NIST Cybersecurity Framework

1. IDENTIFY (Identificar)

Objetivo: Compreender o ambiente organizacional para gerenciar riscos de cibersegurança a sistemas, pessoas, ativos, dados e capacidades.

Atividades no FastPrice:

- **Mapeamento de Ativos:** APIs de integração (Uber, 99, Indrive), infraestrutura do site, servidores, banco de dados com dados dos usuários.
- **Análise de Riscos:**
    - **Financeiros:** Falta de receita inicial, dificuldade em atrair investimento.
    - **Operacionais:** Falhas em APIs e IA incorreta.
    - **Segurança da Informação:** Vazamento de dados, falta de criptografia, engenharia social.
- **Avaliação de Vulnerabilidades:**
    - Falhas de API.
    - Criptografia ausente ou fraca.
    - Sistemas desatualizados.
- **Requisitos Legais e Regulatórios:** LGPD, GDPR e leis locais aplicáveis à proteção de dados e segurança.

2. PROTECT (Proteger)

Objetivo: Desenvolver e implementar salvaguardas apropriadas para garantir a entrega de serviços essenciais e proteger ativos críticos.

Atividades no FastPrice:

- **Segurança da Informação:**
    - Criptografia de dados em repouso e em trânsito.
    - Controle de acesso e autenticação multifator para administradores e usuários.
- **Gestão de Identidades e Acessos:**
    - Políticas claras de quem pode acessar o quê.
    - Treinamento de funcionários para prevenção de engenharia social.
- **Proteção de Dados:**

- Coleta e armazenamento seguindo LGPD/GDPR.
- Explicitação do uso da IA e critérios de comparação de preços.

- **Educação e Conscientização:**

    - Campanhas internas de segurança cibernética.
    - Treinamentos sobre privacidade e uso ético de IA.

DETECT (Detectar)

Objetivo: Desenvolver e implementar atividades apropriadas para identificar a ocorrência de um evento de cibersegurança.

Atividades no FastPrice:

- **Monitoramento Contínuo:**

    - Monitorar tentativas de acesso não autorizado.
    - Monitorar integridade dos dados e APIs.

- **Sistemas de Alerta:**

    - Implementação de alertas para atividades incomuns (padrões de uso anormais, ataques DDoS).

- **Auditoria e Logs:**

    - Armazenar e revisar registros de acesso e ações realizadas no sistema.

4. RESPOND (Responder)

Objetivo: Desenvolver e implementar atividades apropriadas para agir em relação a um incidente de cibersegurança detectado.

Atividades no FastPrice:

- **Plano de Resposta a Incidentes:**

    - Procedimentos claros para lidar com vazamento de dados, ataques DDoS, falhas de API.

- **Comunicação de Incidentes:**

    - Notificação transparente aos usuários em caso de incidente.
    - Contato com órgãos reguladores conforme exigido pela LGPD.

- **Análise Pós-Incidente:**
    - Avaliação de causa raiz.
    - Melhoria contínua dos controles com base nos incidentes ocorridos.

5. RECOVER (Recuperar)

Objetivo: Desenvolver e implementar atividades para restaurar quaisquer capacidades ou serviços que foram prejudicados devido a incidentes de cibersegurança.

Atividades no FastPrice:

- **Plano de Continuidade de Negócios:**
    - Backup regular das bases de dados e código-fonte.
    - Redundância de infraestrutura para evitar downtime em falhas.
- **Comunicação Pós-Incidente:**
    - Informar clientes sobre status da recuperação.
    - Reforçar confiança na marca com ações claras e responsáveis.
- **Melhoria Contínua:**
    - Aprendizado com falhas para fortalecer políticas de segurança.
    - Reforço das proteções técnicas e treinamento após incidentes.

Matrix GUT

Nº	Categoria	Risco	G	U	T	Prioridadae
1	Interno	Falta de receita inicial	4	4	3	48
2	Externo	Falha em captar investimentos	4	3	4	48
3	Externo	Falhas em APIs (Uber, 99, Indrive)	5	5	4	100
4	Interno	IA fornecendo preços incorretos	4	4	4	64
5	Externo	Ataques DDoS / sistema fora do ar	5	5	5	125
6	Interno	Vazamento de dados de clientes	5	5	5	125
7	Interno	Uso indevido de dados – violação da LGPD/GDPR	5	5	4	100
8	Interno	Interface ruim ou erros nos cálculos	3	3	3	27
9	Interno	Algoritmo enviesado – preços injustos	4	4	4	64
10	Externo	Lançamento de concorrente direto (ex: Google/Uber)	5	3	4	60
11	Interno	Falta de confiança/entendimento do serviço	4	4	4	64
12	Interno	Falha em seguir normas de segurança (fraudes)	5	5	5	125
13	Interno	Falhas de criptografia na comunicação	5	5	5	125
14	Interno	Engenharia social com funcionários	5	4	4	80
15	Interno	Sistemas desatualizados	4	4	5	80

Top 5 Riscos Prioritários (com maior GUT):

1. **Ataques DDoS ou sistema fora do ar** (GUT: 125)
2. **Vazamento de dados de clientes** (GUT: 125)
3. **Falha em seguir normas de segurança** (GUT: 125)
4. **Falhas de criptografia na comunicação** (GUT: 125)
5. **Falhas em APIs com plataformas de transporte** (GUT: 100)