

Prof. esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp
- **Professor:** Todo núcleo de T.I. (Graduação e Pós) - Wyden Facimp
- **Diretor:** SCS
- **Gerente de Projetos:** Motoca Systems

Redes sociais:

- **Linkedin:** <https://www.linkedin.com/in/thalles-canela/>
- **YouTube:** <https://www.youtube.com/aXR6CyberSecurity>
- **Facebook:** <https://www.facebook.com/axr6PenTest>
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** <https://github.com/ThallesCanela>
- **Github:** <https://github.com/aXR6>
- **Twitter:** <https://twitter.com/Axr6S>

Informática Corporativa e Normas

**Entendendo a relação entre a Tecnologia da Informação e as normas
padrões.**



O que é Informática Corporativa?

Conceito básico:

- A informática corporativa refere-se ao uso estratégico da tecnologia da informação para alcançar os objetivos de negócios de uma organização.
 - Importância para o ambiente empresarial.
-



Ponto 1: Conceito básico

- Imagine uma empresa de varejo que antes dependia apenas de vendas físicas em lojas.
 - Com a informática corporativa, essa empresa poderia estabelecer uma forte presença online, usando:
 - Sistemas de comércio eletrônico para atender clientes globalmente
 - Sistemas de gestão de relações com clientes (CRM) para rastrear comportamentos e preferências de clientes e soluções analíticas para prever tendências de vendas.
-



Ponto 2: Importância para o ambiente empresarial

- **Texto:** A informática corporativa não só otimiza operações, mas também possibilita novas oportunidades de negócios, melhorando a competitividade no mercado.
-



Ponto 2: Importância para o ambiente empresarial

- **Aplicabilidade:** Bancos, por exemplo, têm usado a informática corporativa para oferecer serviços online 24/7, como internet banking, aplicativos móveis para transações bancárias, chatbots para suporte ao cliente e soluções de inteligência artificial para detectar fraudes em tempo real.
 - Sem a incorporação estratégica da TI, muitos dos serviços que consideramos padrão hoje não seriam possíveis.
-



Importância das Normas

Pontos:

- Estabelecem padrões e melhores práticas.
 - Garantem consistência e qualidade.
 - Facilitam a integração e colaboração entre empresas.
-




Estabelecem padrões e melhores práticas.

- **Exemplo:** Sem normas específicas para a fabricação de cabos USB, cada fabricante poderia criar cabos com especificações diferentes, tornando quase impossível a interconexão de dispositivos de diferentes marcas.
 - **Aplicabilidade:** Uma empresa que produz acessórios para computadores pode usar as normas para garantir a compatibilidade de seus produtos com diferentes marcas e modelos de computadores.
-




Garantem consistência e qualidade.

- **Exemplo:** Ao seguir a norma ISO 9001, uma empresa pode garantir que seus processos de produção sejam consistentes, o que por sua vez garante que cada produto tenha a mesma alta qualidade.
 - **Aplicabilidade:** Uma empresa de software que segue padrões de codificação específicos pode assegurar que todos os desenvolvedores escrevam código de maneira uniforme, facilitando a manutenção e diminuindo bugs.
-



Facilitam a integração e colaboração entre empresas.

- **Exemplo:** No setor financeiro, as normas SWIFT garantem que as transações bancárias sejam realizadas de forma padronizada em todo o mundo, permitindo que bancos de diferentes países colaborem sem complicações.
 - **Aplicabilidade:** Duas empresas que desejem criar uma parceria estratégica podem se referir às normas para estabelecer protocolos de compartilhamento de dados e integração de sistemas.
-



Normas ISO/IEC/NBR para TI


Pontos:

- Definição e abrangência das normas.
 - **Exemplos:** ISO/IEC 27001 (segurança da informação), NBR ISO 9001 (qualidade).
 - **Caso de uso:** "Como a ISO/IEC 27001 ajudou uma empresa a proteger seus dados."
-




Definição e Abrangência das Normas:

- **ISO:** International Organization for Standardization.
 - **IEC:** International Electrotechnical Commission.
 - **NBR:** Normas Brasileiras, padrões técnicos no Brasil.
 - Criadas para estabelecer padrões técnicos e melhores práticas para produtos, serviços e processos.
-



