UC – Sistemas Computacionais e Segurança – Atividade 08

Integrantes:

Nicholas – RA : 824139657
Tobias – RA : 824126059
Wendel – RA : 824212260

DATA FLOW

A **DataFlow** é uma startup de tecnologia fundada em 2022, especializada em soluções de análise de dados na nuvem. A empresa oferece uma plataforma acessível e intuitiva que permite que pequenas e médias empresas armazenem, analisem e visualizem seus dados em tempo real, sem a necessidade de infraestrutura complexa.

Identificação dos Recursos Críticos

- **Infraestrutura de Nuvem**
- Servidores e bancos de dados em nuvem (ex.: AWS, Google Cloud) para armazenamento, processamento e segurança dos dados dos clientes.
- Sistemas de backup em múltiplas regiões para recuperação rápida em caso de falha.
- **Sistemas de Análise de Dados**

- Plataforma de análise que coleta e processa dados em tempo real, composta por algoritmos e scripts essenciais para a entrega de resultados.
- **Equipe Técnica e de Desenvolvimento**
- Desenvolvedores e engenheiros de dados responsáveis pela manutenção e atualização da plataforma e pela resposta a emergências.
- **Equipe de Atendimento ao Cliente**
- Equipe de suporte que auxilia os clientes na resolução de problemas técnicos, garantindo o relacionamento com o cliente durante crises.
- **Dados dos Clientes** Informações confidenciais e registros dos clientes, que precisam de armazenamento seguro e acessibilidade em situações críticas.

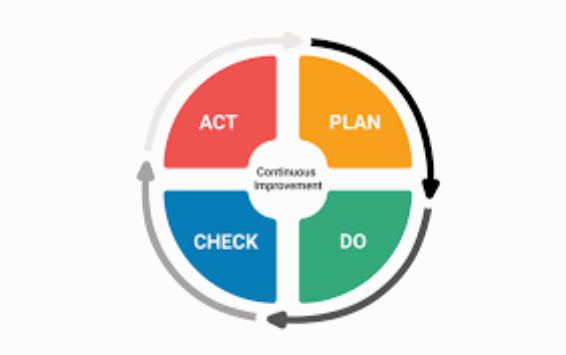
Análise de Impacto nos Negócios (BIA)

Eventos Disruptivos e Impactos:

- **Falha no Provedor de Nuvem**
  - **Impacto**: Inacessibilidade total da plataforma, interrupção no serviço aos clientes e risco de perda de dados.
  - **Consequências**: Perda financeira, diminuição da confiança dos clientes e possíveis multas por violações contratuais.
- **Ataque Cibernético**
  - **Impacto**: Exposição de dados confidenciais, interrupção nos serviços e danos à segurança dos sistemas.
  - **Consequências**: Comprometimento da privacidade dos dados dos clientes, danos à imagem da empresa e custos com recuperação e segurança.
- **Erro Humano em Processos Internos**
  - **Impacto**: Problemas na plataforma, como bugs críticos, degradação de performance e possíveis indisponibilidades.
  - **Consequências**: Impacto na experiência do usuário, custos de correção e perda de produtividade.
- **Desastres Naturais**
  - **Impacto**: Danos ao escritório físico e interrupções na comunicação e coordenação da equipe.
  - **Consequências**: Dificuldades operacionais, necessidade de trabalho remoto forçado e possível atraso na resposta a crises.

Estratégias de Recuperação

1. **Redundância de Sistemas e Backup**
   - Utilizar infraestrutura em nuvem com múltiplas zonas de disponibilidade e backup automático dos dados em diferentes regiões geográficas.
2. **Plano de Recuperação de Desastres**
   - Implementar um plano de recuperação para desastres, incluindo servidores redundantes e canais de comunicação remotos.
3. **Plano de Comunicação em Caso de Emergência**
   - Preparar uma comunicação oficial para clientes e parceiros, orientando sobre o problema e o tempo estimado de recuperação.
4. **Treinamento de Segurança Cibernética e Prevenção de Erros Humanos**
   - Capacitar a equipe sobre boas práticas de segurança cibernética e realizar revisões de código e processos para minimizar falhas humanas.



