Prof. Esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp

- **Consultor de Tecnologia - [aXR6] Cyber Security e NtecSoftware**
- **Professor no Senac (contratado)**
- **Professor na Wyden Facimp (contratado)**
  - **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor na Wyden Facimp (Efetivado)**
  - **Graduação:** Análise e desenvolvimento de sistemas - Wyden Facimp

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

9 motivos para investir na proteção de dados

- A proteção surge do controle eficiente em uma gestão bem-feita dos ativos tecnológicos existentes sob os cuidados da sua empresa.

Proteção de informações sigilosas da organização

- A situação financeira da empresa;
- Lista de clientes e informações de preços;
- Planejamento estratégico;
- Códigos de tecnologias;
- Planos de marketing;
- Pesquisas em inovações;
- Informações confidenciais de parceiros e/ou fornecedores.

Prevenção contra o vazamento de dados dos clientes - EXEMPLO

- Se a sua empresa conta com um extenso cadastro de clientes no banco de dados da organização é preciso garantir que todos esses dados estejam protegidos, evitando o vazamento das informações dos seus clientes e deixando a empresa em conformidade com a LGPD.

Prevenção contra o vazamento de dados dos clientes – CASO REAL

- Recentemente, o banco PAN confirmou que houve vazamento de dados dos seus clientes. Segundo a instituição financeira, dados cadastrais, de limite e saldo devedor tiveram cópias não autorizadas feitas.
- A empresa não divulgou quantos clientes foram expostos, mas a instituição já conta com 17 milhões de clientes ativos. Não é pouca coisa, né?

O que é LGPD?

- A lei nº 13.709/18 é a norma que regulamenta o tratamento de dados pessoais coletados ou compartilhados, inclusive por meios digitais. A LGPD conta com 65 artigos e alterou os artigos 7º e 16º do Marco Civil da internet.
- **LGPD significado:** Lei Geral de Proteção de Dados

Para que serve LGPD?

- O objetivo da LGPD é garantir às pessoas, de uma forma geral, e aos usuários da internet, de forma particular, a proteção de seus dados, compartilhados ou coletados por pessoa física ou jurídica. Assim, a lei nº 13.709/18 busca resguardar os direitos fundamentais de privacidade e de liberdade bem como o livre desenvolvimento da pessoa natural.

Prevenção contra o sequestro de dados

- O sequestro de dados, também conhecido como ataque *ransomware*, é um crime cibernético comum no meio corporativo e visa o recebimento de resgate em dinheiro.

O que é um ransomware?

- O ransomware é um malware que tem como principal função criptografar ou impedir o acesso a uma grande quantidade de arquivos de um computador, sistema de dados ou até mesmo de uma rede inteira.

Capacitação da sua equipe de TI em cibersegurança

- Quando uma empresa não investe em segurança cibernética, cai sobre os profissionais de TI o dever de **gerenciar e monitorar manualmente cada detalhe da cibersegurança**.
- O processo manual, além de cansativo, tem riscos de gerar erros humanos, que podem ser difíceis de se identificar.
- Capacitar sua equipe para que a realizem os processos de maneira automatizada pode ser uma boa opção.

Garantia do exercício das atividades

- Além dos prejuízos indiretos que podem surgir como consequência do comprometimento de dados, um dos maiores riscos para uma empresa ao não investir em cibersegurança é **ter o exercício de suas atividades parcial ou totalmente proibidas**.
- Essa é uma das sanções que uma empresa pode sofrer ao estar em desconformidade com a Lei Geral de Proteção de Dados (Capítulo VIII, Artigo 52, parágrafo XII).
- Além disso, também podem ser aplicadas **punições no âmbito administrativo e admoestativo**, sem contar as restrições de atividade.

Identificação de vulnerabilidades

- Mesmo com grandes investimentos em proteção de dados, é impossível garantir um sistema 100% blindado.
- Porém, o sucesso da sua empresa está na capacidade de reagir quando uma vulnerabilidade é identificada, ou seja, uma boa **gestão de vulnerabilidades.**
- Um sistema bem protegido e com processos de monitoramento e gerenciamento bem definidos garantem alertas imediatos quando há uma brecha de segurança que possa causar problemas em dados importantes para o negócio.

Preservação da imagem e da reputação da marca

- Os dados da empresa, que são em sua maioria sigilosos, como relatórios financeiros e segredos da sua produção;
- As informações confidenciais dos clientes, como dados pessoais e sensíveis, senhas, endereços, CPF, etc.
- O impacto de um vazamento exigirá da sua empresa um grande investimento em marketing e relações-públicas para reverter uma imagem negativa.
- Isso sem contar nos **custos para reparar os prejuízos dos ataques** que, segundo o último levantamento da IBM, chega a cerca de 4,24 milhões de dólares gastos por empresas brasileiras.

Combate de ameaças internas

- A ausência de uma **política de proteção de dados** influencia em problemas internos, como envio incorreto de e-mails, falta de critérios no uso de senhas dos usuários, compartilhamento de documentos com pessoas não autorizadas, entre outros.
- Esses são fatores que podem contribuir tanto para a perda de dados existentes sob os cuidados da sua empresa quanto para o seu relacionamento com os clientes.

Adequação à LGPD

- Outro ponto que não pode ser esquecido é a Lei Geral de Proteção de Dados, que estabelece **diretrizes obrigatórias no cuidado com a coleta, uso e armazenamento de dados** dos seus clientes e usuários.
- Apesar de já estar em vigor há quase dois anos, muitas empresas ainda não estão em conformidade com a lei e continuam **sofrendo com punições** em decorrência do mau uso dessas informações.
- A LGPD foi sancionada com o objetivo de **aumentar a segurança e privacidade das pessoas no que diz respeito aos seus dados pessoais e sensíveis**, evitando que ocorram cenários de perda, vazamento e compartilhamento não autorizado dessas informações.

Por que é importante tomar cuidado com a segurança na nuvem?

??????????????????

Quais são as principais vulnerabilidades presentes em estruturas na nuvem?

- 1. Violação de dados
- 2. Configurações incorretas
- 3. Falta de arquitetura e estratégia de segurança
- 4. Credenciais insuficientes
- 5. Sequestro e invasão de contas
- 6. Ameaças internas
- 7. Interfaces e APIs inseguras

Como aumentar a proteção de dados na nuvem?

Visibilidade

- para moderar os riscos, aumentar a conformidade, e fortalecer o gerenciamento de dados, alcance um alto nível de visibilidade;

Cuidado Cibernético

- execute testes e treinamentos, faça a atualização e correção dos seus dispositivos e reforce bem as defesas já existentes;

Estrutura

- Instale uma estrutura de confiança para amadurecer seus processos de segurança;

Plataforma

- para realizar o gerenciamento de múltiplas soluções de segurança, empregue uma abordagem de plataforma integrada.