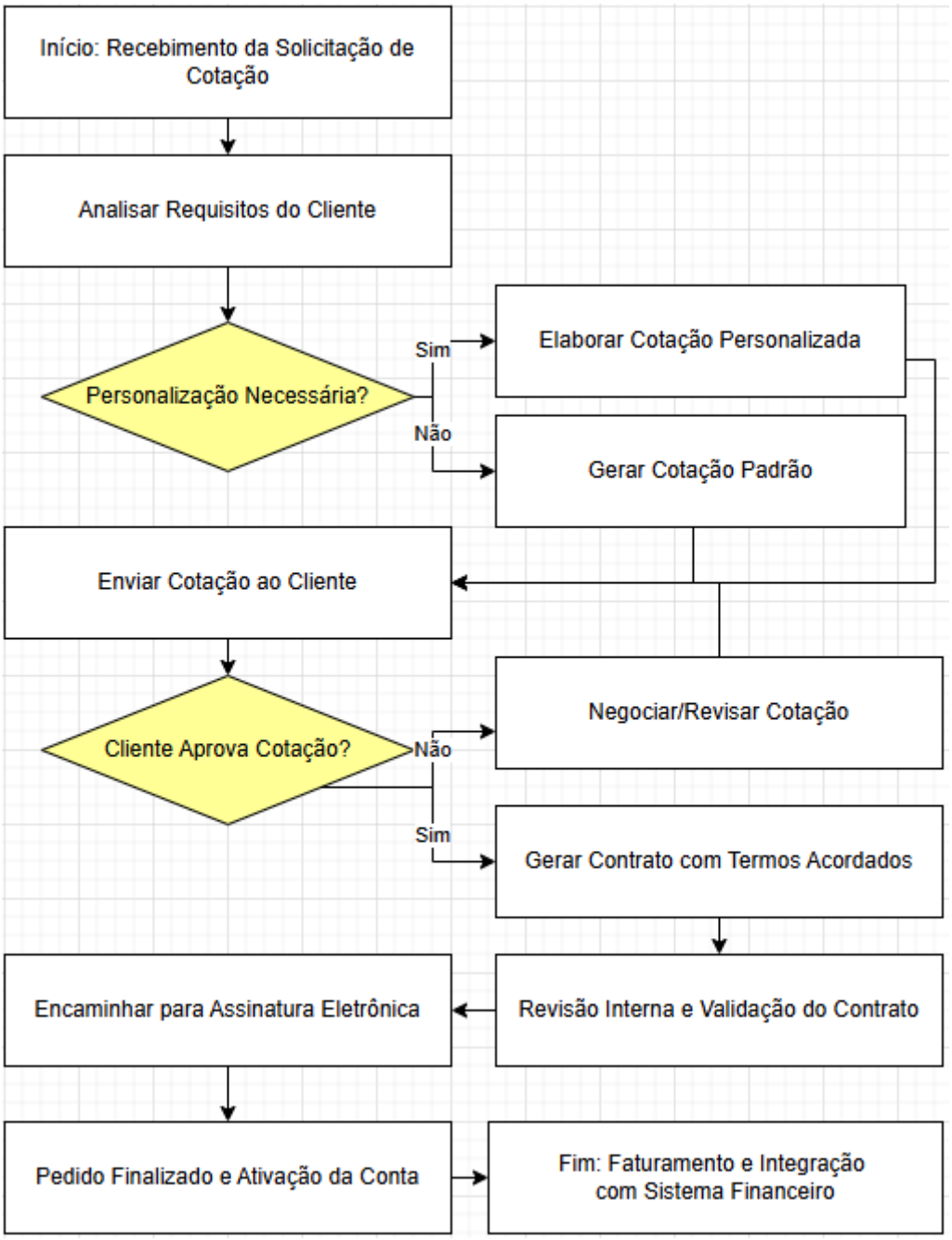
DevStream

Processamento de Pedidos, Cotações e Contratos



2. Componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido.

Processamento de Pedidos, Cotações e Contratos

1. Sistemas de CRM (Customer Relationship Management)
2. Plataformas de e-signature
3. APIs de Integração Financeira
4. Repositórios de Documentos
5. Dispositivos Remotos (laptops, USBs)
6. Ferramentas de Comunicação (e-mails, mensagens)
7. Sistemas de ERP (Enterprise Resource Planning)
8. Redes Domésticas de Funcionários
9. Armazenamento em Nuvem
10. Sistemas de Autenticação
11. Funcionários maliciosos.

