

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>



Objetivos da Aula:

- Compreender os conceitos fundamentais de confidencialidade, integridade e disponibilidade (CID).
 - Identificar as principais etapas da gestão de riscos em segurança da informação.
-



Introdução à Gestão de Risco

- Definir gestão de risco como o processo de identificar, avaliar e priorizar riscos seguido pela aplicação de recursos para minimizar, monitorar e controlar a probabilidade ou impacto desses riscos.
 - Explicar como a gestão de risco é fundamental para manter a segurança da informação e como ela se encaixa na governança corporativa.
-



Modelos de Padronização:

- Introduzir frameworks e padrões internacionalmente reconhecidos, como ISO 27001 (para sistemas de gestão de segurança da informação) e NIST (Framework de Cibersegurança do Instituto Nacional de Padrões e Tecnologia dos EUA).
 - Esses modelos fornecem uma estrutura para a gestão de risco, ajudando as organizações a identificar os controles necessários para tratar riscos específicos.
-



Casos Reais:

- O ataque ao serviço de DNS da Dyn em 2016, que interrompeu serviços de grandes empresas como Netflix e Twitter (a gestão de risco pode ajudar a se preparar para ataques de DDoS).
 - Examinar o incidente de ransomware WannaCry de 2017, enfatizando a importância de avaliações de risco regulares e atualizações de segurança.
-



Confidencialidade:

- **Explicação:** Refere-se à proteção de informações contra acesso não autorizado.
 - **Exemplos:** Utilização de criptografia para proteger dados durante uma transmissão, uso de senhas fortes, autenticação multifator e controle de acesso baseado em roles.
 - **Modelos de Padronização:** ISO/IEC 27001, que estabelece requisitos para sistemas de gestão de segurança da informação (SGSI), incluindo aspectos de confidencialidade.
 - **Casos Reais:** Vazamento de dados da empresa Target em 2013, onde informações de cartões de crédito de milhões de clientes foram acessadas indevidamente devido a falhas de confidencialidade.
-



Integridade:

- **Explicação:** Garantia de que os dados são confiáveis e não foram alterados de forma não autorizada.
 - **Exemplos:** Uso de hash criptográfico para verificar a integridade de dados transferidos, controle de versão em sistemas de gerenciamento de documentos.
 - **Modelos de Padronização:** Princípios da Gestão de Qualidade da ISO 9001, que podem ser aplicados para assegurar a integridade dos dados.
 - **Casos Reais:** O incidente com a SolarWinds em 2020, onde um software de gestão de redes foi comprometido, permitindo a inserção de código malicioso que afetou a integridade do sistema.
-



Disponibilidade:

- **Explicação:** Assegura que as informações e os sistemas de informação estão acessíveis e utilizáveis quando necessários.
 - **Exemplos:** Implementação de redundância de servidores e balanceamento de carga, estratégias de backup e recuperação de desastres.
 - **Modelos de Padronização:** ITIL (Information Technology Infrastructure Library) para a gestão de serviços de TI, que inclui práticas para manter a disponibilidade dos serviços.
 - **Casos Reais:** O ataque de DDoS (Distributed Denial of Service) ao Dyn em 2016, que tornou inacessíveis grandes sites como Twitter e Netflix, é um exemplo de comprometimento da disponibilidade.
-




Etapas da Gestão de Riscos

- **Identificação de Riscos:** Como identificar ameaças e vulnerabilidades.
 - **Avaliação de Riscos:** Metodologias para avaliar a probabilidade e impacto dos riscos identificados.
 - **Mitigação de Riscos:** Estratégias para reduzir, transferir, aceitar ou evitar riscos.
 - **Monitoramento de Riscos:** Técnicas para monitorar riscos ao longo do tempo e responder a novos riscos.
 - **Revisão e Melhoria Contínua:** Como a gestão de riscos deve ser um processo contínuo e adaptativo.
-




