

- Essa visão vai além das noções e conceitos apresentados até aqui. Caso ampliemos este campo, podemos representá-lo como um ciclo de Governança em T.I aplicado às organizações, conforme a figura abaixo.

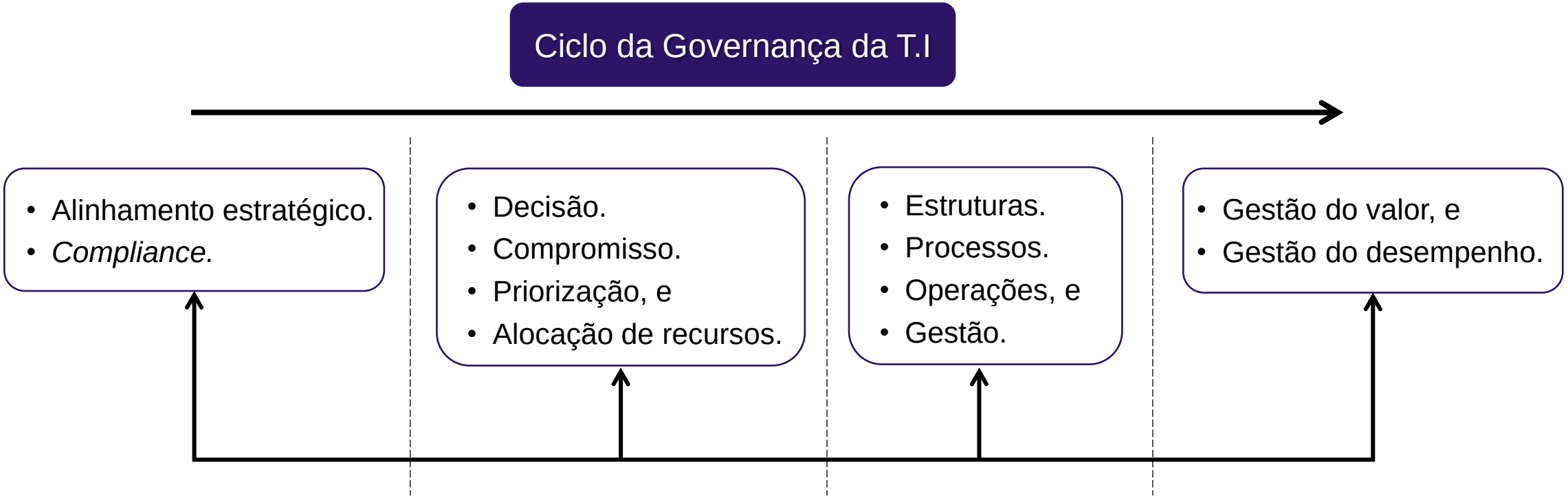


Figura 1. Ciclo da Governança de T.I. (Fernandes & Abreu, 2012).

5.2.1. DO ALINHAMENTO AO *COMPLIANCE*

- De acordo com Fernandes & Abreu (2012), se refere ao planejamento da T.I, levando em consideração as estratégias das organizações para os seus vários produtos e segmentos de atuação, assim como os requisitos de *compliance* internos e externos, *e.g.*, *Sarbanes-Oxley Act*, o Acordo da Basiléia, o Marco Civil da Internet[1], Lei Geral de Proteção de Dados (LGPD)[2], etc.

1, 2. O Marco Civil da Internet e a LGPD foram publicadas posteriormente à obra referenciada.

5.2.2. DECISÃO, COMPROMISSO, PRIORIZAÇÃO E ALOCAÇÃO [...]

- Segundo Fernandes & Abreu (2012), se referem às responsabilidades pelas decisões relativas à T.I em termos de:
  - ✓ Arquitetura de T.I.
  - ✓ Serviços de infraestrutura.
  - ✓ Investimentos.
  - ✓ Necessidades de aplicações.
  - ✓ Definição de mecanismos e tomada de decisões.
  - ✓ Etc.
- Adicionalmente, trata-se do envolvimento dos principais tomadores de decisões da organização, assim como da definição de prioridades de projetos e serviços e da alocação efetiva de recursos monetários no contexto de um portfólio de T.I.

5.2.3. ESTRUTURA, PROCESSO, OPERAÇÕES E GESTÃO

- Refere-se à estrutura organizacional e funcional da T.I.
- Aos processos de gestão e operação dos produtos e serviços, alinhados com as necessidades estratégicas e operacionais da empresa.
- Nesta fase são definidas ou redefinidas:
  - ✓ As operações de sistemas.
  - ✓ Infraestrutura.
  - ✓ Suporte técnico.
  - ✓ Segurança da informação.
  - ✓ Governança de T.I.
  - ✓ Outras funções auxiliares ao CIO.
  - ✓ Etc.