3. Itens relacionados à TI invisível na organização.

Setor	Item de TI não catalogado	Proprietário	Usuários	Risco	Obs.
Desenvolvimento	Conta pessoal na DevsTream	Desenvolvedor sênior	Equipe de desenvolvimento	Vazamento de código proprietário; controle de versão fora do ambiente seguro.	Utilizada para testar projetos paralelos e comparativos de performance.
Suporte Técnico	Aplicativo de chat não oficial	Analista de suporte	Suporte N1 e N2	Exposição de dados sensíveis; falta de logs auditáveis.	App utilizado por ser mais "leve" que o oficial; sem criptografia de ponta a ponta.
Marketing	Ferramenta de automação (Zapier Free)	Coordenadora de Marketing	Estagiários e analistas	Integrações não autorizadas com dados de usuários; risco de API exposta.	Usada para envio automático de newsletters com base em dados do GitHub API.

Financeiro	Planilhas locais não criptografadas (Excel/Google Sheets)	Analista Financeiro	Equipe de Contabilidade	Alto. Dados financeiros expostos a vazamentos	Migrar para sistemas homologados com criptografia
Vendas	CRM não oficial (ex.: versões “free” ou pirateadas)	Gerente de Vendas	Equipe Comercial	Médio. Exposição de dados de clientes.	Adotar CRM corporativo com controle de acesso
Jurídico	Ferramentas de assinatura eletrônica não aprovadas (ex.: aplicativos piratas)	Advogado	Parceiros Externos ou Equipe Interna.	Alto. Fraude em contratos.	Usar plataformas validadas (ex.: DocuSign) com MFA.
TI/Infraestrutura	Roteadores domésticos desatualizados	Funcionário remoto	Equipe de TI/Infraestrutura	Alto. Vulnerabilidades exploráveis em redes.	Exigir VPN corporativa e atualizações automáticas.
Operações	USBs não criptografados para transferência de contratos	Coordenador Operacional	Equipe de operações	Alto. Risco interno de perda ou roubo de dados.	Bloquear USBs e usar soluções em nuvem criptografadas para transferência/armazenamento de arquivos
Marketing	Impressoras pessoais em home office	Designer	Equipe de Marketing	Médio. Vazamento de dados por impressão de documentos confidenciais em dispositivos inseguros.	Proibir impressão de dados sensíveis.
TI/Desenvolvimento	Repositórios de código em nuvem pessoal (ex.: GitHub pessoal)	Desenvolvedor	Equipe de desenvolvimento	Alto. Vazamento de código-fonte.	Restringir código a repositórios corporativos com 2FA.

Atendimento ao Cliente	Apps de comunicação não seguros para ambiente corporativo (ex.: Whatsapp)	Representante de Atendimento	Clientes e equipe interna	Médio. Vazamento de conversas.	Adotar plataformas criptografadas (ex.: Slack com canais privados)
Diretoria	Armazenamento em nuvem pessoal (ex.: Dropbox)	Diretor Executivo	Alta gestão	Alto. Exposição de estratégias confidenciais.	Migrar para aplicações como SharePoint com criptografia.
Recursos Humanos	Softwares de gestão de contratos não homologados	Especialista em RH	Equipe de RH	Médio. Vazamento de dados pessoais e estratégicos de clientes.	Transferir o risco no uso de sistemas corporativos que estejam de acordo com a LGPD.

Recomenda-se assistir os seguintes conteúdos do MF: Legislação em TI.

Unidade 2: Tema 3.

Recomenda-se assistir os seguintes conteúdos do MF: Fundamentos de Segurança. Unidade 1: Tema 1, 2 e 3.

Unidade 2: Tema 1 e 3.

Recomenda-se a leitura da NBR ISO/IEC27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação (2019).

4. Dispositivos pessoais utilizados na organização.

Setor	Dispositivo	Proprietário	Usuários	Risco	Obs.
Suporte Técnico	Smartphone Android	Analista de Suporte Técnico	João	Vazamento de dados via apps não autorizadas; acesso a e-mails corporativos sem criptografia.	Dispositivo usado para autenticação em dois fatores e comunicação via WhatsApp.
Desenvolvimento	Notebook Pessoal (MacOs)	Desenvolvedor ‘Full Stack’	Maria	Execução de código com permissões elevadas; ausência de antivírus corporativo.	Usa o dispositivo local para clonar repositórios e rodar builds locais.

