



Governança_TI



- Governança de TI (GTI) atua em um nível mais estratégico, com foco no planejamento e nas diretrizes. É parte da governança corporativa que adota ações.
- Gestão de TI administrar todos os recursos tecnológicos utilizados no dia a dia do trabalho de uma empresa. Preocupa-se mais com a aplicação das diretrizes no uso diário das ferramentas e tecnologias.





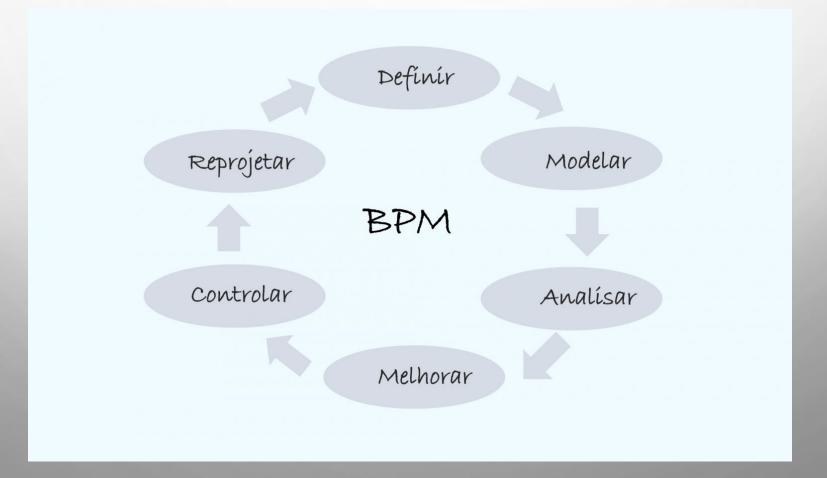
- CMMI (Capability Maturity Model Integration): objetivo desse modelo é fornecer diretrizes para melhores práticas para melhoria o processo de habilidades organizacionais, cobrindo o ciclo de vida de produtos e serviços.
- ITIL (Information Technology Infrastructure Library): objetivo de <u>descrever</u> os processos necessários para gerenciar a infraestrutura de TI de maneira eficaz para garantir os níveis de serviço para os clientes; *Processos
- PMBOK (Project Management Body of Knowledge): manual que define e descrevem as habilidades, ferramentas e técnicas para o gerenciamento de um projeto;
- BSC (Balanced Scorecard): modelo de gestão estratégica, baseado em indicadores financeiros e não-financeiros.
- ISO (International Standards Organization): normas/padrões auditáveis de alto nível voltado ao cliente para sistemas de gerenciamento de qualidade.



- Aspectos gerais e implantação do modelo. https://colaborae.com.br/blog/2022/07/18/sla-acordo-de-niveis-de-servicos/
- CMMI, PMBOK, BPM
- ISO/IEC 38500 (ABNT, 2009);
- ISSO 2700, 27002, 31000, 35030
- 20000
- 9000
- PRINCE
- VAL IT
- COSO
- ISO 17790
- ISSO 15504
- 15000
- eSCM-CL
- eSCM-SP



- BPM (Business Process Management) Os sistemas BPM são sistemas de gerenciamento e automação dos processos operacionais de rotina da empresa ... otimizam processos, reduzem custos e identificam gargalos.
- https://colaborae.com.br/blog/2020/12/04/cmmi-capability-maturity-model-integration/

