**TÍTULO:** Trabalhos para a matéria de Arquitetura em MultiCloud   
(AWS / GoogleCloud / Azure / IBMCloud

**ALUNOS:** Vanessa, Victor, Michell, Jose Camargo

**TÍTULO:** Trabalhos para a matéria de Arquitetura em MultiCloud   
(AWS / GoogleCloud / Azure / IBMCloud

**DESCRIÇÃO DA INICIATIVA:** Evolução tecnológica e incorporar novas nos sistemas e infraestrutura da Rede de Cartões AMES, além de fornecer pagamento via celular sem a necessidade do cartão.

# **CENÁRIOS**

## **CENÁRIO ATUAL**

* Negócio
  + Usuário proprietário do cartão de crédito da rede AMES:
    - Pagamento via cartão de crédito;
    - Bandeira aceita nos principais estabelecimentos;
    - Bandeira internacional, aceita em mais de 210 países;
    - Disponível nas principais instituições financeiras:
      * [Nubank](https://www.foregon.com/blog/como-funciona-analise-do-nubank/)
      * [Ourocard](https://www.foregon.com/cartaodecredito/comparar/banco-do-brasil/)
      * [Santander Free](https://www.foregon.com/blog/banco-santander-contatos-telefone/)
      * [Inter](https://www.foregon.com/solicitar/cartaodecredito/banco-inter/fgn/cartao-de-credito-inter-mastercard/1183/)
      * [Itaucard](https://www.foregon.com/blog/conheca-os-beneficios-do-cartao-itaucard/)
      * [Bradesco Internacional](https://www.foregon.com/blog/banco-bradesco-contatos-telefones/)
    - Perfis de usuário/cartão:
      * Classic: ótimo para suas compras comuns do dia a dia e na internet;
      * [Gold](https://www.foregon.com/blog/gold-platinum-e-black/): exclusividade em serviços e benefícios em viagens;
      * [Platinum](https://www.foregon.com/blog/gold-platinum-e-black/): Infinite: Maior poder de compra.
  + Rede credenciada:
    - Gerenciamento das tecnologias (maquininhas);
    - Cobrar uma porcentagem do estabelecimento a cada venda realizada;
    - Credenciar estabelecimentos via consultor AMES, cujo prospecta clientes através de visitas presenciais.
  + Todos os perfis de clientes:
    - Aceitar as transações;
    - Atendimento 24 horas via telefone.
* Infraestrutura
  + Datacenter:
    - Versão TIER 2:
      * Exige que o desligamento de todo o site para trabalhos de manutenção;
      * Possui falhas de distribuição e capacidade, afetando assim, os sites hospedados no mesmo e;
      * Possui elementos redundantes.
    - Próximos um dos outros: 15 metros, o que aumenta os riscos, por exemplo, uma catástrofe de incêndio;
    - Virtualizador e Sistema Operacional back-level e sem suporte.

## **CENÁRIO PROPOSTO**

* Negócio
  + Usuário proprietário do cartão de crédito da rede AMES:
    - Pagamento via celular;
    - Disponível nas principais instituições financeiras digitais:
      * Agibank;
      * Banco Original;
      * C6 Bank;
      * Mercado Pago;
      * Neon;
      * PagSeguro;
      * Sofisa Direto.
    - Disponível nos bancos digitais de grandes lojas:
      * Banco Renner;
      * Lojas Pernambucanas;
      * Cacau Show.
    - Disponível nos principais bancos digitais internacionais:
      * N26 Bank ;
      * Capital One;
      * Neat;
      * Revolut;
    - Perfis de usuário/cartão:
      * Criar um novo perfil de usuário final – Infinite, cujo terá, além de maior poder de compra o benefício do Cashback.
  + Rede credenciada:
    - Transferir o gerenciamento das tecnologias das maquininhas para um fornecedor parceiro;
    - Credenciar estabelecimentos via portal web;
    - Fornecer informações de perfil de clientes consumidores em seu estabelecimento;
    - Fornecer informações de vendas;
    - Fornecer informações do percentual destinado a AMES.
  + Instituições financeiras:
    - Fornecer informações de clientes que possam auxiliar a instituição na liberação de crédito para o mesmo;
    - Fornecer informações de clientes que possam auxiliar a instituição na migração do perfil do mesmo;
    - Fornecer portal onde o cliente da instituição possa trocar seus pontos AMES por passagens aéreas ou itens de redes de lojas parceiras.
  + Gestor de vendas – prospector de clientes REDE AMES (redes credenciadas e instituições financeiras):
    - Fornecer informações sobre satisfação dos seus clientes em utilizar a rede AMES.
  + Todos os perfis de clientes:
    - Atendimento 24 horas via Whatsapp.
  + Normas:
    - Atender as normas PCI e LGPG;
    - Criar gestão de acessos a fim de atender regulamentações internas de segurança.
* Infraestrutura
  + Evolução tecnológica e;
  + Redução de riscos;
  + Alta disponibilidade.

