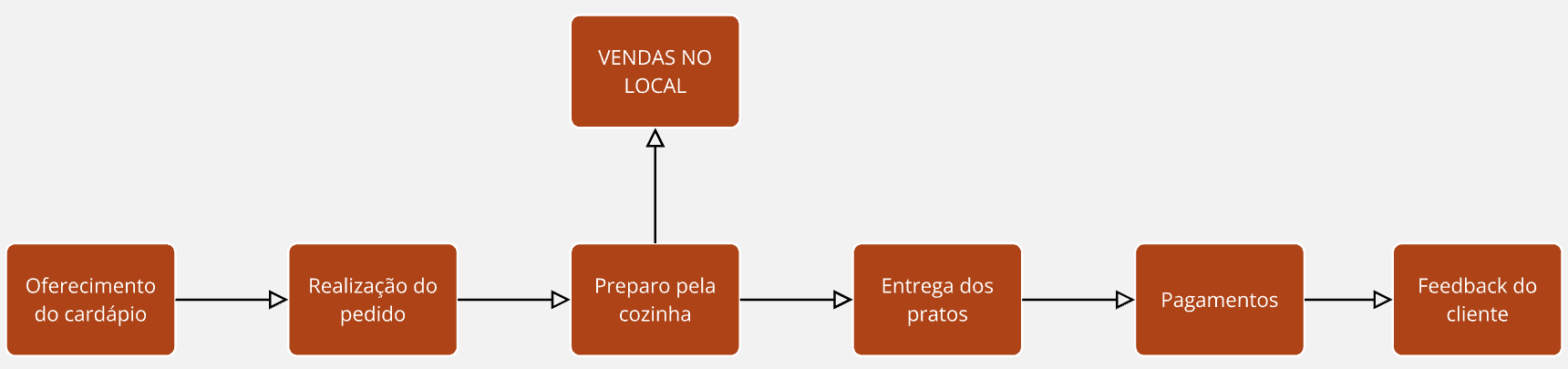
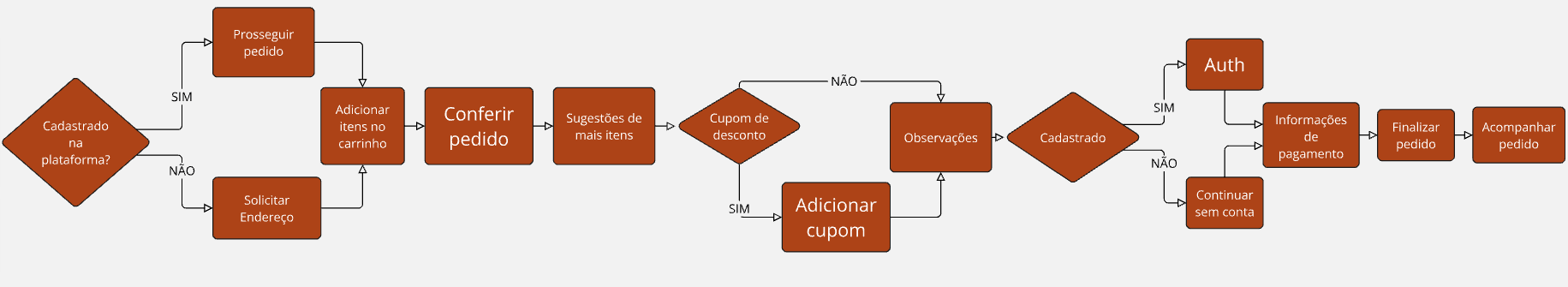
|  |  |  |
| --- | --- | --- |
| Descrição: Descrição: cabecalho2009_logo | Descrição: Descrição: cabecalho2009_linha1 | |
| Etapa 2 – Projeto Fundamentos de Sistemas. | |
| Descrição: Descrição: cabecalho2009_linha2 | |
|  |  |
|  |  |

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





Link para acesso ao fluxograma:

<https://miro.com/app/board/uXjVLY0PwDc=/?share_link_id=419408362836>

## 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.

No processo de vendas online por aplicativo, os componentes suscetíveis a eventos de segurança da informação incluem:

