CLOUD COMPUTING

Atividade Prática: Planejamento Estratégico de Migração para a Nuvem

Nome: Erick Barbara de Araújo RA: 336356

Nome: Thamara da Silva Sousa RA: 309814

Nome: Vitor Da Silva Bezerra RA: 336459

Nome:Wallace Santos Ribeiro RA: 309767

Contexto: Uma empresa de médio porte deseja migrar seus dados e sistemas para a nuvem com o objetivo de modernizar sua infraestrutura de TI, reduzir custos operacionais e aumentar a escalabilidade dos serviços. A diretoria solicitou um plano de migração estruturado e uma análise comparativa entre os principais provedores de serviço em nuvem (CSPs) para tomar uma decisão embasada.

CSP (Cloud Service Provider): sigla utilizada para designar os provedores de serviços em nuvem, como AWS, Microsoft Azure e Google Cloud Platform.

Objetivo da atividade: Assumindo o papel de analista de TI da empresa, elabore uma proposta técnica que contemple as seguintes etapas:

ÍNDICE

1. Avaliação da infraestrutura atual e levantamento de workloads.

Empresa: **Centro Hospitalar União**
Localização: São Paulo.

Resumo do levantamento da infraestrutura atual:

Durante o período de 5 a 9 de maio, foi realizada uma vistoria completa na infraestrutura de Tecnologia da Informação (TI) do Centro Hospitalar União, com foco principal em identificar causas relacionadas à lentidão dos equipamentos, instabilidade na rede de internet e perda de dados no sistema de atendimento aos pacientes.

- **Computadores**:
  Foram inspecionados 15 consultórios, e em todos os computadores (HP) avaliados foi constatado mau estado de conservação e uso. A análise técnica indicou os seguintes fatores como principais causas da lentidão relatada:
  • Acúmulo excessivo de sujeira e poeira interna nos equipamentos, comprometendo o desempenho e a refrigeração adequada dos componentes;
  • Presença de discos rígidos (HDDs) obsoletos, que contribuem para o baixo desempenho dos sistemas operacionais;
  • Ausência de manutenção preventiva e corretiva nos dispositivos. Recomenda-se, como ação imediata, a substituição dos HDDs por unidades de estado sólido (SSDs) e a realização de limpeza interna regular nos equipamentos.

- **Infraestrutura de Rede**:
  A avaliação da rede foi realizada na casa de máquinas (sala técnica do hospital), onde foi possível identificar problemas estruturais:
  • Os cabos de rede conectados ao patch panel não estão devidamente identificados ou organizados, dificultando manutenções e diagnósticos futuros;
  • Foi detectado o uso de uma única conexão com a internet, fornecida pela operadora VIVO, aparentemente compartilhada por todo o hospital, o que pode estar gerando gargalos, especialmente em horários de pico;
  • Não há redundância de link ou segregação de rede por setores, o que compromete a estabilidade e segurança da infraestrutura.

- **Sistema de Atendimento**:
  O sistema utilizado por médicos e funcionários apresenta sérias limitações:
  • Falta de atualizações regulares e suporte técnico reduzido;
  • Ocorrência de perda de dados de pacientes, o que representa um risco significativo à operação e à segurança da informação;
  • Instabilidade e lentidão acentuadas durante horários de alta demanda, possivelmente devido à arquitetura defasada do sistema e à infraestrutura de rede inadequada.

2. Definição do escopo e objetivos da migração.

A vistoria evidenciou a necessidade urgente de melhorias na infraestrutura de TI do Centro Hospitalar União. Recomenda-se a elaboração de um plano de ação abrangente que contemple:

• **Atualização dos equipamentos de informática**:
O upgrade para modelos novos com SSD e 16gb de RAM iram trazer maior agilidade para o atendimento médico, reduzindo o tempo de atraso gerado pelo carregamento de processos no PC;

• **Reestruturação e organização do cabeamento de rede**: O mapeamento correto dos cabos de rede facilitará possíveis manutenções futuras e facilitará a identificação dos equipamentos conectados na rede.