DevOps	Smartphone Android	Engenheiro de ‘DevOps’	Carla	Aplicações de acesso remoto a servidores (SSH); uso de redes Wi-Fi públicas.	Dispositivo usado com apps de monitoramento (PagerDuty, Grafana, etc.).
Design e UX	iPad Pro pessoal	‘UI/UX Designer)	João	Armazenamento de protótipos de interfaces e credenciais de acesso à Figma.	Usa apps conectados às plataformas de design corporativas.
Gestão de Produto	Notebook Windows pessoal	Gestor de Produto	Fernanda	Sincronização com contas pessoais da nuvem; documentos estratégicos expostos.	Usa o notebook pessoal em viagens e reuniões com stakeholders externos.
Operações	Roteador doméstico desatualizado	Coordenador Operacional	Equipe Logística	Vulnerabilidades em Firmware expõem a rede corporativa.	Proibir impressão de dados sensíveis
TI	Dispositivo IoT (ex.: Alexa)	Funcionário de TI	Equipe de suporte	Dispositivos IoT comprometidos como vetores de ataque.	Isolar redes corporativas.
Atendimento	Aplicativo de mensagem pessoal (ex.: WhatsApp)	Representante de Atendimento	Clientes e equipe interna	Conversas confidenciais não criptografadas	Adotar aplicativos especializados em comunicação corporativa interna, como Slack ou Microsoft Teams.
Diretoria	Nuvem pessoal (ex.: Dropbox)	Diretor Executivo	Alta gestão	Armazenamento de estratégias confidenciais em plataformas não homologadas.	Migrar para SharePoint com RBAC.

Jurídico	Impressora pessoal.	Advogado	Parceiros externos ou equipe interna	Documentos confidenciais impressos em ambientes não controlados.	Proibir a impressão de dados sensíveis.

Recomenda-se assistir o seguinte conteúdo do MF: Legislação em TI.

Unidade 2: Tema 4.

Recomenda-se a leitura da NBR ISO/IEC27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação (2019).

5. Riscos de segurança física e lógica encontrados no contexto organizacional estudado.

Ativo	Ameaça	Vulnerabilidade
Dispositivos Remotos (laptops, USBs)	Roubo ou acesso físico a dispositivos em espaços públicos.	Falta de criptografia de disco completo ou políticas de bloqueio automático de tela.
Roteadores domésticos	Exploração de vulnerabilidades em firmware desatualizado.	Falta de atualizações automáticas ou configurações padrão inseguras.
Documentos físicos (contratos)	Acesso visual ou descarte inadequado em ambientes compartilhados.	Impressão não controlada de documentos confidenciais.
APIs financeiras	Ataques de injeção de dados (SQL injection) ou adulteração de transações.	Falta de validação de entradas ou ausência de pentests regulares.
Plataformas de e-signature	Fraude por autenticação inadequada (ex.: phishing de credenciais)	Ausência de MFA (Multi-Factor Authentication) ou certificados digitais.
Sistemas de precificação	Manipulação de fórmulas ou algoritmos por funcionários mal-intencionados.	Falta de revisão em pares (peer review) ou logs de auditoria.
Repositórios de código	Vazamento de código-fonte ou inserção de backdoors.	Armazenamento em plataformas não oficiais (ex.: GitHub Pessoal) sem 2FA.
Redes domésticas	Ataques via dispositivos IoT conectados à mesma rede de trabalho	Falta de isolamento de rede (ex.: VLANs) ou uso de VPN corporativa.
Dados em nuvem não homologado	Exposição de dados sensíveis em serviços como Dropbox ou Google Drive.	Armazenamento em plataformas pessoais sem criptografia ou controle de acesso.

Sistemas de autenticação	Ataques de ‘credential stuffing’ ou força bruta.	Senhas fracas ou ausência de MFA para acesso a sistemas críticos.

https://advisera.com/27001academy/pt-br/blog/2016/05/19/4-opcoes-de-mitigacao-no-tratamento-de-riscos-de-acordo-com-iso-27001/

Recomenda-se assistir os seguintes conteúdos do MF: Fundamentos de Segurança.

Unidade 1: Tema 1, 2 e 3.

Unidade 2: Tema 1 e 3.

Recomenda-se a leitura da NBR ISO/IEC27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação (2019).

6. Política de Segurança da informação para a organização estudada:

Desenvolvido no documento em anexo.