Atividade Proposta para aula e entrega para a próxima semana

• Elaboração de um Plano de Continuidade de Negócios – BCP

Plano de Continuidade de Negócios – Tech4Health

---

1. Introdução da Empresa e Cenário

Descrição Geral:
Tech4Health é uma startup de tecnologia voltada para a saúde, que proporciona soluções de telemedicina e armazenamento de dados médicos em nuvem. Fundada em 2021, a empresa rapidamente se tornou uma parceira confiável para clínicas e hospitais que utilizam o sistema tanto para consultas remotas quanto para o armazenamento seguro de informações médicas dos pacientes.

Missão e Importância do BCP:
A missão da Tech4Health é garantir que serviços médicos estejam acessíveis, seguros e disponíveis 24/7. Um plano de continuidade de negócios é crítico para evitar interrupções nos serviços de atendimento e garantir que a empresa esteja preparada para responder de forma rápida e eficaz a qualquer incidente que possa comprometer a integridade, disponibilidade e confidencialidade dos dados médicos.

2. Identificação dos Recursos Críticos

A continuidade das operações depende dos seguintes recursos, que foram identificados e classificados como críticos:

- **Infraestrutura de TI e Conectividade**
    - **Servidores em Nuvem e Locais: Responsáveis por hospedar o sistema de telemedicina e o banco de dados de informações médicas.**
    - **Serviços de Rede e Conectividade: Internet de alta velocidade para conexões estáveis e suporte a consultas online.**
    - **Firewalls e Ferramentas de Segurança: Protegem contra invasões e acesso não autorizado.**
- **Plataforma de Telemedicina**
    - **Software de Consulta Médica Online: Interface que conecta médicos e pacientes com suporte de vídeo, chat e registro de dados.**
    - **API de Integração com Sistemas de Saúde: Permite a comunicação entre o software de telemedicina e sistemas de clínicas e hospitais parceiros.**

- **Armazenamento e Segurança de Dados**
    - **Banco de Dados Criptografado: Armazenamento seguro de dados de saúde.**
    - **Backups Diários e Semanais: Garantia de cópias atualizadas dos dados para pronta recuperação.**
- **Protocolos de Comunicação Interna e Externa**
    - **Sistema de Mensagens e E-mail Corporativo: Canal para comunicações internas e com clientes.**
    - **Hotline de Atendimento ao Cliente: Linha de apoio aos usuários em caso de problemas técnicos.**
- **3. Análise de Impacto nos Negócios (BIA)**

A Análise de Impacto nos Negócios (BIA) identifica eventos disruptivos e mensura seus impactos. Para Tech4Health, os cenários disruptivos podem impactar de forma significativa a segurança dos dados, a continuidade do atendimento e o relacionamento com parceiros e clientes.

Eventos Disruptivos e Impactos

Evento	Impacto	Descrição	Consequências
• Falha no Servidor de Dados	• Alto	• Interrupção no acesso a dados médicos e a plataforma de consultas	• Cancelamento de consultas, risco à saúde dos pacientes e insatisfação de clientes
• Ataque Cibernético (ex.: ransomware)	• Muito Alto	• Acesso indevido a dados médicos e sigilosos	• Perda de confiança, problemas legais, violação de dados médicos
• Desastres Naturais (incêndios, inundações)	• Alto	• Danos à infraestrutura física e aos servidores locais	• Interrupção nas operações, perda de equipamentos críticos
• Falha de Energia Elétrica	• Médio	• Desligamento de servidores e equipamentos	• Interrupção temporária do serviço, possíveis danos ao equipamento

• Problema de Conectividade de Internet	• Médio	• Conexão instável ou interrompida durante consultas	Consultas canceladas, perda de receita e insatisfação de clientes

4. Estratégias de Recuperação Propostas

Para cada cenário identificado, estratégias de recuperação foram planejadas para mitigar os riscos e garantir a continuidade das operações.

- **Redundância de Sistemas e Backup**
  - **Servidores em Localizações Diferenciadas: Utilização de data centers em múltiplas regiões geográficas.**
  - **Backups Automatizados: Backups diários e semanais, armazenados em local seguro e criptografado para pronta recuperação.**

- **Segurança Cibernética e Resposta a Incidentes**
  - **Política de Segurança Rígida: Implementação de firewalls, antivírus e autenticação multifatorial.**
  - **Monitoramento 24/7 e Testes Regulares de Vulnerabilidades: Equipe especializada em segurança cibernética para identificar ameaças e responder rapidamente.**

- **Plano de Comunicação de Crise**
  - **Linha de Comunicação Emergencial com Clientes: Notificação rápida para os clientes em caso de interrupções nos serviços.**
  - **Treinamento Contínuo de Equipe: Programas de capacitação para que todos os colaboradores saibam agir em situações de crise.**

- **Energia de Emergência e Provedores Alternativos de Internet**
  - **Geradores e Fontes de Energia Alternativas: Mantêm a continuidade do sistema em caso de queda de energia.**
  - **Internet Secundária com Failover Automático: Provedor de internet alternativo para garantir que as consultas não sejam interrompidas.**

5. Plano de Ação Detalhado

O plano de ação define as atividades, responsáveis e prazos específicos para respostas e recuperação dos serviços:

Etapa	Descrição	Prazo	Responsável	Recursos Necessários
1. Implementação de Backup em Nuvem	Configuração de backups em nuvem com failover automático	2 semanas	Equipe de TI	Servidores na nuvem, software de backup
2. Fortalecimento da Segurança	Atualização dos sistemas de segurança, firewall e autenticação multifatorial	1 mês	TI e Segurança	Firewall atualizado, softwares de autenticação
3. Criação de Documentação e Treinamento para Incidentes	Documentação do BCP e treinamento dos colaboradores	3 semanas	RH e TI	Guias, manuais, agenda de treinamento
4. Simulação de Falhas	Teste das estratégias de recuperação em ambiente controlado	Semestral	Equipe de Gerenciamento de Riscos	Recursos de TI, agenda para simulação

6. Sugestão de Teste do Plano

Para garantir a eficácia do BCP, a Tech4Health adotará uma abordagem prática com testes e simulações de cenários.

Proposta de Teste do Plano:

1. **Simulação de Falha de Servidor e Backup:**
   - **Descrição: Desligar o servidor principal em um ambiente controlado, verificando o tempo de ativação do servidor de backup.**
   - **Objetivo: Avaliar a funcionalidade do servidor secundário e o tempo de resposta da equipe.**
   - **Métricas: Medição do tempo de recuperação e análise de possíveis pontos de melhoria.**
2. **Teste de Resposta a Ataque Cibernético (Simulação de Ransomware):**
   - **Descrição: Simulação de ataque de ransomware para avaliar a eficácia do sistema de backup e a resposta da equipe.**
   - **Objetivo: Garantir a integridade dos dados e validar o tempo de resposta dos colaboradores.**

- **Métricas: Tempo de resposta, eficácia das camadas de proteção e plano de mitigação de danos.**

3. **Simulação de Queda de Energia e Backup de Internet:**
   - **Descrição: Simular um corte de energia e verificar o tempo de ativação do gerador, além de testar o failover da internet.**
   - **Objetivo: Validar o tempo de recuperação de energia e internet secundária para garantir a continuidade dos serviços.**
   - **Métricas: Tempo de ativação do gerador e failover da internet.**

Angelo Rodrigues 824139676

Cauã de Cerqueira Ferreira 824110637

Wellington de Oliveira Sousa 824144581

Erick Domingues Soares 82414486