NIST Cybersecurity Framework – Projeto Cannoli

1. Identificar (Identify – ID)

Objetivo: Mapear e compreender os ativos digitais, riscos e responsabilidades para a segurança cibernética.

- **ID.AM (Gerenciamento de Ativos):**
  - **Ativos digitais:** Banco de dados de clientes, informações de vendas, KPIs estratégicos, relatórios exportados, algoritmos de Machine Learning (ML), dashboards e APIs.
  - **Perfis de usuários:**
    - Admin Cannoli: Visualização de indicadores estratégicos e gerenciamento da plataforma.
    - Cliente Cannoli: Visualização de métricas personalizadas de seu próprio negócio.
    - Desenvolvedor Interno: Manutenção, atualizações e alterações no código-fonte e infraestrutura.
  - **Permissões:** Acesso rigorosamente controlado por um sistema de Role-Based Access Control (RBAC), onde Admins e Clientes possuem permissões de visualização (read-only) para dados relevantes, enquanto Desenvolvedores possuem permissões de alteração (write) apenas em ambientes de desenvolvimento e homologação.
  - **Risco de escalonamento de privilégios:** Considerado **baixo**. A arquitetura da aplicação impedirá que usuários alterem seus próprios perfis via API e as permissões serão estritamente segregadas no backend, garantindo que um perfil Cliente não possa acessar endpoints destinados a Admins.
- **ID.BE (Ambiente de Negócios):**
  - O dashboard é um ativo estratégico para a fidelização de clientes e um pilar para a tomada de decisão baseada em dados.
  - Interrupções no serviço podem impactar diretamente a operação dos restaurantes parceiros, a receita e a reputação da startup Cannoli no mercado.
- **ID.GV (Governança):**
  - Conformidade com a Lei Geral de Proteção de Dados (LGPD) é um princípio central e inegociável do projeto.
  - A responsabilidade pelo controle e implementação da segurança cibernética é formalmente atribuída ao time de desenvolvimento, com supervisão da liderança do projeto.
- **ID.RA (Avaliação de Risco):**
  - **Riscos mapeados:**
    - Vazamento de dados pessoais de clientes (alto impacto).
    - Acesso não autorizado a dados estratégicos da Cannoli ou de restaurantes.
    - Indisponibilidade do serviço por falha de servidor (ponto único de falha).
    - Manipulação de KPIs por agentes internos ou externos mal-intencionados.
    - Ataques a APIs (injeção de dados, abuso de endpoints).

- **ID.RM (Estratégia de Gerenciamento de Risco):**
  - Adotada uma estratégia de nível intermediário, que busca um equilíbrio ideal entre segurança robusta e agilidade/usabilidade da plataforma.
  - Uso de matriz de riscos para priorização:
    - Ataques internos: Risco **Alto** (devido ao acesso privilegiado).
    - Erro humano: Risco **Médio** (mitigado por treinamento e interface intuitiva).
    - Falha de infraestrutura: Risco **Alto** (devido à ausência de redundância).
    - Falhas de atualização: Risco **Médio** (controlado por um plano de manutenção).

2. Proteger (Protect – PR)

Objetivo: Implementar controles e salvaguardas para reduzir a probabilidade e o impacto de incidentes.

- **PR.AC (Controle de Acesso):**
  - Autenticação obrigatória para todos os acessos.
  - Perfis de acesso rigorosamente segregados (Admins, Clientes, Desenvolvedores) via RBAC.
  - Recomendação de implementação futura de autenticação multifator (MFA) para todos os perfis, especialmente Admin.
- **PR.AT (Conscientização e Treinamento):**
  - Treinamento obrigatório e contínuo para o time de desenvolvimento em práticas de desenvolvimento seguro (Secure Coding) e nos requisitos da LGPD.
  - Documentação de boas práticas para tratamento de dados pessoais disponível para toda a equipe.
- **PR.DS (Segurança de Dados):**
  - Criptografia de dados **em repouso** (banco de dados MySQL) e **em trânsito** (protocolo HTTPS/TLS 1.2 ou superior).
  - Backup diário automatizado com uma política de retenção de **5 anos**.
  - **Política de descarte de dados:** Dados sensíveis serão completamente anonimizados ou excluídos de forma segura após o término do período de retenção, garantindo que não possam ser recuperados.
- **PR.IP (Processos e Procedimentos):**
  - Aplicação dos princípios de **Privacy by Design** e **Security by Design** desde a concepção do sistema.
  - Toda a gestão de acesso, tratamento e descarte de dados será documentada em um manual de políticas de segurança.
- **PR.MA (Manutenção):**
  - Estabelecida uma **rotina trimestral** para verificação de vulnerabilidades nas dependências (Flask, Dash, Plotly, MySQL, scikit-learn). Ferramentas como pip-audit serão utilizadas para automatizar a detecção de pacotes vulneráveis.
  - As atualizações de segurança críticas serão aplicadas em até 48 horas após sua publicação.

