Eduardo Baptistella

824147595

1. Introdução da Empresa e seu Cenário

Nome da Empresa: HealthTech Solutions

Setor: Saúde Digital

Tipo de Empresa: Startup de Tecnologia focada em soluções de telemedicina e monitoramento remoto de pacientes.

Descrição: A HealthTech Solutions desenvolve aplicativos móveis e plataformas baseadas em nuvem para consultas médicas online, acompanhamento de tratamentos e gestão de dados de pacientes. A empresa conecta médicos, pacientes e clínicas por meio de uma plataforma de videoconferência segura, além de utilizar dispositivos IoT para monitorar a saúde dos pacientes remotamente. A empresa atende a pacientes em várias regiões do país e possui parcerias com diversas clínicas e hospitais.

Cenário: A HealthTech Solutions possui uma infraestrutura de TI baseada em serviços de nuvem, utilizando plataformas como AWS para hospedagem de suas aplicações e dados. O negócio depende da disponibilidade contínua da plataforma para fornecer serviços médicos, realizar consultas em tempo real e monitorar a saúde dos pacientes. Qualquer interrupção nas operações pode ter impactos críticos tanto para a empresa quanto para seus clientes.

2. Identificação dos Recursos Críticos

Os recursos e sistemas essenciais para a operação da HealthTech Solutions são:

- **Plataforma de Videoconferência e Consultas Online:** Sistema que permite que médicos e pacientes se conectem para consultas remotas.
- **Sistemas de Armazenamento de Dados de Pacientes:** Bases de dados de pacientes que armazenam informações pessoais e registros médicos sensíveis.
- **Servidores de Nuvem:** Provedores de infraestrutura em nuvem como AWS ou Google Cloud, responsáveis pela hospedagem de serviços e dados.

- **Aplicativos Móveis:** Aplicações móveis utilizadas por pacientes e médicos para acessar a plataforma e monitorar a saúde.
- **Sistemas de Comunicação com Clientes:** Email, chat ao vivo e outros canais utilizados para suporte ao cliente e comunicações urgentes.
- **Equipamentos de Monitoramento Remoto:** Dispositivos IoT utilizados para coletar dados de saúde (ex: monitores de pressão arterial, termômetros, monitores de glicose).
- **Equipe de Desenvolvimento e Suporte Técnico:** Profissionais responsáveis por manter, atualizar e resolver incidentes técnicos na plataforma.
- **Sistemas de Processamento de Pagamentos:** Plataforma para processamento de pagamentos e cobranças de consultas e serviços.

3. Análise de Impacto nos Negócios

A análise de impacto no negócio identifica os eventos disruptivos que podem afetar os recursos críticos e analisa o impacto potencial de cada um. Abaixo estão os principais riscos:

1. Ataque Cibernético :

- **Impacto:** Acesso não autorizado a dados sensíveis de pacientes, criptografia de dados, ou interrupção do serviço devido à falha de sistemas.
- **Impacto Financeiro:** Perda de receita devido a interrupção dos serviços, custos de recuperação e possíveis multas regulatórias (violação de leis de privacidade de dados).
- **Impacto Operacional:** Necessidade de tempo e recursos significativos para restaurar os sistemas afetados e garantir a segurança dos dados.

2. Falha de TI :

- **Impacto:** Interrupção dos serviços essenciais, como consultas médicas online e acesso a registros de pacientes.
- **Impacto Financeiro:** Perda de receita devido à inatividade dos serviços e possíveis contratos cancelados.
- **Impacto Operacional:** A equipe de TI precisará trabalhar rapidamente para identificar a causa e restaurar os serviços.

3. Desastre Natural :

- **Impacto:** Danos físicos aos data centers locais ou interrupção do fornecimento de energia e conectividade.

- **Impacto Financeiro:** Custos elevados com reparos e recuperação, além de tempo de inatividade dos serviços.
- **Impacto Operacional:** Paralisação das operações até que a infraestrutura seja restaurada ou as cópias de segurança sejam acessadas.

