

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>

Princípios da Segurança e o Ciclo de Vida da Informação.

Objetivos da aula

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

- Entendimento dos fundamentos da Segurança da Informação.
- Conhecimento sobre os princípios básicos de segurança.
- Diferenciar segurança física, lógica e controle de acesso.

Definição de Segurança da Informação

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

- Proteção contra acessos não autorizados, uso indevido, divulgação, destruição, modificação ou interrupção.

Definição Básica:

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


- A Segurança da Informação refere-se à proteção de dados e informações contra acesso não autorizado, uso indevido, divulgação, destruição, modificação ou interrupção.

Elementos-chave:

- **Dados e Informações:** Trata-se não apenas de dados em trânsito ou armazenados, mas também de informações processadas e compartilhadas.
- **Proteção:** Implementação de medidas preventivas, corretivas e reativas.
- **Ameaças:** Elementos que podem causar danos, como hackers, malware, falhas humanas, desastres naturais, entre outros.

Objetivo Principal:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar on the right side.

- Garantir que os dados estejam disponíveis para quem deve acessá-los (disponibilidade), protegidos de acesso não autorizado (confidencialidade) e imunes a alterações não autorizadas (integridade).
- 
- A thin gray horizontal bar is located at the bottom of the slide.

Ciclo de Vida da Informação

- Criação
- Armazenamento
- Uso
- Compartilhamento
- Arquivamento
- Destruição

Etapas do Ciclo:

- **Criação:** A fase inicial onde a informação é gerada. Pode ser o resultado de uma nova entrada de dados, como a criação de um novo registro em um banco de dados ou a composição de um e-mail.

Etapas do Ciclo:

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

- **Armazenamento:** Uma vez criada, a informação é armazenada para uso futuro. Pode ser em dispositivos físicos, como servidores ou na nuvem.

Etapas do Ciclo:

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

- **Uso:** A informação é acessada, lida, atualizada, processada ou de outra forma utilizada.

Etapas do Ciclo:

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

- **Compartilhamento:** A informação é distribuída ou transmitida para outros usuários, sistemas ou organizações. Isso pode ser feito por e-mail, transferência de arquivos, entre outros.

Etapas do Ciclo:

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

- **Arquivamento:** A informação é armazenada a longo prazo, frequentemente em um formato mais estável e menos acessível, para preservação e referência futura.

Etapas do Ciclo:

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

- **Destruição:** Quando a informação não é mais relevante ou necessária, ela é eliminada. A destruição pode ser física (como destruir um disco rígido) ou digital (como deletar um arquivo).

Vulnerabilidades em cada etapa

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

- Discussão sobre como em cada etapa a informação é vulnerável a diferentes tipos de ameaças.

1. Criação:

- **Vulnerabilidade:** Inserção de malwares ou códigos maliciosos durante a geração de dados.
- **Exemplo:** Documentos contaminados ao serem criados em ambientes comprometidos.

2. Armazenamento:

- **Vulnerabilidade:** Falhas na criptografia, ataques de força bruta a senhas e perda física de dispositivos de armazenamento.
- **Exemplo:** HDs externos perdidos ou roubados, ataques a bancos de dados não protegidos.

3. Uso:

- **Vulnerabilidade:** Phishing, engenharia social e malwares que capturam informações durante o uso.
- **Exemplo:** Funcionário sendo enganado por e-mails de phishing e fornecendo informações confidenciais.

4. Compartilhamento:

- **Vulnerabilidade:** Transmissão insegura, compartilhamento excessivo e plataformas de compartilhamento vulneráveis.
- **Exemplo:** Dados enviados por e-mail sem criptografia, acesso concedido a muitos usuários sem necessidade.

5. Arquivamento:

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

- **Vulnerabilidade:** Falta de procedimentos de retenção de dados, sistemas de arquivamento desatualizados e falta de revisão de dados.
- **Exemplo:** Dados sensíveis armazenados além do necessário, tornando-se alvos potenciais.

6. Destruição:

- **Vulnerabilidade:** Destruição incompleta ou inadequada, dispositivos descartados sem a devida limpeza.
- **Exemplo:** Papéis com informações sensíveis não sendo completamente destruídos ou HDs vendidos sem uma limpeza adequada.

Princípios Básicos da Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Não-repúdio

Confidencialidade:

- **Definição:** Garantir que a informação é acessível apenas por aqueles autorizados a ter acesso.
- **Exemplo:** Criptografia de dados, controles de acesso baseados em identidades e autenticação.