Identificação de Riscos

- **Explicação:** Detalhar como identificar potenciais ameaças e vulnerabilidades que podem afetar os ativos de informação.
 - **Exemplo:** Uso de checklists e análise de histórico de incidentes para identificar riscos comuns em uma organização de TI.
 - **Modelo Padrão:** Referência ao modelo OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) para identificação de riscos.
 - **Caso Real:** Incidente de segurança na empresa Target em 2013, onde a identificação precoce de vulnerabilidades poderia ter prevenido a violação de dados.
-



Avaliação de Riscos

- **Explicação:** Como determinar a probabilidade de ocorrência de cada risco identificado e o impacto potencial que ele pode causar.
 - **Exemplo:** Matriz de risco para classificar cada risco como alto, médio ou baixo, com base em sua probabilidade e impacto.
 - **Modelo Padrão:** ISO/IEC 27005, um padrão internacional para a gestão de riscos de segurança da informação.
 - **Caso Real:** Análise do ataque ransomware WannaCry, destacando a importância de avaliar riscos associados a vulnerabilidades de software.
-



Mitigação de Riscos

- **Explicação:** Estratégias para diminuir a probabilidade de ocorrência ou o impacto de riscos identificados.
 - **Exemplo:** Implementação de firewalls e sistemas de detecção de intrusão para mitigar o risco de ataques cibernéticos.
 - **Modelo Padrão:** Framework NIST para melhorar a cibersegurança em infraestruturas críticas.
 - **Caso Real:** Uso de criptografia end-to-end pelo WhatsApp para mitigar o risco de interceptação de mensagens.
-



Monitoramento de Riscos

- **Explicação:** Monitoramento contínuo e revisão dos riscos, bem como das medidas de controle implementadas.
 - **Exemplo:** Uso de dashboards de segurança para monitoramento em tempo real das atividades da rede.
 - **Modelo Padrão:** Aplicação dos controles do CIS (Center for Internet Security) para uma abordagem de defesa em profundidade.
 - **Caso Real:** O monitoramento contínuo da rede da Sony teria ajudado a detectar atividades suspeitas antes do grande vazamento de dados em 2014.
-



Revisão e Melhoria Contínua

- **Explicação:** A gestão de riscos é um processo cíclico que requer revisão regular para se adaptar a novos riscos e mudanças no ambiente de negócios.
 - **Exemplo:** Análises de pós-incidente para refinar as estratégias de mitigação de riscos.
 - **Modelo Padrão:** PDCA (Plan-Do-Check-Act), uma iteração contínua para melhoria de processos dentro do modelo ISO.
 - **Caso Real:** Como a Adobe reforçou suas políticas e controles de segurança após o ataque de 2013 que comprometeu milhões de contas de usuário.
-



Ferramentas de Gestão de Riscos:

- **Risk Management Software:** Apresente softwares como RSA Archer, LogicManager ou SolarWinds Risk Intelligence, que são projetados para ajudar na identificação, avaliação e monitoramento de riscos.
 - **GRC Platforms (Governance, Risk Management, and Compliance):** Ferramentas como ServiceNow, IBM OpenPages e SAP GRC ajudam a integrar a gestão de riscos com a governança e conformidade regulatória.
-



Ferramentas de Colaboração e Gestão de Projetos:

- **JIRA:** Uma ferramenta que pode ser usada para rastrear o progresso do gerenciamento de riscos e a implementação de controles.
 - **Trello ou Asana:** Ferramentas visuais de gestão de projetos que podem ser úteis para organizar as tarefas relacionadas à gestão de riscos e acompanhar o progresso.
 - **Microsoft Teams ou Slack:** Plataformas de comunicação que permitem a colaboração em tempo real, discussão de riscos e compartilhamento de documentos.
-



Metodologias de Avaliação e Gestão de Riscos:

- **ISO 31000:** Esta é uma norma internacional que fornece diretrizes sobre a implementação de gestão de riscos. Mostre como os princípios, a estrutura e o processo descritos na ISO 31000 podem ser aplicados.
 - **NIST Cybersecurity Framework:** Um framework que ajuda as organizações a gerenciar e mitigar riscos cibernéticos de maneira estruturada e sistemática.
 - **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation):** Uma metodologia que se concentra na avaliação de riscos organizacionais e de tecnologia da informação.
-