• **Avaliação de alternativas para redundância e melhoria da banda larga**: A implementação de duas redes separadas garantirá maior segurança e diminuição da instabilidade, proporcionando uma queda de 80% nos incidentes relatados.

• **Substituição ou atualização do sistema de atendimento com foco em segurança, suporte técnico e escalabilidade**: A troca do sistema atual de atendimento para novos sistemas com maior credibilidade de mercado gerará melhor autonomia e armazenamento escalável durante a utilização para atendimento e trabalho.

3. Escolha do Modelo de Nuvem (Pública, Privada ou Híbrida) e justificativa

A escolha do modelo de computação em nuvem para a instituição em questão é a nuvem híbrida, por apresentar uma solução equilibrada entre segurança, desempenho e custo. Essa escolha se baseia nos seguintes aspectos:

- **Segurança e conformidade**: Considerando o tratamento de dados sensíveis, a nuvem híbrida permite que essas informações sejam armazenadas em ambiente de nuvem privada, o que proporciona maior controle sobre criptografia, acesso e conformidade com legislações vigentes, como a Lei Geral de Proteção de Dados(LGPD).

- **Custo-benefício**: Aplicações de menor criticidade, como sistemas administrativos e comunicação institucional, podem ser hospedadas em nuvem pública, o que contribui para a redução de custos operacionais. O modelo híbrido permite, assim, um equilíbrio eficiente entre custo e desempenho.

- **Escalabilidade**: A nuvem híbrida oferece a possibilidade de expansão de recursos sob demanda, utilizando a flexibilidade da nuvem pública para atender a períodos de alta demanda, sem comprometer a estabilidade dos serviços.

- **Continuidade de negócios**: A adoção do modelo híbrido possibilita a configuração de ambientes de recuperação de desastres e estratégias de backup em múltiplas plataformas, garantindo maior resiliência e continuidade dos serviços prestados pela instituição.

Em síntese, a nuvem híbrida reúne os principais benefícios dos modelos público e privado, oferecendo segurança e conformidade para o tratamento de dados sensíveis, ao mesmo tempo em que proporciona flexibilidade e economia para aplicações de menor criticidade. Por esses motivos, trata-se da alternativa mais adequada para o ambiente hospitalar.

4. Definição da Estratégia de Migração por Sistema com Base nos 6 R's da Migração

Com base na escolha do modelo de nuvem híbrida para a instituição hospitalar, define-se a seguinte estratégia de migração utilizando as abordagens conhecidas como os 6 R's da migração para a nuvem. A seleção das abordagens considera o tipo de sistema, sua criticidade, sensibilidade dos dados e viabilidade técnica de migração.

Rehost (Lift-and-Shift):
Esta abordagem será aplicada a sistemas legados estáveis, mas que não demandam customizações específicas para operarem em ambiente de nuvem. Exemplos incluem servidores de arquivos ou sistemas administrativos. A migração será feita com o mínimo de alterações, visando agilidade e continuidade operacional.

Replatform:
Será utilizada em aplicações que, embora estáveis, podem se beneficiar de ajustes mínimos para utilização de recursos gerenciados da nuvem, como bancos de dados, serviços de balanceamento de carga ou armazenamento escalável. Um exemplo é a migração de sistemas de agendamento para plataformas com banco de dados como serviço (DbaaS).

Refactor (ou Rearchitect):
Aplicações críticas, como o sistema de prontuário eletrônico do paciente (PEP), poderão ser parcialmente reescritas ou remodeladas, com o objetivo de aproveitar arquiteturas mais modernas e escaláveis, como microsserviços. Essa abordagem permitirá maior performance, disponibilidade e integração com demais sistemas da instituição.

Repurchase:
Será considerada para sistemas comerciais que possam ser substituídos por soluções SaaS (Software as a Service), reduzindo a complexidade da gestão de infraestrutura e possibilitando atualizações contínuas. Um exemplo seria a substituição de softwares de gestão de RH por soluções SaaS já consolidadas no mercado.

Retire:
Durante o processo de levantamento de sistemas, serão identificadas aplicações obsoletas ou em desuso, que poderão ser descontinuadas. Isso visa otimizar os recursos de TI e eliminar custos desnecessários com manutenção de sistemas inativos.