Plano de Ação

Etapas de Resposta e Recuperação:

1. **Detecção e Diagnóstico Rápido**:
   - **Responsável**: Equipe de TI e segurança.
   - **Prazos**: Imediato (tempo estimado de 30 minutos para diagnóstico inicial).
2. **Comunicação e Notificação**:
   - **Responsável**: Equipe de Atendimento ao Cliente.
   - **Prazos**: Dentro de 1 hora do evento para notificação aos clientes.
3. **Implementação das Soluções de Recuperação**:
   - **Responsável**: Desenvolvedores e equipe técnica.
   - **Prazos**: Dentro de 3 a 6 horas para falhas menores; até 24 horas para incidentes de segurança maiores.

4. **Monitoramento e Avaliação Pós-Recuperação**:
    - **Responsável**: Equipe de TI e desenvolvimento.
    - **Prazos**: Monitoramento contínuo nas primeiras 48 horas após a recuperação.

5. Teste do Plano

1. **Simulação de Ataque Cibernético**
    - Realizar uma simulação de ataque para testar a resposta de segurança, identificando o tempo de resposta e a eficácia das medidas.
2. **Teste de Falha de Infraestrutura**
    - Simular uma falha de servidor na nuvem para avaliar o processo de backup e recuperação de dados.
3. **Treinamento em Cenário de Crise**
    - Executar treinamentos semestrais com a equipe, recriando cenários disruptivos e avaliando o desempenho na execução do plano.

6. Sugestão de Teste do Plano de Continuidade de Negócios (BCP)

1. Simulação de Ataque Cibernético

- **Objetivo**: Testar a resposta da equipe a um ataque cibernético simulado.
- **Descrição do Teste**: Criar um cenário onde um ataque cibernético é comunicado, incluindo mensagens de alerta e bloqueio de acessos.
- **Duração**: 2 a 4 horas.
- **Avaliação**: Medir o tempo de resposta, a eficácia da comunicação interna e a execução do plano de resposta.

2. Teste de Falha de Infraestrutura

- **Objetivo**: Avaliar a capacidade de resposta em caso de falha nos serviços de nuvem.
- **Descrição do Teste**: Simular a interrupção dos serviços de nuvem e a equipe deve realizar a recuperação dos dados a partir de backups.
- **Duração**: 4 a 6 horas.
- **Avaliação**: Observar a capacidade de recuperação e o tempo necessário para restaurar os serviços.

3. Exercício de Trabalho em Equipe em Cenário de Crise

- **Objetivo**: Testar a coordenação e comunicação durante uma crise.
- **Descrição do Teste**: Criar um cenário com múltiplos eventos simultâneos (ex.: falha do servidor e ataque cibernético) para colaboração na resolução de problemas.
- **Duração**: 3 a 5 horas.
- **Avaliação**: Avaliar a eficácia da comunicação entre as equipes e a clareza nas responsabilidades.

4. Revisão do Plano de Ação

- **Objetivo**: Analisar e revisar o plano de continuidade com base em feedback.
- **Descrição do Teste**: Realizar uma reunião após cada simulação para discutir pontos positivos e negativos.
- **Duração**: 1 a 2 horas após cada teste.
- **Avaliação**: Documentar lições aprendidas e atualizar o BCP conforme necessário.

5. Treinamento de Sensibilização e Resiliência

- **Objetivo**: Aumentar a conscientização sobre o plano de continuidade.
- **Descrição do Teste**: Conduzir workshops e sessões de treinamento sobre o BCP e responsabilidades da equipe.
- **Duração**: 1 a 2 horas, programados semestralmente.
- **Avaliação**: Avaliar a compreensão e retenção de informações da equipe por meio de questionários.