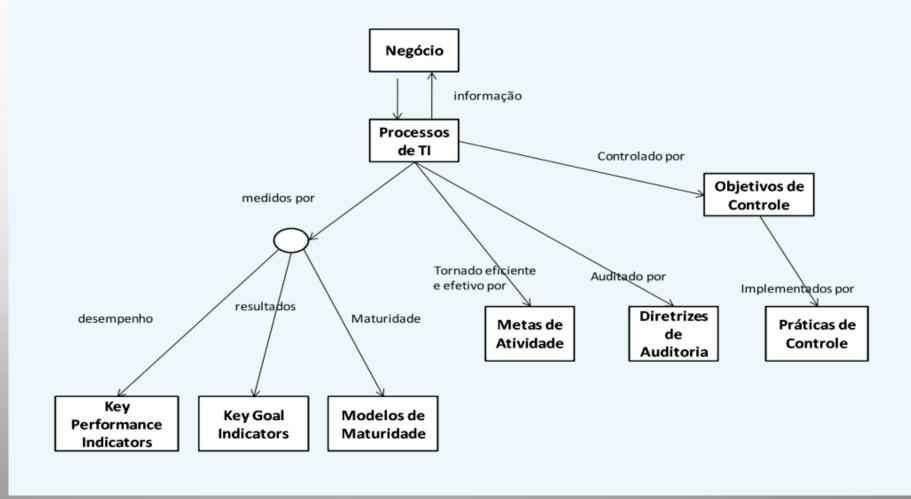




- ISO/IEC38500 Tecnologia da informação Governança da TI.
- Ele fornece um framework para a governança eficaz de TI para ajudar o mais alto nível das organizações a compreender e cumprir as suas obrigações legais, regulamentares e éticas no contexto da utilização de TI de suas organizações. Governança é diferente de gerenciamento e, para evitar confusão, os dois conceitos são claramente definidos na Norma.
- Esta Norma estabelece os princi'pios para o uso eficaz, eficiente e aceitâvel da TI. Ela assegura as organizagoes que seguem estes princi"pios que os dirigentes poderão avaliar melhor os riscos e aproveitar as oportunidades advindas com o uso da TI.
- Processos tratados por TI incorporam riscos específicos que devem ser corretamente abordados. Por exemplo, os dirigentes de organizações podem ser responsáveis por violações de:
 - Normas de Segurança;
 - · Legislação de privacidade;



• COBIT (Control Object for Information and Related Technology)



https://colaborae.com.br/blog/2020/12/04/cmmi-capability-maturity-model-integration/



- ITIL (Information Technology Infrastructure Library)
- https://colaborae.com.br/blog/2018/04/30/itil-information-technology-infrastructure-library/



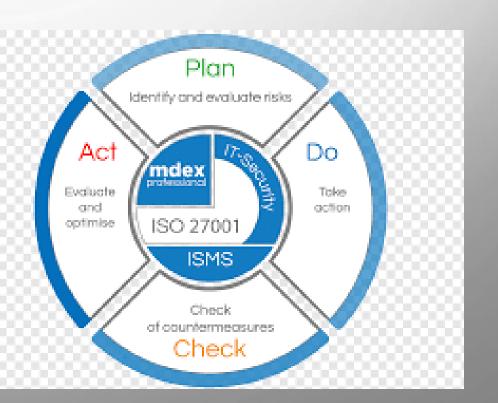


- ISO 27000 É uma norma de certificação que, por sua natureza, exige formalidade, documentação e organização.
 - Políticas e Termos de Responsabilidade;
 - Monitoramento e Controle de Acesso;
 - Conformidade;
 - Resoluções e Instruções Normativas;
 - http://www.iso27000.com.br/index.php?option=com_content&view=article&id=88:cursoisfs&catid=34:seginfartgeral&Itemid=53
 - https://colaborae.com.br/blog/2020/12/04/cmmi-capability-maturity-model-integration/



• ISO 27001 - É o padrão e a referência Internacional para a gestão da Segurança da informação. A norma tem como principio geral a adoção pela organização de um conjunto de requisitos, processos e controles com o objetivo de mitigarem e gerirem adequadamente o risco da organização.







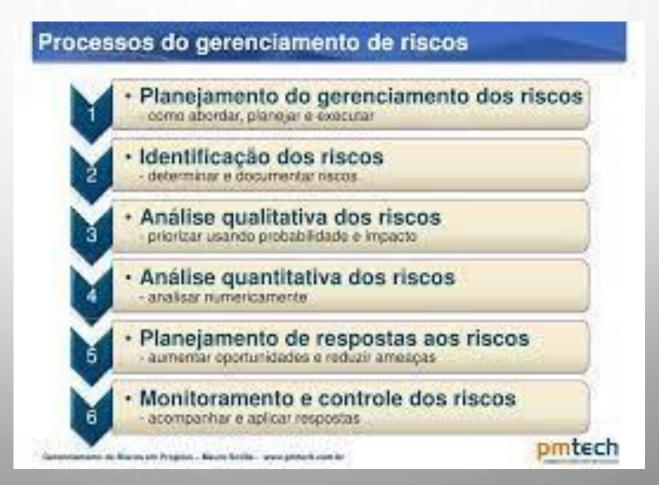
- ISO/IEC 27002 Segurança da informação, segurança cibernética e proteção da privacidade controles de segurança da informação.
- Ela descreve as melhores práticas para aqueles que implementam o SGSI, fornecendo diretrizes sobre a seleção, implementação e gerenciamento de controles levando em consideração os ambientes de risco da organização.
- Essa norma inclui métodos, técnicas e diretrizes genéricas para abordar aspectos de segurança e privacidade, como:
 - Metodologia de captura de requisitos de segurança;
 - Gestão da segurança da informação e das TIC; em particular, sistemas de gerenciamento de segurança da informação, processos de segurança e controles e serviços de segurança;
 - Mecanismos de segurança criptográficos e outros, incluindo, mas não se limitando a mecanismos de proteção da responsabilidade, disponibilidade, integridade e confidencialidade das informações;
 - Documentação de suporte ao gerenciamento de segurança, incluindo terminologia, diretrizes e procedimentos para o registro de componentes de segurança;
 - Mecanismos de segurança criptográficos e outros, incluindo, mas não se limitando a mecanismos de proteção da responsabilidade, disponibilidade, integridade e confidencialidade das informações;

