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

### **Equipe de trabalho.**

* Lucas Shiroma – 884230
* Naiara Almeida Barros – 881598
* Pedro Manoel Fernandes Nogueira –877798
* Talita Fernandes – 877272
* Tiago Rodrigues de Oliveira e Cruz – 888797
* Vagner Cesar Lima – 882575

### **Mapeamento de Segurança da Informação.**

### **Processo de Vendas – Onyx Tech.**

**Objetivo:**

Nesta etapa, foi selecionado o processo de **vendas** da Onyx para mapeamento detalhado em relação à segurança da informação. O objetivo é identificar os componentes sujeitos a eventos de segurança que fazem parte desse processo, além de avaliar riscos e vulnerabilidades associados.  
  
**Atividades do Processo de Vendas:**

Fonte: imagem criada pelo grupo.
**Figura 1 – Fluxograma do Processo de Vendas da Onyx Tech.**  
 *Fonte: Elaborado pelo grupo.*

### **Componentes Vulneráveis e Eventos de Segurança:**

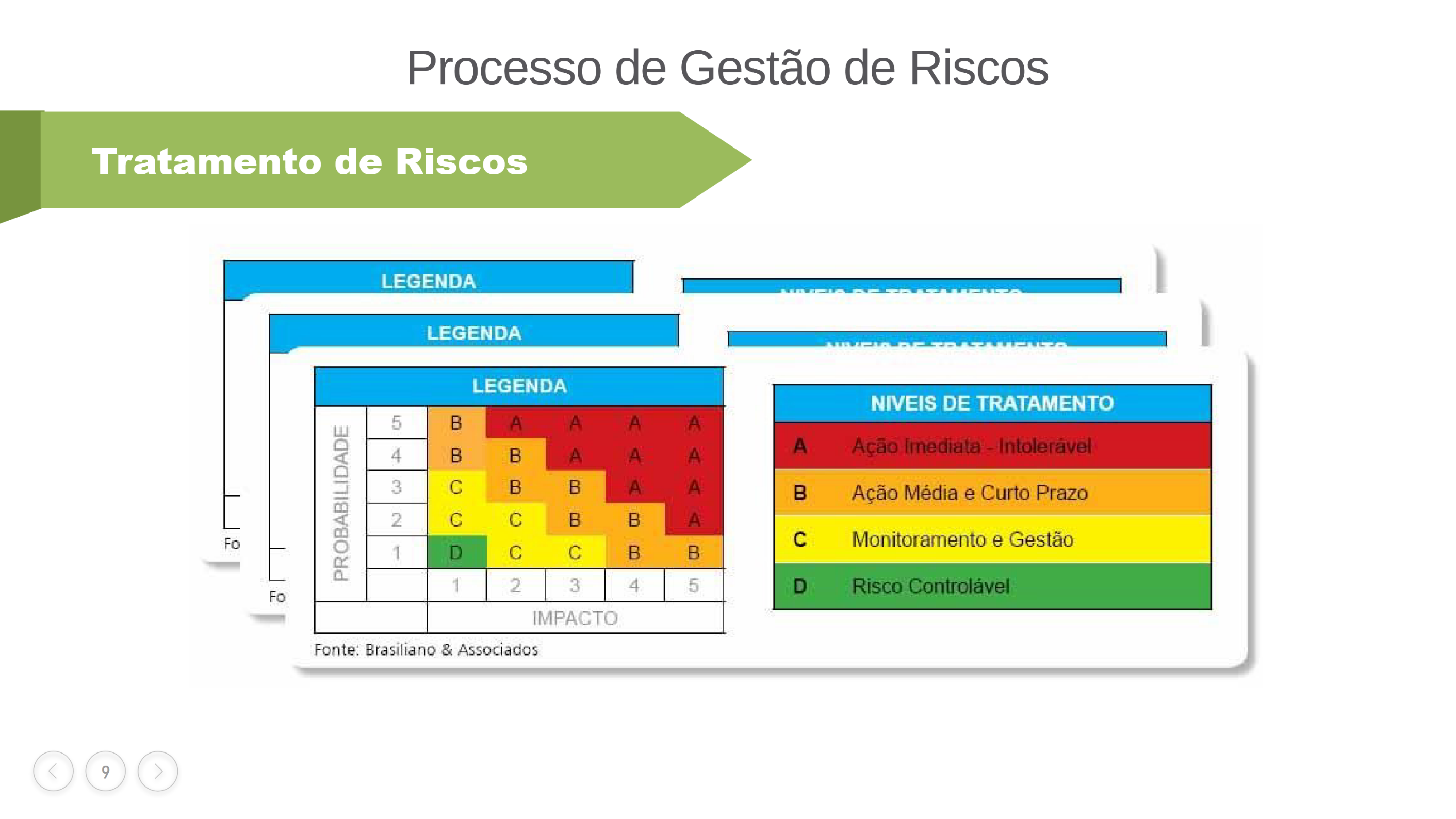
|  |  |  |
| --- | --- | --- |
| **Componentes** | **Tipo de Segurança** | **Evento de Segurança da Informação** |
| Notebooks dos vendedores | Lógica/Informação | * Malware * Roubo de informações * Adulteração de dados * Problemas em componentes |
| Sistema Sankhya | Lógica | * Ataques brute force * Falha na disponibilidade |
| Máquina de cartão de crédito | Física/Lógica | * Clonagem de cartão * Interceptação de dados em trânsito |
| Impressora de notas fiscais | Física/Informação | * Exposição de informação sensível * Impressão indevida de documentos |
| Wi-Fi público | Lógica | * Ataque Man-in-the-Middle * Rogue access points * Roubo de informações * Malware |
| Câmeras de segurança | Física/Lógica | * Acesso não autorizado * Denial of Service (DoS) * Manipulação física * Interceptação de vídeo em trânsito |
| Credenciais de usuários | Lógica | * Engenharia social * Phishing |
| Ambiente Físico | Física | * Acesso não autorizado * Furto   Vandalismo |