ISO/IEC 27001 (Segurança da Informação):

- Define os requisitos para sistemas de gestão de segurança da informação (SGSI).
 - **Aplicabilidade:**
 - Proteção de informações sensíveis.
 - Conformidade com regulamentações de proteção de dados.
 - Caso real: Uma financeira que adota ISO/IEC 27001 para assegurar a confidencialidade das transações e dados de seus clientes.
-



NBR ISO 9001 (Qualidade):

- Estabelece critérios para sistemas de gestão da qualidade.
 - Foco em satisfação do cliente e melhoria contínua.
 - **Aplicabilidade:**
 - Melhoria dos processos internos de uma empresa.
 - Conquistar mais confiança no mercado devido à conformidade.
 - **Caso real:** Uma indústria de eletrônicos que, após adotar a NBR ISO 9001, reduziu defeitos em seus produtos e aumentou a satisfação do cliente.
-



Outras Normas Relevantes:

- ISO/IEC 20000 (Gestão de Serviços de TI).
 - ISO/IEC 38500 (Governança de TI).
 - **Aplicabilidade:**
 - ISO/IEC 20000: Para empresas de TI focadas em oferecer serviços com qualidade e eficiência.
 - ISO/IEC 38500: Auxilia as organizações a otimizar o uso da tecnologia em benefício de stakeholders.
 - **Caso real:** Uma empresa de software que usa a ISO/IEC 38500 para garantir que suas práticas de TI estejam alinhadas com as metas de negócios.
-



Transparência nos Negócios de TI

Pontos:

- Importância da transparência para stakeholders.
 - Relação com normas e padrões.
 - **Caso de uso:** "Empresa X e a revelação de uma falha de segurança."
-



Importância da transparência para stakeholders.

- **Exemplo:** Quando uma organização opta por usar um software open-source, os stakeholders têm a capacidade de visualizar e verificar o código, aumentando a confiança no produto.
 - **Aplicabilidade:** Empresas que buscam investimento frequentemente precisam demonstrar transparência em suas operações de TI para ganhar a confiança de potenciais investidores.
-




Relação com normas e padrões.

- **Exemplo:** A adesão à norma ISO/IEC 27001 de segurança da informação requer transparência na forma como os dados são gerenciados e protegidos.
 - **Aplicabilidade:** Organizações que buscam certificações muitas vezes precisam mostrar evidências claras de suas práticas de TI, o que reforça a importância da transparência.
-



Caso de uso: "Empresa X e a revelação de uma falha de segurança."

- **Descrição:** A Empresa X, uma popular prestadora de serviços de nuvem, descobriu uma falha de segurança que poderia expor dados de clientes. Em vez de esconder a falha, a empresa optou por comunicar proativamente o problema a seus clientes, explicando a natureza da falha, as ações tomadas para corrigi-la e as medidas de prevenção para o futuro.
 - **Resultado:** A resposta dos clientes foi predominantemente positiva. Apesar do inconveniente inicial, a transparência da Empresa X fortaleceu a confiança do cliente a longo prazo.
 - **Aplicabilidade:** No mundo digital atual, onde as falhas de segurança são inevitáveis, a maneira como uma empresa responde pode fazer toda a diferença. Optar pela transparência pode converter uma crise potencial em uma oportunidade de fortalecer relações e confiança.
-



Entendendo a SOX (Lei SarbanesOxley)

Pontos:

- Origem e objetivos.
 - Mecanismos de auditoria e segurança.
 - Responsabilidades dos Diretores Executivos e Financeiros.
 - **Exemplo:** "Empresa Y e a conformidade com SOX."
-



Contextualização da SOX

- **Título:** "Origem da SOX"
 - **Pontos:**
 - Reação aos escândalos financeiros no início dos anos 2000 (Ex: Enron, WorldCom).
 - **Objetivo principal:** Proteger acionistas e o público de fraudes contábeis e práticas empresariais ruins.
 - Implementada em 2002 nos EUA.
-



Contextualização da SOX

Principais Provisões da SOX

- **Título:** "O que a SOX aborda?"
 - **Pontos:**
 - **Seção 302:** Responsabilidade dos Diretores Executivos e Financeiros por relatórios financeiros.
 - **Seção 404:** Empresas devem publicar informações sobre a eficácia de seus controles internos.
 - **Seção 802:** Criminaliza a destruição de registros necessários para investigações federais.
-



