Instituto Superior de Engenharia do Porto

Relatório Sprint 3

Turma 3DD - Grupo 23

1220879 – Rafael Brandão

Professor:

André Moreira, ASC

Unidade Curricular:

Arquitetura de Sistemas

Índice

User Story 1

Requisitos:

“As the organization's administrator, I want a disaster recovery plan that meets the MBCO defined in sprint B.”

Plano de Recuperação de Desastres (DRP)

1. Visão Geral

Este DRP garante a continuidade dos negócios para funções críticas do sistema hospitalar, atendendo aos requisitos definidos do MBCO. Fornece procedimentos estruturados para recuperação do sistema durante desastres ou interrupções importantes.

2. Prioridades e Procedimentos de Recuperação

2.1 Sistema de Autenticação (Prioridade Máxima)

- RTO: 15 minutos
- Meta de Disponibilidade: 99,99%
- Etapas de Recuperação:
    1. Ativar sistema de autenticação Auth0 redundante.
    2. Verificar *failover* do sistema e resolver inconsistências.
    3. Monitorar métricas de saúde do sistema
    4. Notificar pessoal essencial via sistema de alerta por email

2.2 Sistema de Gestão de Pacientes

- RTO: 30 minutos
- RPO: 5 minutos
- Meta de Disponibilidade: 99,95%
- Etapas de Recuperação:
    1. Iniciar *failover* do banco de dados para o sistema de backup
    2. Restaurar último backup válido dos dados.

3. Verificar a integridade dos registos clínicos.

4. Reativar protocolos de acesso ao sistema para emergências.

2.3 Sistema de Gestão de Operações

- RTO: 1 hora
- RPO: 15 minutos
- Meta de Disponibilidade: 99,95%
- Etapas de Recuperação:

1. Ativar o sistema de agendamento de backup.
2. Sincronizar dados operacionais com o backup mais recente.
3. Verificar o agendamento de operações críticas.
4. Notificar as equipas responsáveis sobre os novos protocolos.

2.4 Sistema de Gestão de Pessoal

- RTO: 2 horas
- RPO: 1 hora
- Meta de Disponibilidade: 99,9%
- Etapas de Recuperação:

1. Restaurar banco de dados de pessoal do backup mais recente.
2. Garantir acesso a informações de licenças e especializações.
3. Validar os direitos de acesso e credenciais de usuários-chave.
4. Reestabelecer o sistema de rastreamento de pessoal essencial.

3. Equipa de Resposta e Responsabilidades

3.1 Equipa de Resposta Primária

- Administrador de Sistema:

1. Avaliação inicial do incidente

2. Coordenação da recuperação do sistema

3. Relatório de status para *stakeholders*

- Administrador de Banco de Dados:

1. Operações de recuperação de banco de dados

2. Verificação de integridade dos dados

3. Gerenciamento do sistema de backup

- Oficial de Segurança:

1. Aplicação de protocolos de segurança

2. Gerenciamento de controle de acesso

3. Documentação de incidentes

3.2 Contactos de Emergência

- Suporte Técnico Geral: [Inserir contacto]

- Suporte Auth0: [Inserir contacto]

- Suporte Banco de Dados: [Inserir contacto]

4. Procedimentos Técnicos de Recuperação

4.1 Recuperação de Infraestrutura

- Sistemas de Servidor:

1. Ativar servidores primários/redundantes.

2. Verificar conectividade da rede.

3. Monitorar o desempenho dos sistemas secundários.

- Banco de Dados:

1. Executar *failover* e restaurar dados críticos.

2. Testar consistência do banco de dados antes de qualquer operação.

4.2 Monitoramento e Alertas

- Monitoramento do Sistema:

1. Verificar métricas de saúde do sistema

2. Monitorar disponibilidade do serviço

3. Acompanhar progresso da recuperação

- Gestão de Alertas:

1. Notificar os administradores sobre o *status* do incidente.

2. Atualizar a *dashboard* dos *stakeholders* consoante a recuperação dos sistemas.

3. Documentar a linha do tempo do incidente.

5. Testes e Manutenção

5.1 Cronograma de Testes

- Mensalmente: Verificação de backups e testes de recuperação de arquivos.

- Trimestralmente: Testes de *failover* de servidores e sistemas.

- Semestralmente: Simulação de recuperação completa de funções críticas.

5.2 Manutenção do Plano

- Realizar revisões trimestrais do plano.

- Atualizar após mudanças significativas no sistema, como upgrades ou migrações.

- Documentar resultados dos testes e implementar as melhorias necessárias.

6. *Checklist* de Validação da Recuperação

[ ] Sistema de autenticação operacional.

