Prof. esp. Thalles Canela

- **Graduado:** Sistemas de Informação Wyden Facimp
- Pós-graduado: Segurança em redes de computadores Wyden Facimp
- Professor (contratado):
- Pós-graduação: Segurança em redes de computadores Wyden Facimp
- Professor (Efetivado):
- Graduação: Todo núcleo de T.I. Wyden Facimp
- Tech Lead na 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



Senhas

- Complexidade: Crie senhas fortes e complexas, combinando letras maiúsculas e minúsculas, números e caracteres especiais. Evite informações pessoais óbvias, como nomes, datas de nascimento ou palavras comuns.
- **Comprimento:** Use senhas com pelo menos 8 caracteres. Quanto maior, melhor.
- **Diversidade:** Utilize senhas diferentes para cada conta. Evite reutilizar senhas em várias plataformas.

Senhas

- Alteração regular: Mude suas senhas periodicamente, pelo menos a cada 3 meses, para manter a segurança.
- Autenticação de dois fatores: Ative a autenticação de dois fatores sempre que possível. Isso adiciona uma camada extra de segurança exigindo um código adicional para fazer login.
- Gerenciador de senhas: Considere utilizar um gerenciador de senhas confiável para armazenar e gerar senhas seguras. Isso ajuda a lembrar de senhas complexas sem reutilizá-las.

Treinamento

- Conscientização: Realize treinamentos de conscientização de segurança regularmente para educar os funcionários sobre ameaças cibernéticas, phishing, engenharia social e melhores práticas de segurança.
- **Políticas de senha:** Implemente políticas claras de senha em sua organização, destacando a importância de senhas seguras e práticas recomendadas.
- Atualizações de segurança: Mantenha os sistemas e dispositivos atualizados com as últimas correções de segurança. Certifique-se de que todos os funcionários estejam cientes da importância das atualizações regulares.

Treinamento

Proteção de dispositivos móveis:
 Eduque os funcionários sobre a importância de proteger seus dispositivos móveis com senhas ou biometria e evitar o acesso não autorizado.



Proteção de informações

- Acesso mínimo necessário: Conceda acesso apenas às informações necessárias para cada funcionário. Limite o acesso administrativo apenas a pessoas autorizadas.
- **Criptografia:** Utilize criptografia em arquivos sensíveis, bancos de dados e comunicações online para proteger as informações confidenciais contra acesso não autorizado.
- Backup regular: Faça backup regularmente de todos os dados importantes para garantir que, em caso de perda ou violação, você possa recuperar as informações.



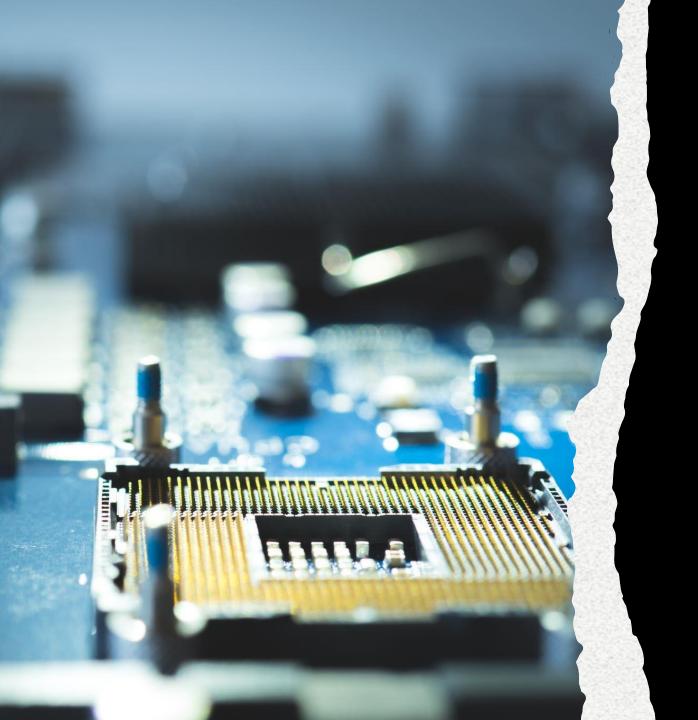
Proteção de informações

- **Restrição física:** Proteja fisicamente os equipamentos e documentos confidenciais. Mantenha-os em locais seguros e restritos, limitando o acesso apenas a pessoal autorizado.
- Monitoramento: Implemente sistemas de monitoramento de segurança para identificar atividades suspeitas e responder rapidamente a ameaças em potencial.
- Políticas de uso aceitável: Estabeleça políticas claras de uso aceitável para os funcionários, definindo o comportamento adequado em relação ao uso de informações e sistemas corporativos.



Proteção de informações

• Conformidade com regulamentos:
Garanta que sua organização
esteja em conformidade com as
regulamentações de segurança de
dados relevantes, como o GDPR
(Regulamento Geral de Proteção
de Dados) ou a LGPD (Lei Geral de
Proteção de Dados).



Trabalho em grupo.

- Objetivo:
- 1. Montagem de documentação para treinamento;
- 2. Montagem de documentação para script;
- 3. Teste do Script;
- O que fazer:
- Elabora um script para geração de senhas com base em dados cadastrais;
- Garantir que o script funcione no Windows e no Linux;