* **Dados do Cliente:** Informações pessoais e financeiras, como nome, endereço, e dados de cartão de crédito, que podem ser alvo de vazamentos ou roubo.
* **Plataforma de E-commerce:** Vulnerabilidades no software da loja virtual, incluindo plugins e temas desatualizados, que podem ser exploradas por hackers.
* **Conexões de Rede:** Redes Wi-Fi inseguras ou falta de criptografia durante a transmissão de dados podem permitir interceptação.
* **Processamento de Pagamentos:** Sistemas de pagamento que não estão devidamente protegidos, expondo transações a fraudes.
* **Armazenamento de Dados:** Bases de dados que não possuem segurança adequada, como criptografia e controle de acesso.
* **Autenticação de Usuários:** Falhas em sistemas de login e autenticação que podem permitir acesso não autorizado.
* **E-mails e Comunicação:** Phishing e outras técnicas que visam enganar usuários para obter informações sensíveis.
* **Atividades de Marketing:** Campanhas que envolvem coleta de dados podem ser vulneráveis a abusos e vazamentos.

Proteger esses componentes é essencial para garantir a segurança e a confiança dos clientes no processo de vendas online.

## Mapear itens relacionados à TI invisível na organização.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Setor | Item de TI não catalogado | Proprietário | Usuários | Risco | Obs. |
| Vendas | WhatsApp (para comunicação com clientes) | Equipe de vendas | |  | | --- | | vendas | | Representantes comerciais | | Vazamento de dados de clientes; falta de controle de informação | Utilizado para agilizar respostas a pedidos e orçamentos |
| Marketing | Trello (gestão de campanhas) | Gerente de Marketing | Equipe de marketing | Perda de controle de dados; falha na integração com sistemas oficiais | Sem integração com CRM oficial da empresa |
| Produção | Planilhas do Google Sheets (controle de produção) | Supervisores de Produção | Equipe de chão de fábrica | Perda de dados críticos; falta de backup na rede corporativa | Dados armazenados na nuvem fora dos sistemas internos |
| Logística | |  | | --- | |  | | Google Maps (para planejamento de rotas) | | Coordenador de Logística | Motoristas e coordenadores de entrega | Inconsistência nas rotas; falta de monitoramento em tempo real | Usado para traçar rotas, mas sem integração com sistema de rastreamento oficial |

## Identificar dispositivos pessoais utilizados na organização.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Setor | Dispositivo | Proprietário | Usuários | Risco | Obs. |
| Vendas | Smartphone pessoal | Analista de Vendas | Funcionário de Vendas | Vazamento de dados sensíveis de vendas para clientes | Aplicar política de criptografia de dados, autenticação de múltiplos fatores e restringir acesso a dados sensíveis pelo dispositivo |
| Financeiros e Contábeis | Notebook pessoal | Contador | Funcionário da Financeira e Contábil | Vazamento de dados financeiros, fraude ou roubo de informações | Aplicar política de criptografia de dados, autenticação de múltiplos fatores |
| Manufatura e Produção | Smartphone pessoal | Supervisor de Produção | Funcionário da Manufatura e Produção | Vazamento de dados operacionais e de produção | Aplicar política de criptografia de dados, autenticação de múltiplos fatores e restringir acesso a dados sensíveis pelo dispositivo |
| Recursos Humanos | Notebook pessoal | Analista de RH | Funcionário do RH | Vazamento de dados pessoais e confidenciais dos funcionários | Aplicar política de criptografia de dados, autenticação de múltiplos fatores |

## 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 |
| Lógico | Intrusão a Rede Wi-Fi | Senha fraca, falta de criptografia, e Firewall |
| Físico | Roubo / Furto | Falta de câmeras |
| Lógico | Vazamento de Dados | Falta de criptografia e configuração de Firewall |
| Físico | Incêndio | Falta de sistema de detecção de incêndio, portas sem vigilância |
| Físico | Vazamento de gás | Falta de manutenção no sistema de gás e verificação diária do mesmo |
| Físico | Equipamentos mal conservados | Falta de manutenção e verificação dos equipamentos de preparo e conservação de alimentos |
| Lógico | Invasão ao aplicativo de pedidos | Vulnerabilidade no software e em dispositivos físicos. |
| Lógico | Ransomware, Malware e furto de dados | Uso inseguro de computadores e celular no sistema/rede do restaurante, falta de segurança com os dados (físicos) |

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