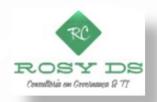


- ISO/IEC 20000 Primeira norma internacional a ter como foco o Gerenciamento de Qualidade de Serviços de Tecnologia da Informação(TI). É uma norma que tem a função de implementar um Sistema de Gerenciamento de Serviço de Tecnologia da Informação (SGSTI) em empresas, das micro às grandes, de qualquer setor, que dependam dos serviços de TI.
- Para realizar esse objetivo, a norma trabalha com uma metodologia muito conhecida: o **PDCA**.
- para conseguir esse certificado é necessária uma auditoria para avaliar se a organização segue a norma e todas as suas diretrizes. Apesar da ISO 20000 ser adaptável para diferentes tipos de empresas, ela traz critérios importantes a serem avaliados.



ISO 31000 - Este documento fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A aplicação destas diretrizes pode ser personalizada para qualquer organização e seu contexto.





• PRINCE - PRojects INControlled Environments (Projetos em Ambientes

Controlados). O PRINCE2® fornece um método que pode ser adaptado para a

"gestão de quaisquer tipos de projetos", independentemente do tamanho e

natureza.





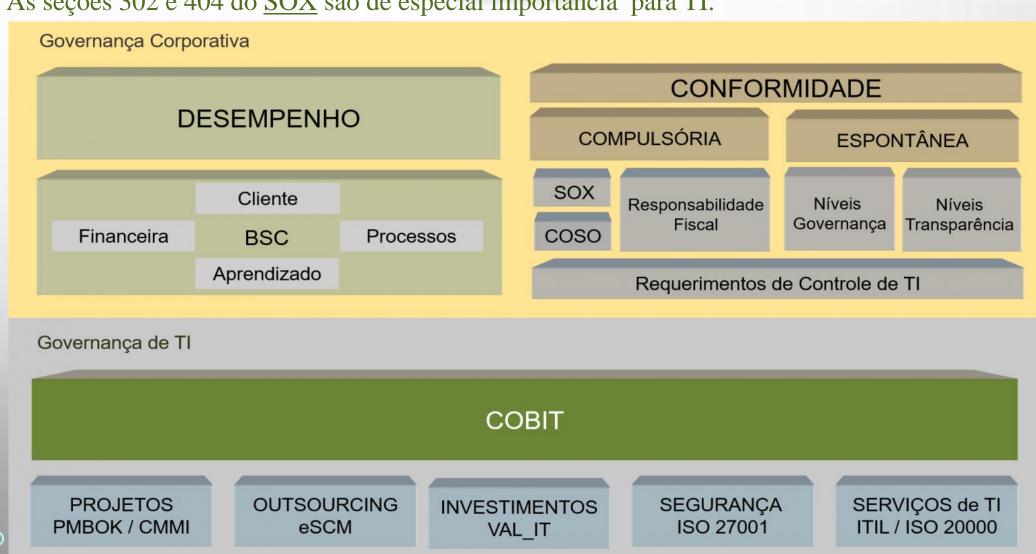
| | Establish informed and committed leadership. | Define and implement processes. | Define portfolio characteristics. |
|---|--|---|--|
| Value Governance (VG) | Align and integrate value management with enterprise financial planning. | Establish effective governance monitoring. | Continuously improve value management practices. |
| • | | | |
| | Establish strategic direction and target investment mix. | Determine the availability and sources of funds. | Manage the availability of human resources. |
| Portfolio Management (PM) | Evaluate and select programmes to fund. | Monitor and report on investment portfolio performance. | Optimise investment portfolio performance. |
| • | | | |
| Develop and evaluate the initial programme business case. | Understand the candidate programme and implementation options. | Develop the programme plan. | Develop full life-cycle costs and benefits. |
| | Develop the detailed candidate programme business case. | Launch and manage the programme. | Update operational IT portfolios. |
| Investment Management (IM) | Update the business case. | Monitor and report on the programme. | Retire the programme. |



- COSO "Committee of Sponsoring Organizations of the Treadway Commission" As áreas de principais de interesse do COSO são Governança Corporativa, Ética de Negócios, Controles Internos, Gestão de Riscos Corporativos, Fraudes e Relatórios Financeiros. É um dos padrões mais usados pelas companhias Norte Americanas para avaliar a própria observância as regras do FCPA. A clássica estrutura do COSO, descrita no ICIF, é baseada em alguns conceito de base:
- Os Controles Internos são um processo. Se trata de um instrumento para uma determinada finalidade.
- Os Controles Internos são influenciados pela pessoas. Não existem somente políticas, manuais, formulários mas sobretudo pessoas, em todos os níveis de uma organização.
- Os Controles Internos podem fornecer somente uma razoável segurança, e não uma segurança absoluta, para a diretoria de uma corporação.