[ ] Dados de pacientes acessíveis e atualizados.

[ ] Sistema de agendamento funcional.

[ ] Banco de dados de pessoal acessível e atualizado.

[ ] Protocolos de segurança e controlo de acesso ativos.

[ ] Todos os serviços críticos atendem ao MBCO.

[ ] Sistemas de monitoramento estáveis.

7. Medidas de Mitigação e Melhoria Contínua

- Automatização: Implementar scripts para *failover* automático e notificações de incidentes.

- Redundância: Expandir a infraestrutura para redundância geográfica.

- Capacitação: Treinar continuamente a equipa para lidar com acidentes críticos.

- Auditoria: Realizar auditorias regulares para garantir conformidade com normas e as melhores práticas.

User story 4

Requisitos: *Como administrador de sistemas quero que utilizando o Backup elaborado na US C3, seja criado um script quer faça a gestão dos ficheiros resultantes desse backup, no seguinte calendário. 1 Backup por mês no último ano, 1 backup por semana no último mês, 1 backup por dia na última semana.*

Assumindo que cada backup será guardado numa pasta, no script seguinte procedemos à gestão dos backups através de um ciclo que percorre cada backup e analisa os seus dados. Caso estes não correspondam ao pedido, a pasta que o contém será eliminada.

```bash
#!/bin/bash

folder_path="/root/bin/testbackups"
mysql_folder_path="/root/bin/mysqlbackups"
log_file="/root/checker_logs.log"

# Função para verificar se uma pasta segue os critérios especificados
check_folder() {
    local folder_name=$1
    local test=0

    # Extrair a parte da data
    date_part=${folder_name#test_}

    # Verificar se é o primeiro dia do mês
    if [ "$(date -d "$date_part" +%d)" -eq 28 ]; then
        echo "Pasta '$folder_name' é um backup para o dia 28 do mês. Mantendo-a." >> "$log_file"
        ((test++))
    fi
    # Verificar se é o mês de dezembro e é o primeiro dia da semana
    if [ "$(date -d "$date_part" +%m)" -eq 12 ] && [ "$(date -d "$date_part" +%u)" -eq 1 ]; then
        echo "Pasta '$folder_name' é um backup para o primeiro dia de dezembro. Mantendo-a." >> "$log_file"
        ((test++))
    fi
    # Verificar se é a última semana do ano
    if [ "$(date -d "$date_part" +%W)" -eq 52 ]; then
        echo "Pasta '$folder_name' é um backup para a última semana do ano. Mantendo-a." >> "$log_file"
        ((test++))
    fi
    if [ $test -eq 0 ]; then
        echo "A eliminar a pasta '$folder_name' porque não segue os critérios especificados." >> "$log_file"
        rm -rf "$folder_path/$folder_name"
    fi
}
```

```bash
# Função para verificar se um ficheiro SQL segue os critérios especificados
check_sql_file() {
    local file_name=$1
    local test2=0

    # Extract the date
    date_part=${file_name#sem5_pi_}
    date_part=${date_part%.sql}

    # Verificar se é o primeiro dia do mês
    if [ "$(date -d "$date_part" +%d)" -eq 28 ]; then
        echo "Ficheiro '$file_name' é um backup para o dia 28 do mês. Mantendo-o." >> "$log_file"
        ((test2++))
    fi
    # Verificar se é o mês de dezembro e é o primeiro dia da semana
    if [ "$(date -d "$date_part" +%m)" -eq 12 ] && [ "$(date -d "$date_part" +%u)" -eq 1 ]; then
        echo "Ficheiro '$file_name' é um backup para o primeiro dia de dezembro. Mantendo-o." >> "$log_file"
        ((test2++))
    fi
    # Verificar se é a última semana do ano
    if [ "$(date -d "$date_part" +%W)" -eq 52 ]; then
        echo "Ficheiro '$file_name' é um backup para a última semana do ano. Mantendo-o." >> "$log_file"
        ((test2++))
    fi
    if [ $test2 -eq 0 ]; then
        echo "A eliminar o ficheiro '$file_name' porque não segue os critérios especificados." >> "$log_file"
        rm -rf "$mysql_folder_path/$file_name"
    fi
}
```

```
# Verificar se a pasta de backup existe
if [ -d "$folder_path" ]; then
    echo "A verificar pastas em $folder_path..."

    # Percorrer cada pasta no caminho especificado
    for subfolder in "$folder_path"/*; do
        # Extrair o nome
        folder_name=$(basename "$subfolder")

        # Verificar contra os critérios
        check_folder "$folder_name"
    done
else
    echo "Erro: A pasta $folder_path não existe."
fi

# Verificar se a pasta de backup do MySQL existe
if [ -d "$mysql_folder_path" ]; then
    echo "A verificar ficheiros em $mysql_folder_path..."

    # Percorrer cada ficheiro SQL no caminho especificado
    for sql_file in "$mysql_folder_path"/*.sql; do
        # Extrair o nome do ficheiro
        file_name=$(basename "$sql_file")

        # Verificar o ficheiro contra os critérios
        check_sql_file "$file_name"
    done
else
    echo "Erro: A pasta $mysql_folder_path não existe."
fi
```