Retain:
Algumas aplicações altamente dependentes de infraestrutura local, ou que possuam restrições legais ou técnicas para a migração imediata, serão mantidas no ambiente atual (on-premises). Esses sistemas poderão ser reavaliados futuramente, conforme houver viabilidade para migração ou substituição. Essa estratégia visa garantir uma migração gradual, segura e eficiente, considerando as particularidades de cada sistema, os benefícios oferecidos pela nuvem híbrida e os objetivos estratégicos da instituição.

5. Planejamento da execução (cronograma, migração piloto, testes).

O plano de execução da migração da infraestrutura de TI do Centro Hospitalar União para a nuvem foi cuidadosamente estruturado para garantir uma transição segura, eficiente e com o mínimo impacto sobre as operações médicas e administrativas do hospital. O cronograma da migração foi dividido em quatro fases principais, iniciando com a preparação e análise dos sistemas existentes, seguido por uma migração piloto, depois a migração dos sistemas em larga escala e, por fim, uma etapa dedicada exclusivamente à validação e testes pós-migração.

Fase 1 – Preparação e Planejamento (Semana 1-2):

- Levantamento detalhado dos sistemas e workloads.
- Priorização dos sistemas menos críticos para iniciar a migração.
- Treinamento da equipe envolvida.
- Definição das ferramentas de migração e ambiente de testes.

Fase 2 – Migração Piloto (Semana 3):

- Escolha de um sistema de menor impacto (ex: arquivo de backups ou sistema de registros administrativos).
- Execução da migração em ambiente controlado.
- Testes de desempenho, integridade de dados e resposta do sistema.
- Correção de falhas e ajustes de processos.

Fase 3 – Migração em Larga Escala (Semana 4-6):

- Migração por módulos, priorizando áreas com menor dependência.
- Execução durante janelas de baixo uso (madrugadas ou finais de semana).
- Ordem lógica de migração respeitando a integração entre sistemas (ex: migrar banco de dados antes do sistema de atendimento).

Fase 4 – Testes Pós-Migração (Semana 6-7):

- Testes de integridade de dados.
- Verificação da performance dos sistemas e da comunicação entre módulos.
- Confirmação de acessos e funcionalidades pelos usuários finais.
- Acompanhamento com suporte técnico para ajustes finais.

6. Medidas de segurança e conformidade (LGPD, criptografia, backup).

Considerando que o Centro Hospitalar União lida com dados extremamente sensíveis, como prontuários eletrônicos, exames e informações pessoais de pacientes, é imprescindível adotar medidas rigorosas de segurança e conformidade com a legislação brasileira, especialmente a Lei Geral de Proteção de Dados (LGPD).

• A primeira medida será a identificação dos dados que exigem maior proteção, como informações de saúde e dados pessoais identificáveis. Esses dados serão protegidos por meio de técnicas robustas de criptografia, tanto em repouso (armazenados) quanto em trânsito (durante a comunicação entre sistemas ou transferências para a nuvem). Isso garante que, mesmo em caso de interceptação, os dados não poderão ser lidos ou utilizados por terceiros.

• O provedor de nuvem será escolhido com base em sua conformidade com normas de segurança internacionais e com a LGPD. Serão observados critérios como políticas claras de privacidade, consentimento de uso de dados, retenção segura das informações e possibilidade de exclusão definitiva dos dados mediante solicitação. O provedor também deverá oferecer suporte jurídico e técnico em relação à proteção de dados, facilitando auditorias e relatórios de conformidade.

• Para garantir a disponibilidade e recuperação dos dados, serão implementadas estratégias de backup automatizado. Os backups serão feitos de forma contínua e replicados em diferentes regiões ou zonas de disponibilidade, o que protege a organização contra falhas físicas, ciberataques ou desastres naturais. Além disso, haverá um plano de recuperação de desastres que permitirá restaurar rapidamente os dados e sistemas em caso de incidentes.