Implicações para a TI

- **Título:** "SOX e a Tecnologia da Informação"
 - **Pontos:**
 - TI desempenha papel crucial para atender às exigências da SOX.
 - Controles internos de TI para assegurar integridade dos dados financeiros.
 - **Exemplo:** Sistema de backup com registros de alterações, monitoramento de acesso a sistemas financeiros.
-



Caso de Uso 1 - HP

- **Título:** "HP e a Conformidade com a SOX"
 - **Pontos:**
 - Em 2006, o escândalo de espionagem da HP levou a preocupações sobre governança.
 - SOX desempenhou papel importante em reformular a responsabilidade.
 - Implementação de melhores práticas em TI para garantir transparência e integridade dos dados.
-



Caso de Uso 2 - Microsoft

- **Título:** "Microsoft: Um Exemplo de Conformidade Proativa"
 - **Pontos:**
 - Microsoft já tinha práticas de contabilidade robustas antes da SOX.
 - Usou SOX como uma oportunidade para melhorar ainda mais.
 - Investiu em sistemas avançados de TI para monitorar e garantir a conformidade, tornando-se referência no setor.
-



Aplicabilidade da SOX no Mundo Corporativo

- **Título:** "Benefícios Indiretos da Conformidade SOX"
 - **Pontos:**
 - Melhoria da confiança dos investidores.
 - Fortalecimento dos controles internos.
 - Prevenção contra fraudes financeiras.
 - Reforça a importância do papel da TI na integridade dos dados financeiros.
-



CMMI: Melhorando a Maturidade em Processos"

Pontos:

- O que é CMMI (Capability Maturity Model Integration).
 - Práticas (Genéricas ou Específicas).
 - CMMIDEV, CMMIACQ, CMMISVC e SEI.
 - **Caso de uso:** "Como o CMMI-DEV transformou o desenvolvimento de software na Empresa Z."
-



Introdução ao CMMI

- **Definição:** "CMMI (Capability Maturity Model Integration) é um modelo de referência que contém práticas (genéricas ou específicas) necessárias à maturidade em disciplinas específicas."
-



Níveis de Maturidade

- **Níveis 1-5:** Inicial, Gerenciado, Definido, Quantitativamente Gerenciado, Otimização.
 - Descrição breve de cada nível
-



Aplicabilidade do CMMI-DEV

- **Definição:** "Focado no desenvolvimento de produtos e serviços."
 - **Exemplo:** Uma empresa de software que busca melhorar seu processo de desenvolvimento de software, visando entrega consistente e de alta qualidade.
-



Aplicabilidade do CMMI-ACQ

- **Definição:** "Centra-se nas práticas de aquisição de produtos e serviços."
 - **Exemplo:** Uma agência governamental que deseja padronizar a maneira como adquire software de terceiros.
-



Aplicabilidade do CMMI-SVC

- **Definição:** "Destinado a provedores de serviços para melhorar seus serviços."
 - **Exemplo:** Uma empresa de hospedagem na web buscando aprimorar a qualidade e consistência de seus serviços.
-




Caso de Uso - Transformação com CMMI

- **História:** "Empresa Z, uma desenvolvedora de software, enfrentava problemas de atrasos e inconsistências em seus lançamentos."
 - **Solução:** Adotou o CMMI-DEV para avaliar e melhorar seus processos de desenvolvimento.
 - **Resultado:** Redução de atrasos em 60% e aumento da satisfação do cliente em 25% no ano seguinte.
-



Benefícios Gerais do CMMI

- **Pontos:**
 - Melhoria contínua dos processos.
 - Maior previsibilidade de custos e prazos.
 - Aumento da satisfação do cliente.
 - Redução de falhas e retrabalhos.
-



SLA nos Negócios de TI (Service Level Agreement)

Pontos:

- O que é SLA.
 - Importância dos indicadores e métricas.
 - Exemplos de acordos de níveis de serviços.
 - **Caso de uso:** "A relação de SLA entre uma empresa de cloud e seus clientes."
-



O que é SLA?

