IMPLEMENTANDO SEGURANÇA INTEGRAL: A JORNADA DEVSTREAM

- Fundamentos de Segurança, Continuidade de Negócios e Estratégias DevSecOps

- Nome dos Participantes:
- Davi Mateus Gaio – 1581196
- Gabrielle Almeida – 879347
- Guilherme Augusto Andrade da Silva Borges – 894766
- Luiz Otávio da Silva Pereira – 883502
- Nicolas Miller – 806349
- Roberto Semantob Junior – 890262

CARACTERIZAÇÃO DA EMPRESA - DEVSTREAM: O NEGÓCIO E A MISSÃO

- A DevStream é uma força distintiva no setor de tecnologia, oferecendo uma plataforma unificada que abrange o ciclo de vida do DevOps.
- Missão: Simplificar e otimizar os processos para equipes de DevSecOps, promovendo colaboração eficiente.
- Proposta de valor: Unificação de funcionalidades como controle de versão, CI/CD, análise de vulnerabilidades e métricas.
- Modelo de negócios: Open Core com versão gratuita e recursos empresariais pagos.
- Missão corporativa: Fomentar contribuição global com código, produto e empresa.

CARACTERIZAÇÃO DA EMPRESA - DEVSTREAM: VALORES E ESTRATÉGIA

- Valores (CREDIT): Colaboração, Resultados, Eficiência, Diversidade, Iteração e Transparência.
- Estratégia: Aceleradora da transformação cultural em software com foco em segurança (Shift Left).
- Tendências: DevSecOps, IA/ML, nuvem híbrida e experiência do desenvolvedor.
- Vantagem: Plataforma única, Open Source + Enterprise, transparência radical.

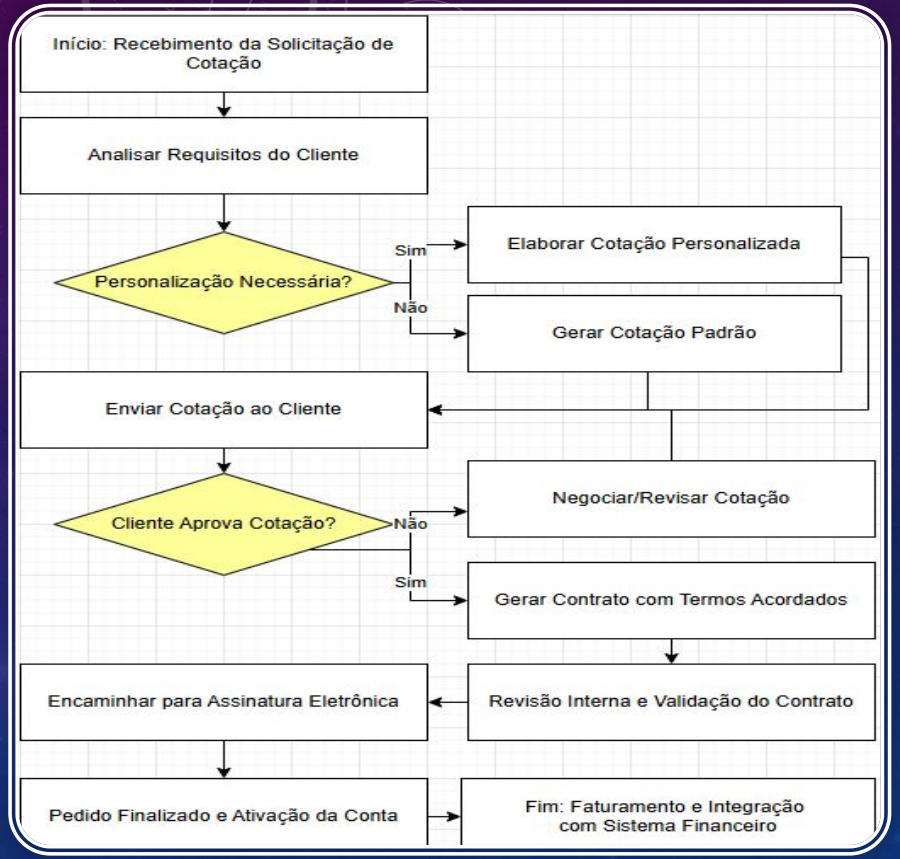
CENÁRIO DE SEGURANÇA - AMEAÇAS E CONCORRÊNCIA

- Concorrência: GitHub, Atlassian, AWS/Azure/GCP, Snyk, SonarQube.
- Desafios: Competição com gigantes, escalabilidade e migração de sistemas legados.

CENÁRIO DE SEGURANÇA - RISCOS INTERNOS E LEGAIS

- Shadow IT e BYOD: Uso de dispositivos e apps não oficiais expõe dados e sistemas.
- Legislação: LGPD, Marco Civil, Lei de Crimes Cibernéticos, Lei do Software, Teletrabalho.