5.2.4. GESTÃO DE VALOR E DESEMPENHO

- Refere-se à determinação, coleta e geração de indicadores de resultados dos processos, produtos e serviços de T.I, à sua contribuição para as estratégias e objetivos do negócio e à demonstração do valor da T.I para o negócio.

5.3. GESTÃO *VERSUS* GOVERNANÇA

GESTÃO	GOVERNANÇA
Controle dos sistemas operacionais.	Fiscalizar o cumprimento das regras.
Suporte aos processos da empresa.	Gerenciar riscos.
Administração dos equipamentos e ferramentas informatizadas.	Realizar auditorias.
Manter o desempenho do serviço.	Auxiliar na tomada de decisão.
Garantir a resolução dos problemas dos usuários.	Adotar políticas de segurança.

6. POLÍTICAS DE GOVERNANÇA EM T.I

Conceitos, abordagens, diretrizes.

6.1. O QUE SÃO POLÍTICAS DE GOVERNANÇA EM T.I?

- Política de Governança de Tecnologia da Informação (PGTI) é definido como:

> O marco normativo que estabelece diretrizes para a organização de pessoas, processos e ferramentas em torno de objetivos que permitam o avanço da T.I alinhada às atividades fins da organizações e suas boas práticas de gestão (CVM, 2022).

- Portanto, Políticas de T.I ou de Governança em T.I, são regras, normas, diretrizes, métodos e procedimentos que estão reunidos em documentos cuja função é orientar todos os colaboradores no uso e nas referências adotadas nas organizações.

- Na elaboração das políticas para uma organização, recomenda-se seguir as 10 etapas descritas abaixo[3]:

RECOMENDAÇÕES	
1. Diagnóstico preliminar.	6. Treinamento.
2. Identificar deficiências.	7. Atualizações.
3. Aprovação.	8. Monitoramento.
4. Criação de um comitê.	9. Nova tecnologias.
5. Aprovação do R.H.	10. Conscientização.

3. Fonte: https://www.scurra.com.br/blog/como-esta-a-politica-de-ti-da-sua-empresa/

6.2. QUAL ABORDAGEM ADOTAR?

- De modo geral, os temas abordados na construção das políticas em T.I, dependem do foco organizacional em relação aos negócios. Geralmente são esses:

1. Uso aceitável da tecnologia: Diretrizes para o uso de computadores, telefones, *internet*, *e-mail*, acesso remoto, bem como as consequências para uso indevido.

2. Segurança: Diretrizes para senhas, níveis de acesso à rede, proteção contra vírus, *spywares*, *malwares*, *pishing*, confidencialidade e uso de dados.

3. Recuperação de dados: Diretrizes para recuperação de dados e métodos de armazenamento de dados e informações (*backups*).

4. Padrões de tecnologia: Diretrizes para determinar o tipo de *software*, *hardware* e sistemas que serão adquiridos e utilizados pela organização, incluindo programas proibidos.

5. Configuração de rede e documentação: Diretrizes sobre como a rede é configurada, como adicionar novos funcionários à rede, níveis de permissão para funcionários e licenciamento de *software*.

6. Serviços de T.I: Diretrizes para determinar como as necessidades e os problemas de tecnologia serão abordados, quem na organização é responsável pelo suporte técnico, manutenção, instalação e planejamento de tecnologia de longo prazo.

- É importante observar, que as Políticas de T.I, não devem ser muito extensa e de complexa compreensão. Caso seja, provavelmente será ignorado institucionalmente.

6.3. QUAIS TIPOS DE ORGANIZAÇÕES PRECISAM DE POLÍTICAS DE T.I?

- A resposta é simples:

  Toda empresa que possui infraestrutura de T.I, e que diariamente utilizam computadores, sistemas de impressão, *e-mail*, *internet* e *softwares* deve ter Políticas de T.I em vigor.

- Existem vários motivos, mas apresentamos aqui dois:
  1. A empresa se protege com políticas para lidar com questões como uso pessoal de *internet* e *e-mail*;
  2. Os funcionários sabem o que é esperado e exigido deles ao usar a tecnologia fornecida pelo seu empregador.

6.4. DEFINIÇÕES APLICÁVEIS À GOVERNANÇA EM T.I

- Alguns conceitos são importantes na aplicação em áreas afins. Segue aqui algumas definições aplicadas ao contexto de Políticas e Governança em T.I segundo o art. 2º da Portaria CVM/PTE/nº 92, 17.ago.2020[4].