Integridade:

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

- **Definição:** Assegurar que a informação é protegida contra alterações não autorizadas e que está correta e completa.
- **Exemplo:** Assinaturas digitais, checksums e controles de versão.

Disponibilidade:

- **Definição:** Garantir que a informação e os recursos associados estejam disponíveis quando necessário.
- **Exemplo:** Redundância de sistemas, backups regulares e balanceamento de carga.

Autenticidade:

- **Definição:** Garantir que a informação é proveniente de uma fonte confiável e legítima.
- **Exemplo:** Certificados digitais e sistemas de autenticação multifatorial.

Não-repúdio:

- **Definição:** Garantir que a origem da informação ou transação não possa negar sua autoria ou envio.
- **Exemplo:** Assinaturas digitais e registros de auditoria detalhados.

Segurança Física

- **Definição e exemplos:** trancas, câmeras, alarmes, guardas de segurança, controle de acesso por cartões magnéticos.

Definição:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar on the right side.

- A Segurança Física refere-se à proteção dos ativos tangíveis de uma organização e ao ambiente em que esses ativos estão localizados contra ameaças físicas.

Importância:

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

- Evitar acesso não autorizado a locais restritos.
- Proteger contra desastres naturais e calamidades.
- Prevenir perda ou dano de equipamentos críticos.
- Garantir a continuidade das operações.

Componentes Principais:

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

- **Controle de Acesso Físico:** Portões, portas trancadas, cartões de acesso e sistemas biométricos.

Componentes Principais:

A thick yellow horizontal bar spanning the width of the slide, with a vertical yellow bar on the right side.

- **Monitoramento:** Câmeras de vigilância, patrulhas de segurança e sensores de movimento.

Componentes Principais:

A thick yellow horizontal bar spanning the width of the slide, with a vertical yellow bar on the right side.

- **Proteção contra desastres:** Sprinklers, detectores de fumaça, planos de evacuação e zonas seguras.

Componentes Principais:

A thick yellow horizontal bar spanning the width of the slide, with a vertical yellow bar on the right side.

- **Energia:** Geradores de backup, UPS (fontes de alimentação ininterruptas) e proteção contra surtos elétricos.

Componentes Principais:

A thick yellow horizontal bar spanning the width of the slide, with a vertical yellow bar on the right side.

- **Ambiente:** Climatização adequada e controle de umidade para salas de servidores e data centers.

Desafios:

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

- Equilibrar acessibilidade e segurança.
- Atualizar regularmente as infraestruturas de segurança.
- Treinar pessoal para situações de emergência.

Segurança Lógica

- **Definição e exemplos:** firewalls, antivírus, sistemas de detecção de intrusão, criptografia, VPNs.

Definição:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar on the right side.

- Enquanto a segurança física se preocupa com proteções tangíveis e o ambiente, a segurança lógica foca na proteção de recursos digitais, como sistemas, redes e dados.

Software de Segurança:

- **Firewalls:** Barreiras que monitoram e controlam o tráfego de rede com base em regras de segurança predeterminadas.
- **Antivírus:** Programas projetados para detectar, evitar e remover software malicioso (malware) dos sistemas.
- **Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS):** Monitoram redes e sistemas em busca de atividades maliciosas ou violações de políticas.

Criptografia:

- Processo de converter informações de um formato legível para um formato codificado, para proteger sua confidencialidade.
- **Tipos:** Criptografia simétrica, Criptografia assimétrica.
- Uso comum em transações online, comunicações seguras e armazenamento de dados sensíveis.

Controle de Acesso Lógico:

- Mecanismos para garantir que apenas usuários autorizados possam acessar recursos digitais.
- Inclui autenticação (verificar a identidade do usuário) e autorização (determinar quais recursos o usuário pode acessar).

Virtual Private Networks (VPNs):

- Redes que criam um canal seguro de comunicação sobre uma rede pública, geralmente a Internet.
- Usado para garantir privacidade e segurança ao se comunicar através de redes não confiáveis.

Controle de Acesso

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

- O que é e por que é importante.

Definição:

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

- Controle de acesso refere-se ao mecanismo pelo qual sistemas determinam quem pode acessar recursos específicos e o que eles podem fazer com eles.

Importância do Controle de Acesso:

- Protege informações confidenciais de acesso não autorizado.
- Garante a integridade e disponibilidade dos dados.
- Regula quem pode realizar quais operações (por exemplo, ler, escrever, executar).