• O controle de acesso será outra medida fundamental. Somente usuários autorizados terão acesso aos sistemas e informações confidenciais, e esse acesso será monitorado e gerenciado por meio de políticas de identidade e autenticação multifator (MFA). Isso adiciona uma camada extra de proteção, dificultando o acesso indevido mesmo que credenciais sejam comprometidas.

• O ambiente será submetido a testes periódicos de segurança, como simulações de ataque (testes de penetração) e auditorias técnicas. Essas ações têm o objetivo de identificar vulnerabilidades e manter a conformidade contínua com a LGPD e outras normas de segurança. A política de segurança será revista e atualizada regularmente para acompanhar as melhores práticas e responder rapidamente a novas ameaças.

• Garantir que o ambiente em nuvem siga padrões reconhecidos de segurança da informação, como a norma ISO/IEC 27001, assegurando a proteção dos dados por meio de controles e práticas que previnem acessos não autorizados, perdas e vulnerabilidades.

7. Ações de Capacitação da Equipe e Comunicação Interna e Justificativa da Escolha do Provedor de Nuvem (CSP)

Ações de Capacitação da Equipe e Comunicação Interna

A migração para a nuvem exige uma preparação adequada da equipe e um plano de comunicação eficaz. A seguir, estão as ações essenciais para garantir a capacitação da equipe e a comunicação interna durante o processo.

Identificação das Competências Necessárias

• Times de TI: Capacitação no uso de ferramentas de nuvem (AWS, Azure, GCP) e Infraestrutura como Código (IaC).
• Segurança: Treinamento em práticas de segurança e conformidade (ex: criptografia, controle de acesso).
• Suporte: Capacitação em monitoramento e automação de sistemas em nuvem.
• Compliance: Conhecimento sobre governança e regulamentações (ex: GDPR, LGPD).

Planejamento de Treinamentos

• Treinamentos Online: Utilização de plataformas dos próprios provedores, como AWS Training, Microsoft Learn e Google Cloud Skills Boost.
• Workshops Internos: Sessões práticas para aplicação de conhecimentos em cenários simulados.
• Certificações: Incentivo à obtenção de certificações, como AWS Certified Solutions Architect ou Microsoft Certified: Azure Solutions Architect.

Plano de Comunicação Interna

• Comunicados Periódicos: Envio de atualizações regulares sobre o andamento do projeto.
• Reuniões de Alinhamento: Envolvimento dos times técnicos e gestores para alinhamento e resolução de problemas.
• Feedback Contínuo: Estabelecimento de canais para que os membros da equipe possam fornecer feedback durante o processo.

Justificativa da Escolha do Provedor de Nuvem (CSP)

A escolha do provedor de nuvem (CSP) é um fator crítico na migração. Abaixo, apresentamos uma análise comparativa entre Amazon Web Services (AWS) e Microsoft Azure, com base nos critérios de custo-benefício, segurança, desempenho e suporte técnico.

Custo-benefício

• AWS: Modelo de pagamento por uso, flexível e escalável, mas com uma estrutura de preços complexa.
• Azure: Preço competitivo, especialmente vantajoso para empresas já utilizando soluções Microsoft.

Segurança e Conformidade

• AWS: Oferece ferramentas robustas como IAM, AWS Shield e Amazon Macie, com diversas certificações de conformidade (ISO 27001, GDPR).
• Azure: Integração com Azure Active Directory e Azure Security Center, também com certificações de conformidade (ISO 27001, HIPAA).

Desempenho e Disponibilidade

• AWS: Reconhecida por sua alta disponibilidade e escalabilidade global.
• Azure: Alta disponibilidade com forte integração com ambientes híbridos e soluções Microsoft.

Suporte Técnico

• AWS: Suporte 24/7 com diversos planos, além de uma vasta comunidade de desenvolvedores.
• Azure: Suporte robusto, com expertise em ambientes corporativos Microsoft.

Conclusão

A escolha entre AWS e Azure dependerá das necessidades específicas da organização. O Azure é ideal para empresas já integradas ao ecossistema Microsoft, enquanto a AWS oferece maior flexibilidade e uma ampla gama de serviços.