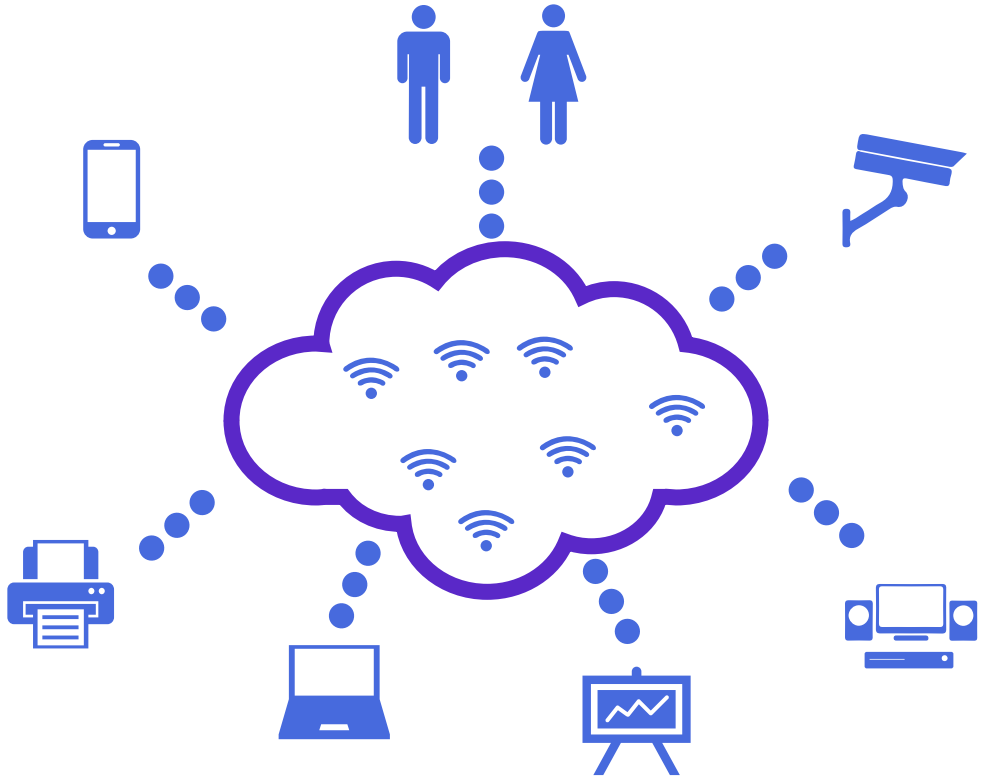
    I. T.I: Ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar e disseminar informações.

    II. Governança de T.I: Sistema pelo qual o uso da T.I é dirigido e controlado, consistindo de políticas, de papéis, de fluxos e de regras que alinham a T.I aos objetivos estratégicos da organização.

4. Acesse o ícone para a Portaria CVM/PTE/nº 92/2020.

III. Planejamento Estratégico: Processo gerencial que permite estabelecer a direção a ser seguida pela autarquia, visando maior grau de interação com o ambiente.

IV. Solução de T.I: Conjunto de bens e/ou serviços de T.I e automação que se integram para o alcance dos objetivos da organização.



6.5. OS OBJETIVOS [...]

- Citemos alguns objetivos políticos da Governança em T.I, de acordo com art. 4º do CVM/PTE nº 92/2020:

I. Alinhar a T.I às necessidades do negócio, às normas e aos padrões aplicáveis, buscando a otimização de resultados, o tratamento de riscos e a sustentabilidade das soluções.

II. Engajar pessoas em processos de melhoria contínua para garantir a elevação do nível de competências individuais e organizacionais.

III. Aumentar o valor das soluções entregues, a produtividade do trabalho e a capacidade de atendimento aos usuários.

IV. Promover o uso eficaz, eficiente e gerenciado da T.I pelos componentes organizacionais.

V. Promover alinhamento das boas práticas de Governança e Gestão de T.I às estratégias, planos e processos de T.I.

VI. Definir os mecanismos de transparência e prestação de contas dos investimentos de recursos aplicados em iniciativas de T.I.

6.6. OS PRINCÍPIOS [...]

Os princípios da Governança de T.I, segundo art.11 CVM/PTE nº 92/2020, são:

