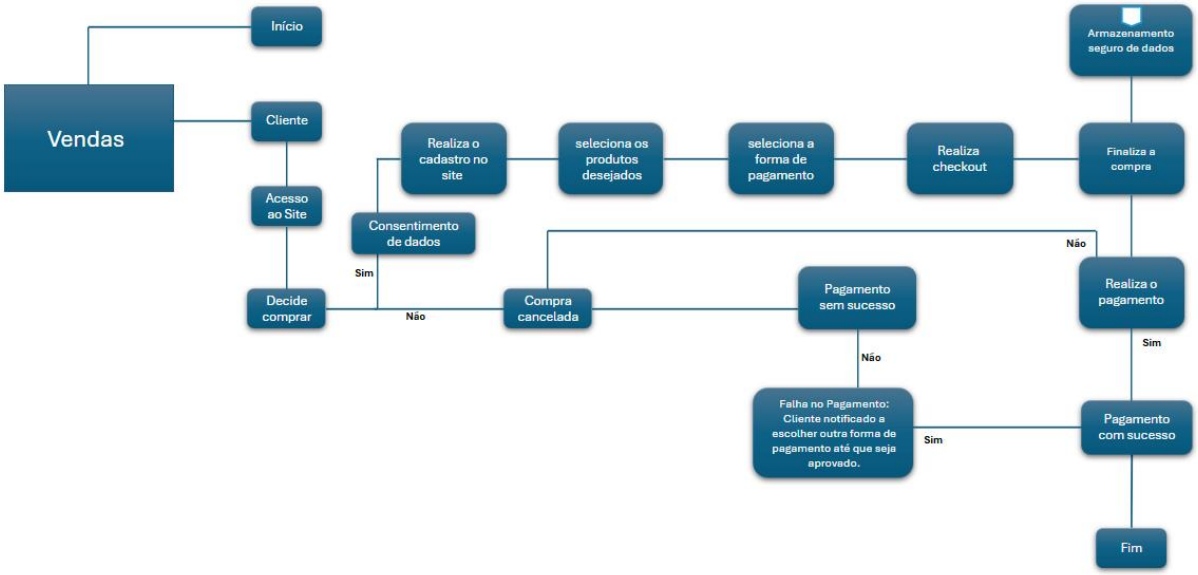
1. **Escolher 1 processo de negócio entre os que foram identificados na etapa 1 e detalhá-lo usando uma ferramenta de construção de fluxograma.**



2. **Identificar os componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido vistos no MF de Fundamentos de Segurança.**

- Realizar o cadastro no site.
- Seleção de forma de pagamento.
- Finalizar compra.
- Realização do pagamento.

3. **Mapear itens relacionados à TI invisível na organização.**

Setor	**Item de TI não catalogado**	**Proprietário**	**Usuários**	**Risco**	**Observações**
Vendas	Software de CRM pessoal	Representante de vendas individual	Equipe de vendas	Risco de perda de dados e falta de integração com sistemas oficiais	Utilizado para rastreamento de clientes individualmente

Marketing	Ferramentas de design online	Equipe de marketing	Designers e equipe de marketing	Risco de segurança e conformidade com dados pessoais	Ferramentas usadas para criar materiais rapidamente
RH	Planilhas de RH	Gerente de RH	Equipe de RH	Vulnerabilidade de dados sensíveis	Utilizado para acompanhamento de dados de colaboradores
Operações	Software de gestão de tarefas	Líder de operações	Equipe de operações	Falta de integração com sistemas de produtividade	Ferramenta pessoal usada para gestão de tarefas
Finanças	Ferramentas de análise de dados	Analista financeiro	Equipe financeira	Vazamento de dados financeiros	Utilizado para análises financeiras e projeções
Suporte Técnico	Ferramenta de controle remoto	Técnico de suporte	Equipe de suporte	Risco de acesso não autorizado	Utilizado para suporte rápido sem supervisão
Logística	Aplicativos de rastreamento	Coordenador de logística	Equipe de logística	Exposição de dados de localização e uso de redes não seguras	Usado para rastreamento de entregas por apps externos

4. Identificar dispositivos pessoais utilizados na organização.

Setor	Dispositivo	Proprietário	Usuários	Risco	Obs.
N/A	N/A	N/A	N/A	N/A	N/A

Conforme mencionado no anexo "Sabor do Campo - Política de Segurança.docx", o uso de dispositivos pessoais não é permitido para a realização de atividades relacionadas a empresa. Para mais detalhes, consulte a política.

