LEVANTAMENTO DE RISCOS, VULNERABILIDADE E AMEAÇAS

EMPRESA: Cannoli

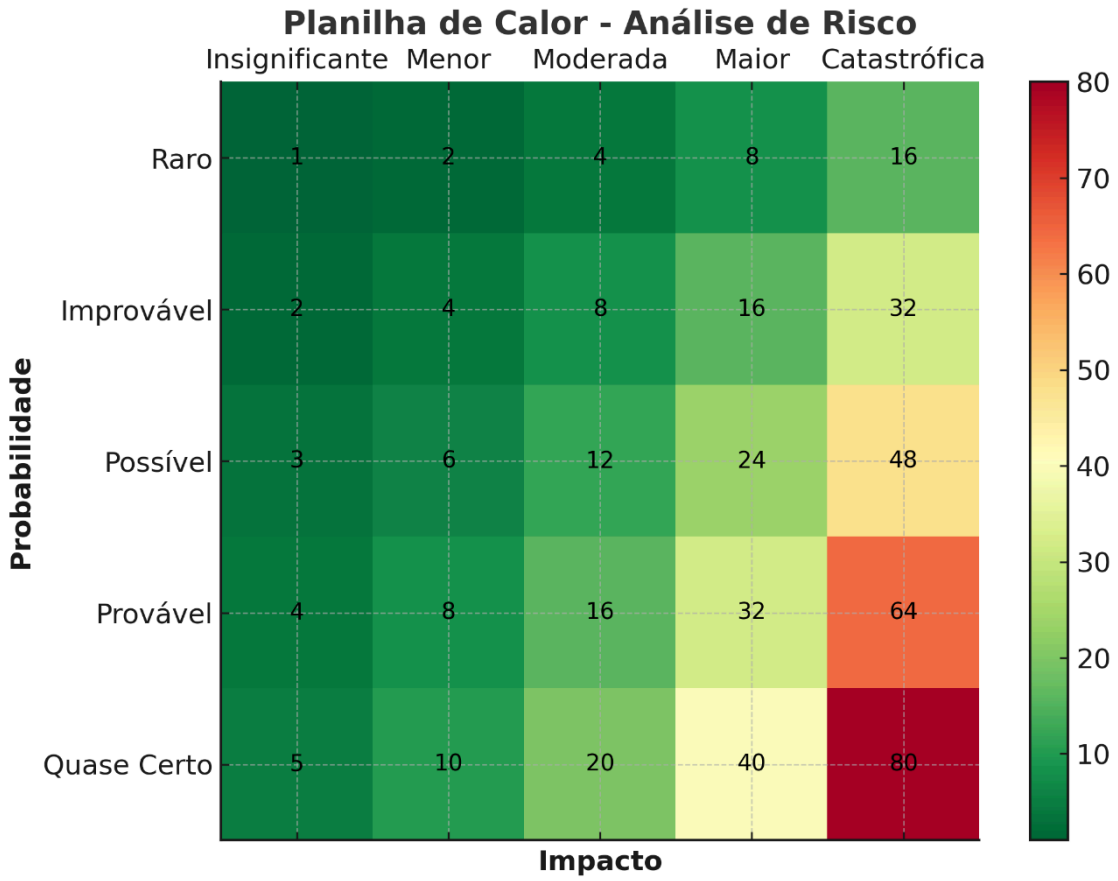
Responsável: Luan Meireles Franchini

1. **Referencial Utilizado**
   Para avaliação e priorização dos riscos, foram utilizados os seguintes frameworks e ferramentas:
   - NIST Cybersecurity Framework (CSF): Identificar, Proteger, Detectar, Responder e Recuperar.
   - Matriz GUT (Gravidade, Urgência e Tendência): definição de prioridade dos riscos.
   - Matriz de Riscos (Heatmap): avaliação de Probabilidade x Impacto.
2. **Levantamento de Ameaças e Vulnerabilidades**
   Considerando que a Canolli lida com dados de restaurantes, campanhas de marketing e clientes,
   foram identificados os seguintes riscos:
   R1 - Interno: Falta de mão de obra qualificada
   R2 - Interno: Vazamento de dados de clientes
   R3 - Externo: Ataque hacker ao site
   R4 - Externo: Tentativa de DDoS
   R5 - Externo: Ataque hacker ao banco de dados financeiro
   R6 - Externo: Aumento de custos de infraestrutura
3. **Matriz GUT (Gravidade, Urgência, Tendência)**

Risco	G	U	T	Índice GUT	Prioridade
Vazamento de dados de clientes (R2)	5	5	5	125	1
Ataque hacker ao site (R3)	4	4	4	64	2
Ataque hacker financeiro (R5)	5	3	4	60	3
Tentativa de DDoS (R4)	3	4	3	36	4
Falta de mão de obra (R1)	2	3	2	12	5
Aumento de custos (R6)	2	2	2	8	6

4. **Análise de Riscos (Probabilidade x Impacto)**
   - Vazamento de dados de clientes → Impacto catastrófico (16), probabilidade provável (4) → Nível 64 (Risco crítico).
   - Ataque hacker ao site → Impacto maior (8), probabilidade provável (4) → Nível 32 (Risco alto).
   - Ataque financeiro → Impacto catastrófico (16), probabilidade possível (3) → Nível 48 (Risco alto).
   - Tentativa de DDoS → Impacto moderado (4), probabilidade possível (3) → Nível 12 (Risco médio).
   - Falta de mão de obra → Impacto menor (2), probabilidade possível (3) → Nível 6 (Risco baixo).
   - Aumento de custos → Impacto moderado (4), probabilidade improvável (2) → Nível 8 (Risco baixo).