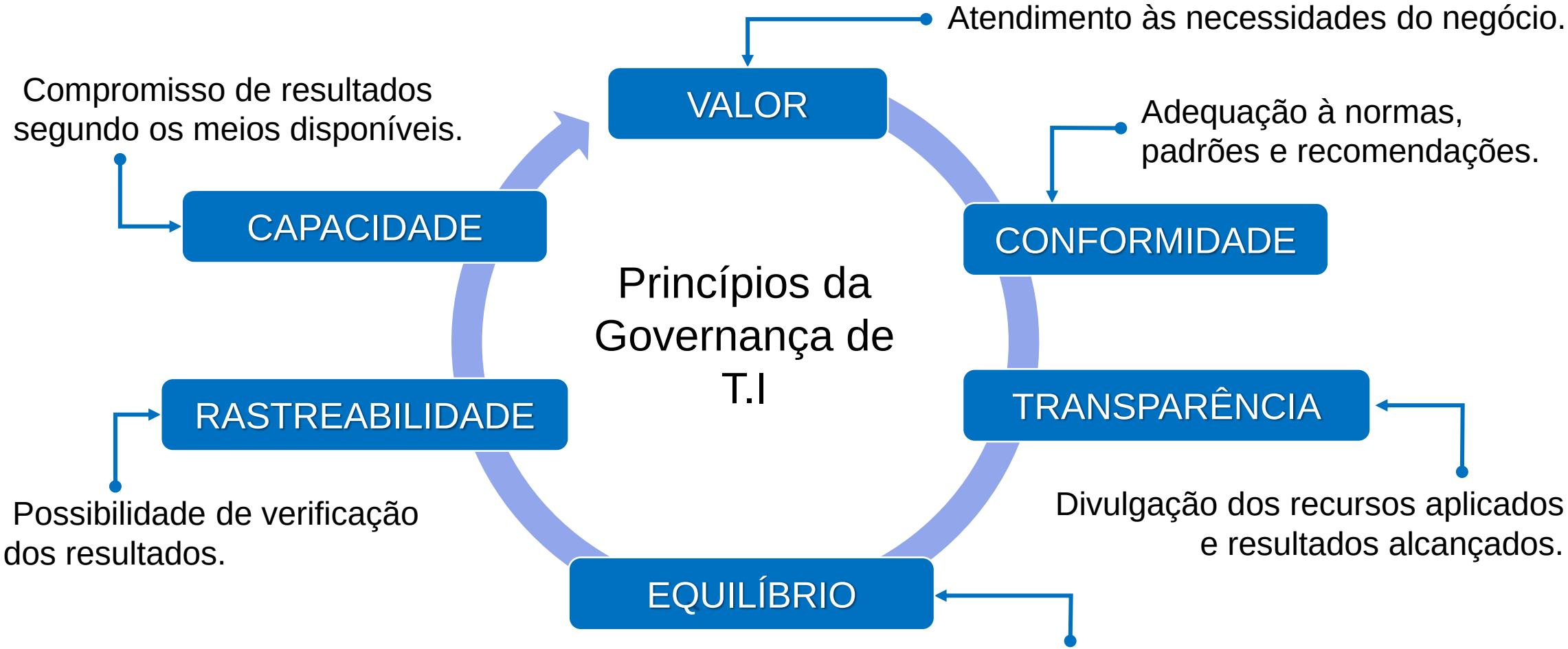


Figura 2. Princípios políticos da Governança em T.I.

6.7. A GOVERNANÇA DOS DADOS

- Já no artigo 14, da mesma portaria, as diretrizes que regem a Governança de Dados nas organizações são:

  I. A Governança de dados deve compreender todos os dados críticos para o negócio, sejam eles brutos ou tratados, públicos ou confidenciais, estruturados ou não.

  II. Os processos de gestão dos dados devem compreender todo o ciclo da informação: produção, processamento, uso, disseminação, armazenamento e retenção.

  III. A T.I e o negócio devem desenvolver parcerias produtivas, contínuas, estruturadas, de modo que, conjuntamente, capacitem-se para os crescentes desafios sobre dados.

  IV. Os dados devem ser autênticos, significativos, íntegros, consistentes, em tempo apropriado e disponíveis à tomada de decisão.

IV. Dados relevantes à sociedade devem estar disponíveis no Portal de Dados Abertos[5] mediante processos adequados de liberação e publicação.

V. As taxas de crescimento do volume e do custo do armazenamento devem ser estimadas, antecipando-se a eventos de restrição de capacidade.

VI. Os dados devem ser protegidos contra o acesso indevido, seja pela adoção de meios tecnológicos, seja pela adequada compreensão das normas aplicáveis.

VII. A terminologia deve ser unívoca, atual, documentada, de uso cotidiano, capaz de promover o melhor entendimento sobre os dados.

VIII. Os metadados e as regras de negócio relativas aos dados devem ser atualizados e gerenciados em sincronia com as mudanças no modelo e na arquitetura dos dados.

5. Fonte: https://dados.gov.br/

6.8. PRINCIPAIS DESAFIOS DA GESTÃO DE POLÍTICAS EM T.I

Políticas de conformidade.

Políticas de formação/capacitação em revisão de artefatos documentais.

Políticas de divulgação.