- **PR.PT (Tecnologia de Proteção):**
    - Implementação de proteções no código contra vulnerabilidades comuns, como SQL Injection (usando ORM ou *prepared statements*) e Cross-Site Scripting (XSS) (usando *escaping* de saídas).
    - Monitoramento ativo de dependências externas.
    - Recomendação de uso de um Web Application Firewall (WAF) no ambiente de produção para proteção adicional.

3. Detectar (Detect – DE)

Objetivo: Garantir a detecção rápida de incidentes e comportamentos suspeitos.

- **DE.CM (Monitoramento Contínuo):**
    - Monitoramento contínuo de logs de acesso, autenticação e atividades críticas.
    - Configuração de **alertas automáticos** (via e-mail para a equipe de desenvolvimento) para eventos como:
        - Mais de 5 tentativas de login falhas para o mesmo usuário em menos de 1 minuto.
        - Tentativa de acesso a endpoints por perfis não autorizados.
        - Exportação de relatórios com volume de dados acima de um limite pré-definido.
- **DE.DM (Processos de Detecção):**
    - Análise automatizada de logs para identificar padrões de uso anômalos.
    - Monitoramento especial sobre a funcionalidade de exportação de relatórios, considerado um ponto crítico de potencial vazamento de dados.
    - **Definição de KPIs de segurança com metas claras:**
        - % de incidentes detectados e tratados: Meta > 95%.
        - Tempo Médio para Resposta (MTTR): Meta < 4 horas para incidentes críticos.
        - Taxa de sucesso em autenticação segura: Monitorar falhas para identificar ataques de força bruta.

4. Responder (Respond – RS)

Objetivo: Minimizar os impactos de incidentes detectados por meio de ações coordenadas.

- **RS.RP (Planejamento de Resposta):**
    - Um **Plano de Resposta a Incidentes** será documentado, contendo:
    - **Níveis de severidade** dos incidentes (Baixo, Médio, Alto, Crítico).
    - **Papéis e responsabilidades** (quem lidera a resposta, quem executa, quem comunica).
    - **Fluxos de comunicação** internos (equipe) e externos (clientes, autoridades).
    - **Checklists de ação** para tipos comuns de incidentes (ex: negação de serviço, vazamento de dados).
- **RS.CO (Comunicação):**

    - Obrigatoriedade de notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares em caso de incidentes relevantes, conforme determina a LGPD.
    - Comunicação transparente com administradores e clientes sobre a natureza do incidente e as medidas tomadas.
- **RS.AN (Análise):**
    - Análise de logs e evidências digitais para identificar a causa raiz do incidente e sua extensão.
    - O processo de análise será documentado para reconstruir a cronologia dos eventos.
- **RS.MI (Mitigação):**
    - Ações imediatas para conter o incidente, como bloqueio de endereços IP suspeitos, revogação de credenciais comprometidas e aplicação de patches emergenciais.
- **RS.IM (Melhorias):**
    - Após cada incidente, será realizada uma reunião de "lições aprendidas" para identificar falhas e ajustar continuamente os controles de segurança e o plano de resposta.

5. Recuperar (Recover – RC)

Objetivo: Restaurar as operações de forma rápida, segura e resiliente.

- **RC.RP (Planejamento de Recuperação):**
    - O plano se baseia no backup diário para restauração de dados.
    - **Risco identificado:** A infraestrutura atual possui um ponto único de falha (um servidor, sem redundância).
    - **Objetivos de Recuperação definidos:**
        - **RPO (Recovery Point Objective):** 24 horas. Em um cenário de desastre, a perda máxima de dados será de 24 horas.
        - **RTO (Recovery Time Objective):** 8 horas. Em caso de falha total do servidor, a equipe se compromete a restaurar a aplicação e o último backup em um novo ambiente em até 8 horas.
- **RC.IM (Melhorias):**
    - Revisão pós-incidente para fortalecer pontos frágeis na arquitetura ou nos processos.
    - Reavaliação periódica da arquitetura de infraestrutura para incorporar maior resiliência e escalabilidade, como o uso de balanceadores de carga e bancos de dados replicados.
- **RC.CO (Comunicação):**
    - Comunicação proativa com clientes e parceiros sobre o status da recuperação e o tempo estimado para a normalização dos serviços.
    - Elaboração de relatórios pós-incidente para stakeholders, detalhando o ocorrido, o impacto e as melhorias implementadas para prevenir recorrências.