User story 7

Requisitos: *"Como administrador da organização quero que me seja apresentado um BIA (Business Impact Analysis) da solução final, adaptando-se onde aplicável o(s) risco(s) identificados no sprint anterior."*

BIA da Solução de Armazenamento em Nuvem

1. Introdução

O objetivo desta análise é identificar a criticidade das operações do sistema de armazenamento na nuvem, avaliar os riscos e interrupções associados, e determinar os objetivos de tempo de recuperação (RTO) e ponto de recuperação (RPO). As vulnerabilidades identificadas no sprint anterior são consideradas nesta análise, com estratégias propostas para mitigação

2. Identificação de Vulnerabilidades e Impactos

Vulnerabilidade	Impacto Potencial	Exemplo Real

Falta de Controlo de Acessos Adequados (US2/US3)	Acessos não autorizados, manipulação ou eliminação de dados sensíveis.	Um utilizador mal-intencionado acede a dados confidenciais.
Vulnerabilidades na Criptografia	Exposição de dados confidenciais e possível manipulação de informações.	Algoritmos de criptografia fracos ou chaves comprometidas.
Falta de Monitorização e Resposta a Incidentes	Ataques prolongados sem deteção, resultando em danos.	Malware não detetado a operar durante semanas.

3. Probabilidade e Criticidade

Risco	**Probabilidade**	**Impacto**	**Criticidade**
Controlo de Acesso Inadequado	Média-Alta	Médio-Alto	Alta
Vulnerabilidades na Criptografia	Média	Alto	Alta
Monitoramento Insuficiente	Média	Médio-Alto	Média

4. RTO e RPO para Sistemas e Processos Críticos

Componente	**RTO (Tempo Máx. Aceitável)**	**RPO (Ponto Máx. de Recuperação)**	**Justificação**
Controlo de Acessos	15 minutos	5 minutos	Minimizar acessos não autorizados em tempo real.
Criptografia de Dados	1 hora	0 minutos	Dados confidenciais não podem ser perdidos ou expostos.
Monitorização e Resposta a Incidentes	1 hora	15 minutos	Detetar e mitigar ameaças rapidamente para reduzir o impacto.

5. Recursos Necessários

Área de Risco	**Recurso Técnico**	**Recurso Humano**

Controlo de Acesso	Autenticação multifator (MFA); ferramentas de auditoria automatizada.	Administrador de segurança para auditorias e revisão de permissões.
Criptografia	Algoritmos como AES-256; HSMs; ferramentas de gestão de chaves automatizadas.	Especialista em criptografia para auditorias e resposta a incidentes.
Monitorização e Resposta	Ferramentas SIEM; sistemas de alerta.	Analistas de SOC para análise de registos.

6. Estratégias de Mitigação

Vulnerabilidade	**Medidas de Mitigação**
Falta de Controlo de Acessos	Implementar MFA, realizar auditorias regulares, e aplicar o princípio do menor privilégio.
Vulnerabilidades na Criptografia	Utilizar algoritmos fortes, gerir chaves de forma segura, e implementar criptografia de ponta a ponta.
Falta de Monitorização e Resposta	Configurar sistemas SIEM, criar playbooks de resposta e realizar formações regulares para a equipa de TI.

7. Recuperação e Continuidade

Componente Crítico	**Plano de Recuperação**
Controlo de Acessos	Ativar MFA e políticas de emergência; bloquear utilizadores suspeitos; automatizar a deteção de permissões incorretas.
Criptografia	Reconfigurar sistemas para usar algoritmos seguros e restaurar chaves comprometidas a partir de backups.
Monitorização	Analisar registos históricos, identificar anomalias e reativar ferramentas de monitorização com ajustes necessários.

8. Conclusão

Este BIA organiza os riscos, impactos e estratégias de mitigação de forma estruturada, permitindo à organização uma resposta rápida e eficaz em caso de

interrupções. A implementação destas medidas garantirá a continuidade operacional e a proteção dos ativos mais críticos.