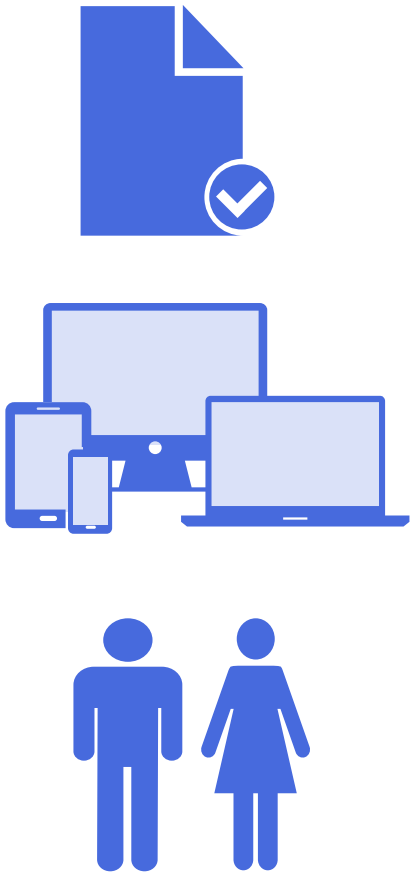
Políticas de controle.

7. POLÍTICAS EM T.I

Estruturas funcionais, regras e normas.

7.1. FINALIDADE, ÁREAS DE APLICAÇÕES [...]

- De acordo com Serqueira (2017), a finalidade de um documento de Políticas de T.I é estabelecer um conjunto de controles e responsabilidades que resultem em maior segurança na disponibilização e utilização de recursos de *hardwares*, sistemas de aplicativos, *softwares,* etc., que serão utilizados na organização, assim como garantir a manutenção do parque tecnológico e continuidade do negócio.
- Esta política se aplica a todos os usuários que irão desenvolver as diversas atividades ali desempenhadas.



7.2. DOS PRINCÍPIOS BÁSICOS: GERAIS E OBRIGATÓRIOS

A . GERAIS

- Os aspectos referentes aos controles internos poderão ser objeto de auditoria quanto à sua efetiva aplicação e eficácia.
- Já em relação à violação da política de segurança de T.I, esta pode levar a suspensão temporária, ou até mesmo definitiva do acesso do usuário aos recursos de T.I, e também às sanções em conformidade com a legislação trabalhista e normas internas da organização.

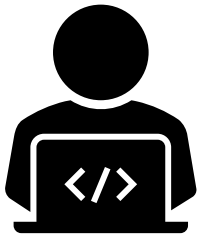
B . DAS OBRIGAÇÕES

- Em relação às obrigações, atribui-se responsabilidades para os principais a-gentes.

B.1. Obrigações do corpo diretivo

a. Validar as propostas de revisão visando contínua adequação e eficácia dos controles implementados.
b. Autorizar providências para obtenção dos recursos necessários para o cumprimento da política de segurança de T.I.
c. Promover o desenvolvimento da cultura de segurança de T.I junto aos usuários sob sua responsabilidade e zelar pelo cum-primento da mesma.

B.2. Obrigações dos usuários



a. Zelar pelos recursos de T.I (equipamentos e *softwares*) sob sua responsabilidade ou que venha a ter acesso.
b. Proteger todas e quaisquer informações às quais tenha acesso e responsabilidade.
c. Relatar qualquer situação relacionada ao uso dos recursos de T.I, que possam prejudicar a continuidade dos serviços oferta-dos pela organização.

B.3. Obrigações da T.I

a. Zelar pela disponibilidade dos recursos de modo a não gerar atrasos ou prejuízos em nenhum processo, garantindo a não descontinuidade das operações pelos usuários.

b. Envidar esforços na busca de soluções nas interrupções, procurando eliminar ou minimizar ao máximo os prejuízos às operações.

c. Monitorar e implementar os processos de controle e operação propostos nesta política garantindo sua atualização e proteção quanto ao uso inadequado dos recursos de T.I, mudanças na legislação e/ou nos requisitos do negócio.

d. Assegurar que o acesso aos recursos de T.I estejam em conformidade com as definições constantes na “Política de acesso e condições de uso”.

7.3. DOS PROCEDIMENTOS GERAIS

A. CONTROLE DE ACESSO

- Todo cadastro de usuário será mantido no sistema ou aplicação.
- As informações dos usuários deverão possuir, no mínimo, os seguintes campos:
    1. Nome completo do usuário;
    2. Tipos de usuários:

✓ Empregado	✓ Estagiário
✓ Prestador de serviço	✓ Auditor
✓ Consultor	

B. PERFIL DO USUÁRIO

- O perfil serve para identificar as funcionalidades, os poderes de acessos e permissões dos usuários ao sistema em geral, podendo ser:

i. Gerente/Administrador. ii. Usuário comum.

- É importante que o S.I registre qual o motivo da criação do usuário:

i. Admissão.

ii. Contratação.

ii. Autorização.

Obs.: É importante que o sistema mantenha as datas de alterações nas permissões dos usuários, assim como a identificação de quem realizou as atualizações.