As seções 302 e 404 do <u>SOX</u> são de especial importância para TI.





https://institutodc.com.br/

LGPD- Lei 13.709/18

ESCOPO DE APLICAÇÃO - Art. 1º

Afeta qualquer atividade que envolva utilização de dados pessoais, incluindo o tratamento pela internet, de consumidores, empregados, entre outros.

AUTORIZAÇÃO PARA O TRATAMENTO DE DADOS - Art. 7º

O consentimento será umas das 10 possibilidades que legitimarão o tratamento de dados pessoais

PRINCÍPIOS DE PROTEÇÃO DE DADOS - Art. 6º

Introduzidos 10 princípios da proteção de dados, incluindo-se o de demonstrar medidas adotadas para cumprir a lei (prestação de contas)

DIREITOS DOS TITULARES DE DADOS - Art. 17 a 22

Titulares dos dados terão amplos direitos: informação, acesso, retificação, cancelamento, oposição, portabilidade, entre outros.

AUTORIDADE

Autoridade Nacional de Proteção de Dados, responsável por garantir cumprimento da Lei -(MP nº 869/2018)

NOTIFICAÇÕES OBRIGATÓRIAS

- Art. 48 em caso de incidentes de segurança envolvendo os dados, nas situações aplicáveis

Conheça os 12 principais pontos
sobre a

SANÇÕES

Multa de até 50 milhões de reais por infração, entre outras sanções

OPICE BLUM

www.opiceblum.com.br

@000

APLICAÇÃO EXTRATERRITORIAL - Art. 3º

Aplica-se também a empresas que não possuem estabelecimento no Brasil

DADOS: SENSÍVEIS, DE MENORES E TRANSF. INTERNACIONAL - Art. 11, 14 E 33

Regras específicas para tratar dados sensíveis, transferência internacional de dados e utilizar dados de crianças e adolescentes

ASSESSMENT SOBRE O TRATAMENTO DE DADOS - Art. 38

Necessidade de realizar assessment de impacto à proteção de dados (semelhante ao DPIA)

MAPEAMENTO DO TRATAMENTO DE DADOS - Art. 37

Atividades de tratamento de dados devem ser registradas em relatório

DATA PROTECTION OFFICER (DPO) - Art. 41

Todo controlador de tratamento de dados pessoais, e os operadores em casos apontados pela Autoridade, deverão nomear um Encarregado pelo Tratamento de Dados Pessoais.



PUNIÇÕES ADMINISTRATIVAS











Advertência

comindicação de prazo para adoção de medidas. Corretivas.

Multa simples/multa diária

De até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluidos os tributos, limitada, no total, a RS 50.000.000,00 (cinquenta milhões de reais) por infração.

Publicização da infração

Após devidamente apurada e confirmada a sua ocorrência (Evidente prejuizo reputacional)

Bloqueio dos dados pessoais

A respeito da intração até a sua regularização

Eliminação dos dados pessoais

Referente à infração.



Direito Digital - LGPD

- Art. 1° Objetivo
- Art. 2° Fundamentos
- Art. 5° Conceitos relevantes
 - I Dado pessoal;
 - II Dado pessoal sensível;
 - III– Dado Anonimizado.
 - Pseudonimização. Consideranda (28/GDPR). Técnica de segurança.

Privacidade & Proteção de dados

- Art. 7° Respeito pela vida privacidade e familiar.
- Art. 8° Proteção de dados pessoais.
- Nossa estrutura de lei segue o GDPR.
- ANPD (Autoridade Nacional de Proteção de Dados)





LGPD & GDPR – Principais diferenças.

- Registro de Tratamentos de Dados
- A LGPD exige registro de tratamento dos dados pessoais.
- A GDPR exige o registro de tratamento de dados pessoais e especifica as informações sujeitas à manutenção de registros.
- Avaliação de Impacto sobre a Proteção de Dados
- A LGPD exige que o controlador de dados realize uma avaliação de impacto para avaliar os riscos de certas atividades de tratamento. Contudo, deixou a cargo da ANPD determinar quando essa avaliação é necessária.
- A GDPR exige que o controlador de dados realize uma avaliação de impacto para avaliar os riscos e detalha quando requer tal avaliação e o que exatamente as avaliações devem cobrir.