Tipos de Acesso:

- **Autenticação:** Processo de verificar a identidade de um usuário, sistema ou aplicação.
- **Autorização:** Determina quais recursos o usuário, sistema ou aplicativo pode acessar e o que pode fazer com eles.
- **Auditoria (ou accounting):** Rastreia e registra atividades do usuário para posterior revisão.

Modelos de Controle de Acesso:

- **Discrecional (DAC):** O proprietário da informação determina quem pode acessá-la.
- **Mandatory (MAC):** Acessos são baseados em políticas definidas centralmente, não pelo proprietário do recurso.
- **Baseado em Funções (RBAC):** Acesso é dado com base nas funções de um usuário dentro de uma organização.

Modelos de Controle de Acesso

- **Descrição e diferenças entre:**
 - Discrecional (DAC)
 - Mandatory (MAC)
 - Baseado em Funções (RBAC)

Definição:

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar on the right side.

- O controle de acesso refere-se à prática de permitir ou negar o acesso a um recurso com base nas credenciais de um usuário ou sistema. O modelo de controle de acesso define como essas decisões são tomadas e como os direitos ou privilégios são distribuídos.

1. Discrecional (DAC - Discretionary Access Control):

- **Descrição:** No DAC, o proprietário de uma informação determina quem pode acessá-la. O proprietário tem total discricionariedade sobre como os acessos são concedidos.
- **Características Principais:**
 - **Baseado em permissões:** Ler, Escrever, Executar.
 - Os proprietários podem conceder ou revogar permissões.
 - **Exemplo:** Em sistemas de arquivos, um usuário que cria um arquivo pode decidir quem pode ler, escrever ou executar esse arquivo.

2. Mandatory (MAC - Mandatory Access Control):

- **Descrição:** Os acessos são determinados por políticas definidas centralmente, não pelo proprietário individual do recurso. É geralmente baseado em rótulos de segurança.
- **Características Principais:**
 - Usa etiquetas/classificações (por exemplo, "Top Secret", "Confidential").
 - Decisões de acesso são feitas com base na comparação dos rótulos com as credenciais do usuário.
 - **Exemplo:** Em ambientes governamentais ou militares, documentos classificados como "Top Secret" só podem ser acessados por indivíduos com a devida autorização.

3. Baseado em Funções (RBAC - Role-Based Access Control):

- **Descrição:** O acesso é concedido com base nas funções (ou cargos) que os usuários têm dentro de uma organização, e não suas identidades individuais.
- **Características Principais:**
 - Usuários são associados a funções.
 - Funções são associadas a permissões.
 - Flexível e escalável para grandes organizações.
 - **Exemplo:** Em um hospital, médicos podem ter acesso a registros médicos completos, enquanto recepcionistas podem apenas acessar informações de contato do paciente.

Atividade Prática

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

- Instruções para o debate em grupo.
- Diretrizes para o estudo de caso.

Artigos Científicos:

- Anderson, R. (2008). Security engineering: a guide to building dependable distributed systems (2nd ed.). Wiley.
- Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

Periódicos:

- Journal of Computer Security - IOS Press.
- International Journal of Information Management - Elsevier.
- Computers & Security - Elsevier.

Revistas de Publicações Científicas:

- IEEE Security & Privacy - Uma publicação do IEEE dedicada a questões de privacidade e segurança em computação e tecnologia.
- ACM Transactions on Information and System Security (TISSEC) - Publicações da ACM focadas em pesquisa de segurança.
- Information Systems Security Association (ISSA) Journal - Aborda práticas, ferramentas e técnicas atuais de segurança da informação.

Sites:

- OWASP (Open Web Application Security Project): <https://www.owasp.org/> - Uma comunidade aberta dedicada a permitir que organizações desenvolvam, adquiram e mantenham aplicações/trusted softwares.
- SANS Institute: <https://www.sans.org/> - Oferece treinamento em segurança cibernética e certificações, e seu site tem uma ampla variedade de recursos educacionais em segurança da informação.
- CERT: <https://www.cert.org/> - O Centro de Resposta a Emergências de Computadores da Software Engineering Institute, que oferece recursos de pesquisa em segurança cibernética.
- Cybersecurity & Infrastructure Security Agency (CISA): <https://www.cisa.gov/> - Agência governamental dos EUA que fornece uma variedade de recursos e atualizações sobre ameaças e vulnerabilidades de segurança.