5. **Conclusão e Recomendações**
   - Prioridade máxima: proteção contra vazamento de dados (adoção de criptografia, controle de acesso e monitoramento).
   - Mitigação: aplicar firewall e monitoramento contínuo contra ataques externos (DDoS, SQL Injection, etc.).
   - Gestão de recursos internos: treinamento de equipe de TI e planejamento de contingência em caso de falta de pessoal.
   - Custos: avaliar alternativas de cloud computing e escalabilidade para reduzir impacto de custos variáveis.



OBS: Imagem gerada com ajuda de IA

Matriz de Riscos – Canolli

1. Risco Financeiro

- **Descrição:** Falta de capital de giro e dificuldade de manter fluxo de caixa.
- **Impacto:** Alto – pode comprometer continuidade do negócio.
- **Probabilidade:** Média.
- **Ações Preventivas:**
  - Planejamento financeiro detalhado.
  - Reserva de emergência.
  - Controle rígido de custos.
- **Plano de Mitigação:**
  - Revisar preços e fornecedores.

    - Buscar linhas de crédito.

2. Risco Operacional

- **Descrição:** Falha na produção, atraso em entregas ou indisponibilidade de insumos.
- **Impacto:** Alto – pode afetar imagem e confiança do cliente.
- **Probabilidade:** Média.
- **Ações Preventivas:**
    - Mapeamento do processo produtivo.
    - Fornecedores alternativos.
    - Controle de estoque.
- **Plano de Mitigação:**
    - Reorganizar cronogramas.
    - Comunicação rápida com clientes.

3. Riscos Estratégicos

- **Descrição:** Concorrência acirrada e variação da demanda.
- **Impacto:** Médio.
- **Probabilidade:** Alta.
- **Ações Preventivas:**
    - Monitoramento de tendências de consumo.
    - Estratégias de marketing digital.
    - Diferenciação de produto.
- **Plano de Mitigação:**
    - Promoções e combos.
    - Ajuste de cardápio conforme demanda.

4. Risco Legal/Regulatório

- **Descrição:** Falta de conformidade com normas sanitárias e fiscais.
- **Impacto:** Alto – pode gerar multas ou interdição.
- **Probabilidade:** Baixa/Média.
- **Ações Preventivas:**
    - Cumprir todas as normas da vigilância sanitária.
    - Contabilidade organizada.
- **Plano de Mitigação:**
    - Correção imediata de não conformidades.
    - Consultoria jurídica/contábil quando necessário.

5. Riscos à Segurança da Informação

- **Descrição:** Falha em sistemas de vendas online ou problemas de segurança digital.
- **Impacto:** Médio.

- **Probabilidade:** Média.
- **Ações Preventivas:**
  (ID – Identify) → mapeamento de ativos digitais, classificação de dados críticos.
  (PR – Protect) → controle de acessos, backups, antivírus, conscientização dos colaboradores.
  (DE – Detect) → monitoramento de logs, alertas de intrusão, auditorias periódicas.
  (RS – Respond) → plano de resposta a incidentes, comunicação imediata, equipe preparada.
  (RC – Recover) → plano de recuperação de desastres, restauração de backups, análise pós-incidente.

- **Plano de Mitigação:**
  - Ativação de canais de venda alternativos.
  - Restauração rápida de sistemas.

6. Riscos de Conformidade

- **Descrição:** Rotatividade de funcionários e falta de mão de obra qualificada.
- **Impacto:** Médio.
- **Probabilidade:** Média.
- **Ações Preventivas:**
  - Treinamento contínuo.
  - Incentivos e benefícios.
- **Plano de Mitigação:**
  - Redistribuição temporária de tarefas.
  - Contratações emergenciais.

7. Risco à Reputação

Descrição: Reclamações de clientes, críticas em redes sociais ou falhas de qualidade que prejudiquem a imagem da marca.

Impacto: Alto – pode gerar perda de credibilidade e queda nas vendas.

Probabilidade: Média.

Ações Preventivas:

- Monitoramento ativo das redes sociais.
- Garantia de padrões de qualidade e higiene.
- Treinamento da equipe para bom atendimento ao cliente.

Plano de Mitigação:

- Resposta rápida e profissional a críticas.
- Ações de marketing e campanhas de confiança.
- Correção imediata de falhas apontadas.