Ferramentas de Análise e Avaliação de Riscos:

- **Qualys ou Nessus:** Ferramentas para análise de vulnerabilidades que podem ajudar a identificar e priorizar riscos em sistemas de TI.
 - **Tableau ou Power BI:** Ferramentas de visualização de dados que permitem a criação de dashboards interativos para acompanhar métricas de riscos e a eficácia dos controles.
-



Técnicas de Priorização e Decisão:

- **Matriz de Risco:** Uma ferramenta que permite visualizar e priorizar riscos com base em sua probabilidade e impacto.
 - **Análise SWOT (Strengths, Weaknesses, Opportunities, Threats):** Uma técnica que pode ser usada para avaliar o ambiente interno e externo na gestão de riscos.
-

Implementando um modelo

Implementação de Ferramentas:

- **Gestão de Projetos e Tarefas:** Adotar o JIRA para gerenciar projetos de TI e o Trello para tarefas do dia a dia.
- **Colaboração:** Usar o Microsoft Teams para comunicação interna e o Git para controle de versão e colaboração em código.
- **Monitoramento de Rede e Sistemas:** Implementar o Zabbix ou o Nagios para monitoramento contínuo da infraestrutura de TI.
- **Análise de Vulnerabilidade:** Integrar ferramentas como Qualys ou Nessus para realizar varreduras regulares de vulnerabilidades.

Utilização de Padrões:

- **Segurança da Informação:** Adotar a norma ISO/IEC 27001 para estabelecer um sistema de gestão de segurança da informação (SGSI).
- **Gestão de Riscos:** Seguir a ISO 31000 para as práticas de gestão de riscos.
- **Qualidade de Software:** Implementar padrões como o ISO/IEC 25010 para garantir a qualidade de software.

Utilização de Boas Práticas:

- **ITIL para Gestão de Serviços de TI:** Implementar as práticas do ITIL para a gestão de serviços de TI, focando em estratégia de serviço, desenho de serviço, transição de serviço, operação de serviço e melhoria contínua do serviço.
- **Práticas de Segurança da Informação:** Estabelecer políticas de senha forte, treinamento regular de conscientização em segurança para todos os funcionários e uso de autenticação multifator (MFA).
- **Desenvolvimento de Software:** Adotar a metodologia ágil para o desenvolvimento de software e práticas de DevOps para integração e entrega contínuas.

Utilização de Mecanismos:

- **Controle de Acesso:** Implementar o controle de acesso baseado em funções (RBAC) para garantir que os usuários tenham apenas os privilégios necessários.
- **Criptografia:** Usar criptografia tanto em repouso quanto em trânsito para proteger dados sensíveis.
- **Backup e Recuperação de Desastres:** Estabelecer políticas de backup regulares e planos de recuperação de desastres.



Implementação Passo a Passo:



Avaliação Inicial e Planejamento:

- Realizar um levantamento das necessidades atuais do departamento de TI e infraestrutura.
- Definir objetivos claros e metas para a padronização e organização.
- Criar um roadmap para a implementação das ferramentas e práticas.

Configuração e Customização de Ferramentas:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.

- Instalar e configurar as ferramentas escolhidas.
- Personalizar as ferramentas de acordo com as necessidades específicas da empresa.

Desenvolvimento de Políticas e Procedimentos:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.

- Redigir políticas e procedimentos baseados nos padrões e melhores práticas selecionados.
- Realizar treinamentos com a equipe para garantir o entendimento e a aderência às políticas.

Implementação e Execução:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.

- Implementar os mecanismos de controle e segurança.
- Iniciar o uso das ferramentas de gestão de projetos e tarefas, e monitoramento.

Monitoramento e Ajustes:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.

- Monitorar a eficácia das ferramentas e práticas implementadas.
- Fazer ajustes conforme necessário para melhorar a eficiência e segurança.

Revisão e Melhoria Contínua:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.

- Revisar periodicamente as práticas e procedimentos adotados.
- Implementar um ciclo de feedback para melhoria contínua.