4. Falha de Provedor de Nuvem :

- **Impacto:** A empresa pode perder acesso aos seus servidores ou dados armazenados na nuvem, resultando na interrupção dos serviços.
- **Impacto Financeiro:** Potencial perda de receita enquanto os serviços estão fora do ar.
- **Impacto Operacional:** Necessidade de redirecionar para sistemas de backup ou outra plataforma de nuvem temporariamente.

- 5. Problemas de Recursos Humanos :
- **Impacto:** Falta de pessoal para suportar a plataforma ou atender os pacientes, resultando em atrasos e insatisfação do cliente.
- **Impacto Financeiro:** Custos adicionais para contratar temporários ou serviços externos.
- **Impacto Operacional:** A equipe precisa ser redirecionada para garantir a continuidade do serviço, afetando o desenvolvimento de novos recursos.

4. Estratégias de Recuperação

1. Redundância de Sistemas e Infraestrutura:

- **Redundância Geográfica:** Distribuição dos dados e aplicações em diferentes regiões de nuvem para garantir que se uma falha ocorrer em uma região, os serviços possam ser rapidamente restaurados a partir de outra região.
- **Serviços de Backup em Nuvem:** Implementação de backups diários em provedores de nuvem diferentes para garantir a continuidade dos dados.

2. Estratégias de Backup de Dados:

- **Backup Completo e Incremental:** Realizar backups completos semanalmente e backups incrementais diários, garantindo que os dados sejam preservados e possam ser rapidamente restaurados.

- **Armazenamento Offline:** Manter backups offline em dispositivos físicos seguros, além de backups em nuvem, para evitar a perda de dados durante um ataque cibernético.

3. Plano de Recuperação de Desastres (DRP):

- **Plano de Recuperação Imediata:** Em caso de falha de sistema, os dados e sistemas devem ser restaurados rapidamente a partir dos backups mais recentes.
- **Deslocamento para Sistemas de Backup:** Caso o provedor de nuvem falhe, a empresa pode mover os serviços críticos para uma plataforma de nuvem secundária.

4. Plano de Comunicação de Emergência:

- **Comunicação Interna:** Comunicação imediata com todos os funcionários e parceiros sobre o incidente, incluindo as medidas que estão sendo tomadas.
- **Comunicação com Clientes:** Enviar atualizações contínuas aos clientes sobre o status do serviço e o tempo estimado para a recuperação.

5. Plano de Ação Detalhado

1. **Identificação do Problema:**
    a. Assim que um incidente é detectado, a equipe de TI e segurança deve ser acionada para investigar a causa do problema.
2. **Ativação do Plano de Recuperação:**
    a. Caso a interrupção seja crítica (falha de servidores, ataque cibernético), a equipe de recuperação de desastres deve ser ativada.
3. **Recuperação de Dados e Sistemas:**
    a. A partir dos backups mais recentes, os dados devem ser restaurados em servidores alternativos ou novos servidores em nuvem.
4. **Recuperação Operacional:**
    a. A equipe médica e de suporte deve ser realocada para garantir que as consultas possam ser realizadas, mesmo que com recursos limitados.
5. **Monitoramento Contínuo:**
    a. Durante a recuperação, a equipe de TI deve monitorar constantemente os sistemas para garantir que não haja novas falhas.
6. **Verificação de Sistema e Validação:**
    a. Após a recuperação, a funcionalidade do sistema deve ser testada para garantir que os serviços estejam operando normalmente.

6. Sugestão de Teste do Plano

Simulação de Cenário de Crise:

- **Cenário:** Simular uma falha de provedor de nuvem, onde todos os serviços e dados críticos ficam inacessíveis. A equipe de TI deverá ativar o plano de recuperação, restaurando dados a partir de backups e movendo os sistemas para uma nuvem alternativa.
- **Objetivo:** Avaliar a capacidade da equipe de reagir a falhas em tempo real, a eficácia do backup e a velocidade de recuperação dos serviços.
- **Frequência:** Realizar simulações semestrais para garantir que o plano seja atualizado e funcional.