5. Identificar riscos de segurança física e lógica discutidos no MF de Fundamentos de Segurança da Informação e encontrados no contexto organizacional estudado.

Ativo	Ameaça	Vulnerabilidade
Servidores	**Ataques de DDoS (Distributed Denial of Service):** Sobrecarga de	**Configurações inadequadas:** Configurações padrão ou

	servidores com tráfego, tornando-os indisponíveis. **Malware e Ransomware:** Software malicioso que pode comprometer dados e funcionalidades. **Acesso não autorizado:** Hackers podem explorar vulnerabilidades para obter acesso a dados sensíveis	mal configuradas podem ser exploradas. **Falta de atualizações:** Servidores desatualizados são vulneráveis a exploits conhecidos. **Credenciais fracas:** Senhas fracas ou não alteradas regularmente.
Computadores e notebooks	**Ameaças:** • **Phishing:** Tentativas de obter informações sensíveis por meio de e-mails ou sites fraudulentos. • **Spyware e Adware:** Software que coleta dados sem o consentimento do usuário. • **Roubo físico:** Dispositivos podem ser roubados, expondo dados armazenados.	**Falta de criptografia:** Dados não criptografados são facilmente acessíveis se o dispositivo for comprometido. **Software desatualizado:** Sistemas operacionais e aplicativos não atualizados são suscetíveis a ataques. **Uso de redes inseguras:** Conexões a redes Wi-Fi públicas sem proteção adequada
Infraestrutura de Rede	**Ameaças:** • **Intercepção de dados:** Ataques Man-in-the-Middle (MitM) podem capturar dados em trânsito. • **Injeção de pacotes maliciosos:** Pacotes de dados falsificados podem ser usados para explorar a rede. • **Ataques de redirecionamento:** Alteração de rotas para desviar o tráfego para	**Configurações de firewall inadequadas:** Falhas na configuração podem permitir acessos não autorizados. **Falta de segmentação de rede:** Redes não segmentadas podem facilitar a propagação de ataques. **Protocolos inseguros:** Uso de protocolos de comunicação obsoletos e inseguros.

	servidores maliciosos.	
Serviços de Nuvem	**Fuga de dados:** Acesso não autorizado a dados armazenados na nuvem. **Configurações inadequadas de segurança:** Exposição de dados devido a configurações incorretas. **Dependência de terceiros:** Risco associado ao provedor de serviços de nuvem.	• **Gerenciamento inadequado de credenciais:** Senhas fracas ou compartilhadas. • **Controle inadequado de acesso:** Falta de políticas de acesso rigorosas. • **Falta de criptografia:** Dados não criptografados durante o armazenamento ou trânsito. **Softwares**
Softwares	**Exploração de vulnerabilidades:** Uso de falhas de software para comprometer sistemas. **Backdoors:** Acesso escondido que permite a entrada não autorizada. **Trojan Horses:** Software aparentemente legítimo que executa ações maliciosas.	**Código mal escrito:** Bugs e falhas que podem ser explorados. **Falta de atualizações:** Software não atualizado é suscetível a exploits conhecidos. **Permissões excessivas:** Aplicativos com permissões além do necessário
Sistemas de Controle de Acesso	**Bypassing:** Técnicas para contornar sistemas de controle de acesso. **Social Engineering:** Manipulação de pessoas para obter acesso não autorizado. **Credential Stuffing:** Uso de combinações de usuário/senha roubadas.	**Autenticação fraca:** Uso de métodos de autenticação não robustos. **Gestão inadequada de privilégios:** Usuários com mais acesso do que o necessário. **Falta de monitoramento:** Ausência de auditoria e monitoramento de acessos.

6. **Elaborar uma Política de Segurança da informação para a organização estudada e baseada em modelo disponibilizado em material de apoio da etapa 2.**

[Verifica anexo - Sabor do Campo - Política de Segurança.docx]