### **Shadow IT identificados:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Setor** | **Itens de TI não catalogados** | **Proprietários** | **Usuários** | **Risco** | **Tratamento de risco** |
| Gestores | Celulares com WhatsApp corporativo, notebook com informações sigilosas | Equipe de gestão | Mardem e equipe | Perda ou roubo dos dispositivos sem backup | A-5 |
| Vendas | Celulares com WhatsApp corporativo sem controle | Vendedores | Talita, Ricardo, Dayane | Perda do dispositivo móvel sem backup | A-4 |
| Atendimento | WhatsApp Business com tráfego pago | Equipe de atendimento | Helen, Erick, Ingrid | Perca do acesso, e envio de links maliciosos à clientes. | A-5 |
| Marketing | Aplicativo Canva sem controle de conta | Equipe de marketing | Felipe e equipe | Falta de controle da conta pode resultar em edições e alterações indesejadas | C-3 |
| Estoque | Planilhas Excel e Sankhya | Gil(estoque) | Gil e auxiliares | manipulação incorreta de dados | B-4 |
| Financeiro | App da conta PJ no celular | Deise(financeiro) | Deise e assistente | Phishing para roubo de dados da conta PJ. | A-5 |

## **Dispositivos pessoais utilizados na organização:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Setor** | **Dispositivo** | **Risco** | **Obs.** | **Tratamento de risco** |
| Marketing | Dispositivo móvel pessoal (celular) | Roubo/perda | Vazamento de dados | C-3 |
| Financeiro | Dispositivo móvel pessoal (celular) | Roubo/perda | Vazamento de dados | **A-5** |
| Atendimento | Dispositivo móvel pessoal (celular) | Roubo/perda | Vazamento de dados | **A-5** |
| Vendas | Dispositivo móvel pessoal (celular) | Roubo/perda | Vazamento  de dados | **A-5** |
| Administração | Dispositivo móvel pessoal (celular) | Roubo/perda ou phishing | Mais suscetível pelo maior privilégio de informações | **A-5** |

  
**Figura 2 – Matriz de Classificação e Tratamento de Riscos da Informação.**  
*Fonte: Material* da disciplina / Professor Fabio Leandro Rodrigues Cordeiro (2025)

**Riscos associados aos ativos da Onyx Tech:**

|  |  |  |
| --- | --- | --- |
| **Ativo** | **Ameaça** | **Vulnerabilidade** |
| Notebooks corporativos | * Furto * Malwares * Vazamento de dados * Acesso não autorizado * Engenharia social | * Falta de criptografia nos dados * Uso sem monitoramento * Senhas fracas * Falta de conscientização sobre golpes de phishing |
| Celulares corporativos | * Vazamento de dados * Acesso não autorizado * Engenharia social | * Uso de apps que se encaixam em shadowIT * Falta de criptografia nos dados * Senhas fracas * Não possui MFA * Smishing * Vishing |
| Planilhas de controle de estoque | * Perda de acesso * Vazamento de dados | * Armazenamento em contas pessoais * Ausência de backup |
| Sistema Sankhya(ERP) | * Acesso não autorizado * Alteração de dados | * Não possui MFA * Acesso não monitorado |
| Produtos vendidos | * Furto * Extravio | * Estoque sem monitoramento * Controle de acesso físico frágil |
| Rede da empresa | * Acesso não autorizado à rede dos funcionários | * Configuração fraca * Criptografia legacy * Falhas no isolamento entre redes |
| Dados de clientes | * Vazamento de dados * Roubo de identidade * Engenharia social | * Armazenamento inseguro * Acesso irrestrito * Funcionários podem ser manipulados a fornecer dados de clientes |
| Câmeras de segurança | * Invasão * Indisponibilidade | * Acesso remoto sem autentificação forte * Câmeras IP desprotegidas |
| Máquina de cartão de crédito | * Captura de dados de pagamento | * Falta de verificação física regular * Firmware desatualizado |
| Impressora de notas fiscais | * Impressão indevida de documentos | * Conexão em rede sem controle de acesso |
| Local físico da loja | * Invasão * Roubo * Vandalismo | * Acesso físico desprotegido * Portas sem algum tipo de controle |
| Contas de usuário no ERP Sankhya | * Acesso não autorizado * Abuso de privilégios | * Controle de acesso ineficaz * Compartilhamento de contas |
| Credenciais de acesso (PINs) | * Acesso não autorizado * Engenharia social | * PINs compartilhados * Ausência de política de troca * Funcionários podem ser enganados para fornecer suas credenciais |
| Laboratório técnico | * Vazamento de dados * Furto de aparelhos | * Controle de acesso frágil * Equipamentos não protegidos |
| Sistema de alarme terceirizado | * Desativação intencional * Interrupção de serviço * Roubo de informações operacionais | * Dependência de terceiros * Falta de criptografia nas comunicações * Credenciais fracas ou compartilhadas |