**Riscos (Número de Falhas em um Ano)**

* 1: Incidente no Banco de Dados
* 2: Incidente em um Servidor da Aplicação
* 3: Usuário não consegue acessar sua conta
* 4: Outro indivíduo acessa a conta de um usuário
* 5: Incidente com API

**1) Incidente no Banco de Dados**

**Mitigação**

* Planos de Contenção:
* Implementação de diferentes níveis de acesso;
* Autenticação multifator para usuários do BD;
* Manutenção do Hardware para servidores On-Premises.
* Planos de Contingência:
* Manter Backup do servidor atualizado;
* Implementação e manutenção de um servidor de Fallback;
* Criação de um plano de recuperação (Rollback) e capacitação de funcionários.

**Monitoramento**

* Monitoramento de métricas de desempenho (tempo de resposta, utilização de CPU, etc)
* Registro e Auditoria de atividades no BD;
* Notificações automáticas para anomalias no BD (por e-mail ou via canal de chat).
* **Periodicidade: Diária**

**Definição de Prioridade**

* Dados:
* Probabilidade: 0,05
* Impacto: 0,9
* Exposição: 0,045
* **Prioridade: Baixo**

**2) Incidente no Servidor da Aplicação**

**Mitigação**

* Planos de Contenção:
* Controle de acesso ao ambiente de produção
* Versionamento da aplicação
* Planos de Contingência:
* Possuir um servidor de Backup da aplicação
* Utilizar balanceamento de carga para distribuir o tráfego entre vários servidores.
  + Implementar uma arquitetura de alta disponibilidade para os servidores de aplicação.
  + Automatizar a migração de failover para servidores reserva em caso de falha.

**Monitoramento**

* Configurar alertas para detectar anomalias e falhas em tempo real;
* Implementar um plano de manutenção preventiva regular para servidores de aplicação.
* **Periodicidade: Diária**

**Definição de Prioridade**

* Dados
* Probabilidade: 0,05
* Impacto: 1
* Exposição: 0,05
* **Prioridade: Baixa**

**3) Usuário não consegue acessar sua conta**

**Mitigação**

* Planos de Contenção
* Gerenciamento de senhas.
* Planos de Contingência
* Implementação de métodos de recuperação (e-mail, celular, perguntas de segurança);
* Canal de comunicação em caso de falhas na recuperação;
* Redefinição de senha pelo aplicativo.

**Monitoramento**

* **Periodicidade: Em caso de falha total de recuperação**

**Definição de Prioridade**

* Dados
* Probabilidade: 0,3
* Impacto: 0,3
* Exposição: 0,09
* **Prioridade: Baixo**

**4) Outro indivíduo acessa a conta de um usuário**

**Mitigação**

* Planos de Contenção
* Autenticação multifator para usuários da aplicação
* Incentivo à mudança periódica da senha do usuário
* Definição de padrão de criação de senha para desincentivar o ataque (mínimo de caracteres, caracteres especiais,...).
* Planos de Contingência
* Implementação de métodos de recuperação;
* Notificação de atividades suspeitas (tentativa de login em localizações incomuns);
* Bloqueio temporário da conta após múltiplas tentativas de acesso mal-sucedidas.

**Monitoramento**

* **Periodicidade: Em caso de acesso indevido**

**Definição de Prioridade**

* Dados
* Probabilidade: 0,15
* Impacto: 0,6
* Exposição: 0,12
* **Prioridade: Médio**

**5) Incidente com API**

**Mitigação**

* Planos de Contenção
* Documentação de API
* Balanceamento de carga;
* Planos de Contingência
* Atualização de APIs terceiras;
* Notificações automáticas para erros em endpoints;
* Criação de um plano de recuperação (Rollback);

**Monitoramento**

* **Periodicidade: A cada ciclo de desenvolvimento**

**Definição de Prioridade**

* Dados
* Probabilidade: 0,15
* Impacto: 1
* Exposição: 0,15
* **Prioridade: Média**