Startup: SafeCloud AI

Setor: Tecnologia e Segurança Cibernética **Missão:** Proteger empresas contra ameaças digitais, oferecendo uma plataforma de inteligência artificial para monitoramento e prevenção de ataques cibernéticos. **Visão:** Tornar a segurança digital acessível e automatizada para empresas de pequeno e médio porte.

Contexto Inicial

A SafeCloud AI foi fundada por dois engenheiros de segurança cibernética e um especialista em aprendizado de máquina, visando criar uma solução de monitoramento proativo que alerta e mitiga riscos antes que se tornem um problema.

🏗️ Plano de Continuidade de Negócios (PCN)

1. Identificação dos Recursos Críticos

Os principais recursos e sistemas essenciais para a operação incluem:

- **Plataforma de Inteligência Artificial**: Core do negócio, realiza análise em tempo real para detecção de ameaças.
- **Servidores e Bancos de Dados**: Hospedam as informações de clientes e os logs de segurança.
- **Equipe Técnica**: Especialistas em segurança e IA responsáveis por atualização e manutenção.
- **Parcerias Estratégicas**: Provedores de nuvem e fornecedores de infraestrutura.
- **Canais de Comunicação**: Sistemas de suporte ao cliente e gestão de incidentes.

2. Análise de Impacto nos Negócios (BIA)

Possíveis eventos disruptivos e seus impactos incluem:

- **Falha de TI**: Se o sistema principal cair, os clientes ficam expostos a ataques. Impacto: reputação e perdas financeiras.
- **Ataque Cibernético**: Violação de dados dos clientes pode resultar em processos legais e perda de confiança. Impacto: jurídico e operacional.
- **Desastre Natural**: Danos físicos ao data center podem comprometer a operação. Impacto: infraestrutura e continuidade.

3. Estratégias de Recuperação

Medidas para garantir continuidade do negócio incluem:

- **Redundância de Servidores**: Uso de data centers em locais distintos para replicação em tempo real.
- **Backup Regular**: Sistema automatizado para armazenar e proteger dados em múltiplas instâncias.
- **Plano de Comunicação de Crise**: Procedimentos internos e externos para informar clientes e parceiros rapidamente.
- **Treinamento da Equipe**: Simulações periódicas de resposta a incidentes.
- **Acordos de Contingência**: Parcerias com terceiros para suporte emergencial.

4. Plano de Ação

Detalhamento das etapas de resposta e recuperação:

1. **Detecção e Análise** – Sistemas de monitoramento identificam falhas ou ameaças.
2. **Resposta Rápida** – Ativação de servidores de backup e notificação da equipe de segurança.
3. **Comunicação Interna e Externa** – Informar clientes sobre a situação e fornecer atualizações.
4. **Recuperação Total** – Aplicação de correções e restauração completa dos serviços.
5. **Revisão e Melhoria** – Análise pós-incidente para fortalecer medidas preventivas.

5. Teste do Plano

Para garantir a eficácia do PCN, a SafeCloud AI realiza:

- **Simulações periódicas** de ataques cibernéticos e falhas de sistema.
- **Testes de backup** para verificar integridade dos dados armazenados.
- **Treinamento prático** com funcionários para garantir resposta rápida e eficiente.
- **Auditorias internas** para ajustar estratégias conforme novas ameaças emergem.