- O S.I deverá permitir:

a. Customização de senhas:
   - ✓ Definição de tempo para bloqueio ou expiração de contas e/ou senhas.
   - ✓ Definição do número máximo de tentativas de acesso incorretas consecutivas com bloqueio de contas e/ou senhas.

b. Controlar o acesso de forma uniforme, utilizando uma única rotina de verificação e gerenciamento centralizada:
   - ✓ Os usuários deverão ter acesso concedido apenas através do perfil, e nenhum usuário poderá ter mais de um perfil.
   - ✓ A autorização para utilização de cada função, tela ou módulo do sistema deverá ser concedida pela hierarquia superior.

c. O bloqueio de acesso ao sistema de forma automática, ou manual, quando da ausência temporária do usuário por motivo diversos.

d. Todo acesso ao sistema deverá ser realizado através da identificação do usuário e autenticação de senha.
   - ✓ É de responsabilidade do usuário os cuidados com a manutenção de segurança e sigilo da senha, evitando sua utilização indevida: “As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em hipótese nenhuma”.

e. As contas com privilégios administrativos das bases de dados, serão concedidas apenas para a equipe de T.I, com assinatura do “Termo de responsabilidade de Acesso e Concessão de Acesso ao Banco de Dados” da organização.

f. Os sistemas desenvolvidos ou adquiridos pela organização não devem utilizar contas administrativas ou privilegiadas (*e.g*., *root*, *administrators*, *dba*, etc.) de sistemas operacionais, servidores *web* ou banco de dados.

g. O sistema, ou a rede à qual estiver utilizando, deverá desconectar o usuário por tempo de inatividade superior a X minutos.

h. Nos casos em que a aplicação necessite estar conectada diretamente à *internet* (*e.g*., portais *web*), a mesma deverá estar segregada física e/ou logicamente da rede corporativa (*e.g*., através de *firewall*) e protegida por mecanismo de detecção e prevenção de intrusos, em rede própria ou terceirizada.

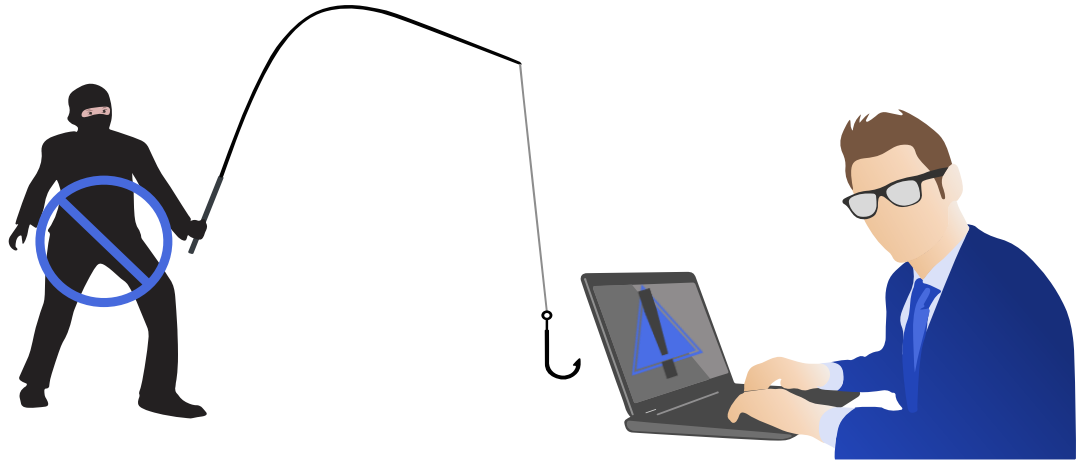
i. Os desenvolvedores e testadores devem estar autenticados lógica e fisicamente ao acessar os ambientes de desenvolvimento e homologação.

   - ✓ Não é permitido, mesmo nestes ambientes, acesso não identificado ou com conta genérica.

j. A extração da base de dados deve ser efetuada pela equipe de T.I, e com autorização formal do superior imediato, i.e., afim de evitar o vazamento de informações.

7.4. SEGURANÇA DA INFORMAÇÃO

- Os sistemas que utilizam informações confidenciais deverão usar mecanismos criptográficos para a proteção dos dados. Este procedimento aplica-se principalmente às transmissões eletrônicas.
- Sistemas disponíveis na *internet* e que trafeguem informações confidenciais deverão utilizar mecanismos de autenticação para a segurança e proteção.
- Os sistemas cujas informações estiverem expostas ao risco de perda de integridade deverão utilizar mecanismos de verificação para a proteção.