PROCESSOS CRÍTICOS: PEDIDOS, COTAÇÕES E CONTRATOS



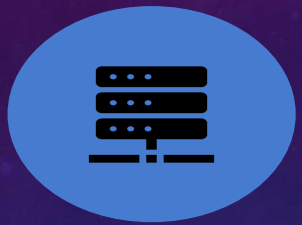
SHADOW IT E BYOD: A SEGURANÇA FORA DO RADAR

- Ex.: Zapier Free, Dropbox pessoal, planilhas locais

- Riscos: Vazamentos, fraude, falhas de compliance

- Dispositivos: notebooks e iPads pessoais, roteadores desatualizados

RISCOS DE SEGURANÇA FÍSICA E LÓGICA ENCONTRADOS NO CONTEXTO ORGANIZACIONAL ESTUDADO.



• APIS, E-SIGNATURE, ROTEADORES, REPOSITÓRIOS = RISCOS ALTOS

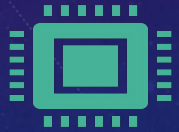
• MEDIDAS: MFA, CRIPTOGRAFIA, VPN, PLATAFORMAS HOMOLOGADAS

• BASEADO NA NORMA ISO 27001 COM FOCO EM REDUÇÃO DE IMPACTO

CULTURA DE SEGURANÇA: CONSCIENTIZAÇÃO CONTÍNUA

- Programa mensal de segurança: phishing, engenharia social

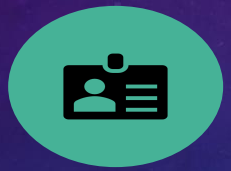
- Simulações realistas: e-mails falsos, alertas



- Treinamentos obrigatórios e por função (Dev, TI, Liderança)

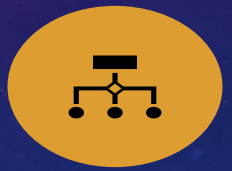
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

• ACESSO: SSO + RBAC, AUDITORIAS TRIMESTRAIS



• AUTENTICAÇÃO: MFA OBRIGATÓRIO, CERTIFICADOS DIGITAIS

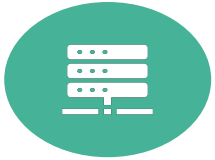
• REDES E DEV: VPN, SAST, DAST, SCANNING CONTÍNUO



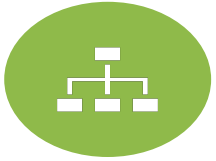
• INCIDENTES: SIRT, PLAYBOOKS, CONFORMIDADE ISO/LGPD

SOLUÇÕES SEGURAS - CONTROLES E GERENCIAMENTO DE RISCOS

IAM: SSO, RBAC, MFA e controle de privilégios.



Rede: Segmentação, VPN, Firewalls, DDoS, SIEM, IDS/IPS.



DevSecOps: SAST, DAST, Secret Detection, gestão de dependências.

BC/DR: Redundância, backups, simulações de desastre.

CONTINUIDADE DE NEGÓCIOS: PREPARAÇÃO PARA O INESPERADO

- Sistema de Gestão de Continuidade de Negócios (SGCN)

- Classificação de ativos: críticos x não críticos

- Projeto prático: Script C# para inventário de hardware/software

INVESTIMENTOS EM SEGURANÇA E INFRAESTRUTURA

- • CAPEX: Laptops, periféricos (R$850.000)
- • OPEX: AWS, segurança, backups, treinamentos (R$752.000/ano)
- • Justificativa: performance, proteção, continuidade

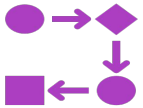
CONSOLIDAÇÃO - APRENDIZADOS E IMPACTO DO PROJETO

Compreensão aprofundada das vulnerabilidades reais em ambientes corporativos modernos.Aplicação prática da norma ISO 27001 em avaliações e tratamento de riscos.Vivência de um ciclo completo de segurança: da fundamentação até a continuidade de negócios.Integração entre conhecimento técnico (ex.: C#, AWS) e governança (ex.: políticas, compliance).

- Impacto GeradoCultura de segurança fortalecida na empresa fictícia DevStream.Criação de um plano viável de continuidade de negócios, com base em recursos e riscos reais.Estruturação de uma política de segurança sólida, adaptada a ambientes remotos.Consciência sobre a importância da educação contínua em segurança (treinamentos e simulações).

CONSOLIDAÇÃO - INOVAÇÃO E RESILIÊNCIA

Gestão de riscos contínua e conformidade legal.



Cultura de transparência e iteração contínua.

Aplicação prática da segurança com MFA, criptografia, SIEM, inventário de ativos via C#.