- "Um compromisso entre um provedor de serviço e um cliente, detalhando o nível de serviço esperado."
 - **Elementos:** Descrição do serviço, indicadores de performance, responsabilidades, penalidades, etc.
-



Importância do SLA

- Estabelece expectativas claras entre as partes.
 - Protege ambas as partes em caso de desvios.
 - Fornece um padrão para avaliação de desempenho.
-



Exemplo 1 - Empresa de Hospedagem Web

- **Métrica:** Uptime (Disponibilidade) - 99.9% do tempo.
 - **Aplicabilidade:** Se o site de um cliente fica offline por um tempo maior do que o acordado, a empresa pode ter que oferecer reembolsos ou créditos.
 - **Detalhes:** Outages programados para manutenção não são incluídos na métrica de downtime.
-



Exemplo 2 - Provedor de Cloud

- **Métrica:** Tempo de Resposta - Tickets de suporte devem ser respondidos em até 2 horas.
 - **Aplicabilidade:** Ajuda os clientes a saberem quanto tempo esperar por uma resposta, melhorando a satisfação do cliente.
 - **Detalhes:** Tempo de resposta pode variar dependendo da gravidade do ticket (P1, P2, P3, etc.).
-



Exemplo 3 - Empresa de Telecomunicações

- **Métrica:** Qualidade da Chamada - Taxa de queda de chamadas deve ser menor que 1%.
 - **Aplicabilidade:** Garante que os usuários tenham chamadas de alta qualidade sem quedas frequentes.
 - **Detalhes:** A empresa monitora constantemente a rede para evitar congestionamentos.
-



Adicionando Penalidades ao SLA

- SLAs frequentemente incluem penalidades se os níveis de serviço não são cumpridos.
 - **Exemplo:** Um provedor de serviços de cloud pode oferecer um crédito de 10% na próxima fatura se o uptime cair abaixo do acordado.
-



Benefícios de um SLA bem definido

- Estabelece confiança entre provedor e cliente.
 - Fornece transparência na entrega de serviços.
 - Facilita a resolução de conflitos.
-



Conclusão - SLA

- O SLA é uma ferramenta crucial para definir e manter padrões de serviço em TI.
 - Empresas e clientes devem revisar regularmente os SLAs para garantir que as expectativas sejam atendidas.
-



A Importância da Informática Corporativa e Normas

Pontos:

- Recapitulação dos tópicos abordados.
 - A constante evolução da TI e a necessidade de padrões.
 - **Chamado para ação:** "Vamos implementar e aderir às normas em nossos projetos!"
-

Referências Bibliográficas:

- Laudon, K. C., & Laudon, J. P. (2016). Sistemas de informação gerenciais. São Paulo: Pearson.
- Sommerville, I. (2011). Engenharia de software. São Paulo: Pearson.

Artigos Científicos (Exemplos relacionados à TI):

- Khan, S. N. (2011). A study of the applicability of CMMI in software industries. *Procedia Computer Science*, 3, 1393-1398.
- Mishra, D., & Mishra, A. (2010). Software quality attributes and their inter-relationships: a study. *International Journal of Computer Applications*, 9(11), 11-16.

Periódicos/Revistas de Publicação Científica:

- IEEE Transactions on Software Engineering
- Journal of Systems and Software
- Communications of the ACM

Sites Científicos:

- **Google Scholar (scholar.google.com)**
 - Um motor de busca gratuito que indexa o texto completo ou metadados de trabalhos acadêmicos em várias disciplinas, formatos e idiomas.
- **PubMed (www.ncbi.nlm.nih.gov/pubmed)**
 - Base de dados de pesquisa em ciências da vida e biomedicina, principalmente na área da medicina. Pode não ser especificamente voltado para TI, mas é útil para áreas interdisciplinares.
- **IEEE Xplore (ieeexplore.ieee.org)**
 - Biblioteca digital que fornece acesso a publicações do IEEE (Institute of Electrical and Electronics Engineers), incluindo revistas, conferências e padrões em áreas de eletrônica, engenharia elétrica e ciência da computação.
- **ACM Digital Library (dl.acm.org)**
 - Biblioteca digital que fornece acesso às publicações da ACM (Association for Computing Machinery), incluindo artigos, periódicos, proceedings de conferências e revistas na área de computação.