7.5. AUDITORIA E MONITORAÇÃO ELETRÔNICA

- Todos os sistemas desenvolvidos ou adquiridos pela organização devem conter registros de auditoria (*logs*).
- Estes registros devem ser gravados com data/hora de ocorrência, endereço I.P e *hostname* (endereço da estação de trabalho), conta utilizada, e deve registrar, minimamente, os seguintes eventos:
  - ✓ Falhas de acesso nos sistemas.
  - ✓ Acessos e alterações em dados confidenciais utilizados pelos sistemas.
  - ✓ Criação e remoção de usuários.
  - ✓ Atribuição e remoção de direitos e acessos do usuário.
- Deve haver uma *interface* amigável para consulta dos *logs*.

- Todos os *logs* devem ser protegidos, cabendo apenas, usuários com perfis específicos e restritos, o acesso e a possível deleção dos dados.
- Os registros devem ser desenvolvidos e configurados de forma a evitar a exaustão da trilha de auditoria (*e.g.*, através de *log rotation*).
- Os *logs* deverão ser mantidos por um período mínimo de tempo determinado pelos gestores, devendo considerar os aspectos legais e regulatórios envolvidos, bem como as necessidades de negócio.
  - ✓ Recomenda-se, nos casos omissos, a manutenção dos mesmos por um período não inferior a 5 anos.

7.6. TESTES E HOMOLOGAÇÃO

- Todo sistema desenvolvido ou adquirido deve ser testado e homologado antes de ser colocado em produção. Os testes devem contemplar no mínimo:
    1. Validação de todas as entradas de dados (de usuários ou *interface* com outros sistemas) quanto a formato dos dados e valores/caracteres esperados.
    2. Implementação de funcionalidades de segurança, incluindo todas as condições definidas neste documento.
- Todo sistema desenvolvido ou adquirido deve garantir que:
    1. Os arquivos e componentes desnecessários para o funcionamento do sistema aplicativos sejam removidos no ambiente de produção.
    2. As bibliotecas e componentes externos utilizados no sistema aplicativo devem ser homologadas previamente.

7.7. DOCUMENTAÇÃO

- Todo sistema desenvolvido ou adquirido deverá possuir manual de instrução, contendo:
  - Procedimentos de instalação que contenham, no mínimo:
    1. Itens de verificação do ambiente antes da instalação (*e.g.*, espaço mínimo em disco, memória, etc.).
    2. Definições de configuração e primeiro uso (*e.g.*, parâmetros alteráveis e configuráveis para primeira utilização do sistema).
  - Procedimentos de segurança que contenham, no mínimo:
    1. Informações para recuperação em casos de erro, falhas ou incidentes.
    2. Definições sobre atualização, *backup*, auditoria e monitoração (caso não atendam ao padrão estabelecido pela área de T.I).

7.8. ARQUITETURA DE SEGURANÇA E INTEGRIDADE DOS DADOS

- Os ambientes de desenvolvimento, homologação e produção devem ser física e logicamente isolados, a fim de:
    a. Reduzir o acesso físico de pessoas externas aos ambientes.
    b. Reduzir o acesso dos desenvolvedores ao ambiente de produção.
    c. Garantir a qualidade das funções de segurança do sistema gerado.
- Deve-se evitar misturar informações entre os ambientes de desenvolvimento.
- Os aplicativos devem ser passados do ambiente de desenvolvimento para homologação somente após a conclusão bem sucedida da remoção de informações de depuração.

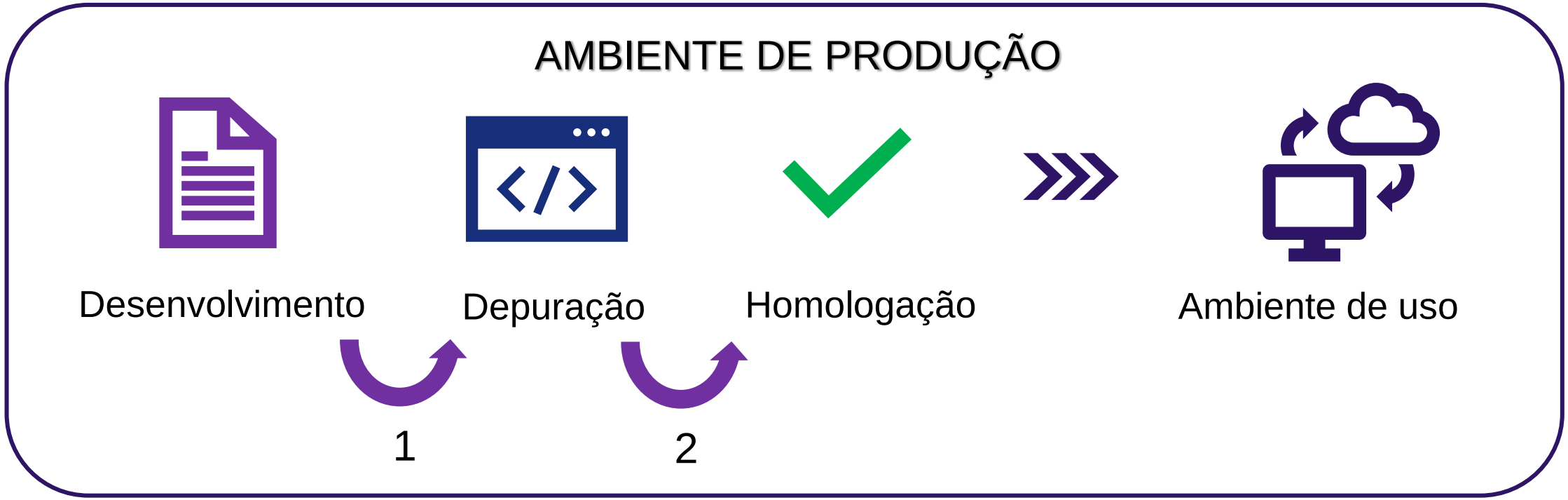


Figura 3. Transição entre os ambientes de desenvolvimento, depuração e homologação e início no ambiente de uso.

- A arquitetura do ambiente de homologação deve ser o mais semelhante possível ao do ambiente de produção, a fim de garantir a qualidade dos testes e evitar o emascaramento de falhas.

1. Somente após a conclusão bem sucedida da remoção de informações de depuração.
2. Somente após a conclusão bem sucedida de todos os testes funcionais de segurança e vulnerabilidades previstos.

- No S.I não deverá haver portas lógicas ou meios alternativos (*e.g*., *backdoors*, *maintenance hooks*) de acesso aos sistemas desenvolvidos ou adquiridos pela organização.
- Todas as aplicações *web* deverão ser desenvolvidas de forma componentizada, permitindo a distribuição destes componentes (*e.g*., *front-end*, *back-end* e banco de dados) por diferentes áreas da rede (*e.g*., DMZ, rede interna), própria ou terceirizada.
- Todo sistema desenvolvido e/ou adquirido pela organização deverá preferencialmente conter mecanismos de *backup* e restauração dos dados processados, além de possuir capacidade de tolerância a falhas e retorno à operação. Em casos omissos, fica a T.I responsável pela elaboração de política de *backup* e *restore* dos bancos de dados e ou arquivos dos sistemas instalados.

- Na ocorrência de erros nos sistemas aplicativos instalados, os usuários deverão enviar *email*, descrevendo o erro, a tela ou a função que estava executando, e se possível o *print* da tela em anexo.
- A área de T.I então encaminhará o erro ao fornecedor do sistema, aguardará o recebimento da correção e de sua aplicação em ambiente de validação para serem realizados testes pelo usuário reclamante e se aprovado, através de *email*, o mesmo irá solicitar a instalação da correção no ambiente de produção.

7.9. CONCLUSÃO

- Apresentamos aqui alguns elementos considerados essenciais para a elaboração de um documento que contenha as Políticas em T.I de uma organização.
- É fator condicionante que essas políticas estejam de acordo com as dimensões técnicas, humanas e organizacionais das empresas, considerando que as regras e instruções normativas já fazem partem de nossas rotinas.
- E é claro, que a responsabilidade é da gestão superior desenvolver esse trabalho e por em prática na organização.
- Torna-se necessário também as revisões sistemáticas, isto para adequar as políticas ao contexto atual da T.I

OBRIGADO!

Políticas e Qualidade em T.I & Gestão do Conhecimento

REFERÊNCIAS

LAUDON, Kenneth C., LAUDON, Jane P. Sistemas de Informações Gerenciais. 11ª ed. Pearson, 2014.

PGTI - Política de Governança de Tecnologia da Informação. Disponível em: <https://conteudo.cvm.gov.br/menu/acesso_informacao/planos/politicas/pgti/pgti.html>. Acesso em: 02.set.25.

PORTARIA CVM/PTE/No 92, DE 17 DE AGOSTO DE 2020. Disponível em: <https://www.gov.br/cvm/pt-br/acesso-a-informacao-cvm/acoes-e-programas/politica-de-governanca-de-ti/portaria_cvm_pte_092_2020_pgti.pdf>. Acesso em: 02.set.25.

Portal Brasileiro de Dados Abertos. Disponível em: <https://dados.gov.br/>. Acesso em: 02.set.25.

SCURRA T.I. Como esta a política de sua empresa? Disponível em: <https://www.scurra.com.br/blog/como-esta-a-politica-de-ti-da-sua-empresa/>. Acesso em: 02.set.25.

SERQUEIRA, Aurélia Amaro. Políticas de Tecnologia da Informação. Disponível em: https://silo.tips/download/politica-de-tecnologia-da-informaao. Acessado em: 02.set.25.