# **REQUISITOS**

## **REQUISITOS FUNCIONAIS**

1. O usuário final, proprietário do cartão de crédito da rede AMES deverá realizar pagamentos via celular, ou seja, ao aproximar o seu celular da maquinha de cartões o pagamento deverá ser estabelecido;
2. O usuário final, cujo possui perfil Infinite deverá ter o benefício o Cashback, ou seja, cada compra é retornado 2% como crédito para o mesmo através da sua conta bancária/ carteira digital;
3. O cliente proprietário de um estabelecimento, cujo execute transações financeiras deverá, através de um portal web realizar o seu cadastro solicitando o seu credenciamento à rede de cartões AME;
4. O cliente proprietário de um estabelecimento, cujo seja credenciado à rede de cartões AME deverá receber através de um portal web informações sobre:
   1. Perfil de consumo dos seus clientes: Poder de compra: baixo, médio ou alto;
   2. Ticket médio;
   3. Vendas: valor total de vendas: diário, semanal e mensal;
   4. Percentual destinado a AMES: % de cada venda efetuada via cartão de AMES.
5. As instituições financeiras que atuam com cartão da rede AMES deverão receber através de API:
   1. Informações de seus clientes, cujos possuem cartão da bandeira AMES: histórico de compra, ticket médio, histórico de faturas pagadas em atraso, débitos em aberto e informações demográficas das compras;
   2. Receber notificações sugerindo a migração de perfil do cliente final, proprietário do cartão de crédito da rede AMES;
   3. Lista de itens que possam ser trocados por pontos AMES: passagens aéreas ou produtos de lojas parceiras.
6. Os gestores de vendas da rede AMES deverão acessar, através de um portal web:
   1. Lista de redes credenciadas pelo mesmo;
   2. Lista de redes credenciadas pelo mesmo, porém, que cancelaram o contrato e;
   3. Satisfação das redes credenciadas - informações que deverão ser coletadas através de pesquisa via portal web rede credenciada.
7. Todos os clientes da rede AMES deverão ter canal de atendimento através de WhatsApp e caso o motivo do atendimento não seja finalizado através da plataforma o mesmo deverá ser encaminhado para o atendimento humano.
8. LGPD:
   1. Usuário final: todos os clientes que possuem cartão rede AMES devem consentir através do contrato realizado na instituição financeira, na qual adquiriu o seu cartão AMES, o compartilhamento dos dados com a rede AMES, instituições financeiras e redes credenciadas da rede AMES.
9. Gestão de Acesso:
   1. Todos os colaboradores da rede AMES devem ter os seus acessos monitorados no nível de usuário e perfil;
   2. Todos os colaboradores da rede AMES devem ter acesso apenas aos sistemas e informações, cujas concessões foram aprovadas por um agente de gestão de riscos;
   3. Todos os colaboradores da rede AMES não devem ter acessos indevidos;
   4. Todos os ex-colaboradores da rede AMES devem ter seus acessos revogados.

## **REQUISITOS NÃO FUNCIONAIS**

1. Tecnologia que permita pagamento por aproximação (NFC);
2. Desenvolvimento e disponibilização de forma segura de nova API que permita calcular o retorno de 2% das compras realizadas via cartão AMES Infinity;
3. Criação de um portal web para que redes credenciadas e redes possam se tornar credenciadas através de cadastro na plataforma;
4. Desenvolver e disponibilizar de forma segura API’s para instituições financeiras;
5. Criação de um portal web para que equipe os gestores de vendas da rede AMES;
6. Utilização de IA para servir como canal de atendimento através do WhatsApp;
7. Criação e disponibilização de uma infraestrutura que possa atender todos os requisitos da LGPD;
8. Implantação de uma solução IGA (IDM – Identity Maganer + IG – Identity Governance);
9. Evolução tecnológica de todo parque tecnológico da rede AMES.

# **DESCRIÇÃO TÉCNICA DOS ITENS**

## **DATA CENTER**

1. Classificação de disponibilidade do Datacenter: Tier IV;
2. Localidade estão hospedados os Data Centers: localidade da massa de usuários.

## **INFRAESTRUTURA**

1. A plataforma deve possuir escalabilidade horizontal e vertical;
2. As aplicações devem ser concebidas com o máximo de escalabilidade;
3. As aplicações devem acomodar milhões de usuários sem impacto no desempenho;
4. Deve ser realizado mensalmente, trimestralmente e anualmente previsões de capacidade de recursos por meio da análise, modelagem, monitoramento de histórico de clientes, novas vendas e estimativa de uso dos clientes;
5. Os componentes tecnológicos e servidores adicionais devem estar totalmente configurados caso necessário;
6. Servidores de aplicação / web devem ser mantidos no modo de espera para uso imediato;
7. A infraestrutura do datacenter deve fazer uso de Balanceadores de Carga para distribuição em múltiplos servidores;
8. O gerenciamento de carga deve ser realizado em todos os níveis da infraestrutura, fornecendo redundâncias em todos os níveis.

## **MONITORAMENTO**

1. Método que deverá ser utilizado para o monitoramento do Datacenter:
   1. O monitoramento de performance deve ser realizado de forma proativa, incluindo os seguintes métodos:
      1. Experiência do usuário simulada: Monitoramento da performance da aplicação simulada a cada 5 minutos;
      2. Performance individual de servidores: Monitoramento de cada servidor individualmente;
      3. Visibilidade end-to-end das transações e aplicações Java, permitindo identificar problemas em servidores de produção;
      4. Coletar estatísticas de performance;
      5. Gerar alertas de utilização e tendência.
2. A provedora da cloud deverá disponibilizar aos clientes uma ferramenta própria com alto nível de serviços que inclui informações como número de logins, transações, performance de páginas, tempo de resposta para o usuário e tempo de resposta da rede;
3. Monitoramento de segurança: A provedora da cloud deverá utilizar vários scanners para analisar os Servidores Web e Aplicativos, visando identificar possíveis tentativas acesso de hackers e monitoramento de possíveis falhas de segurança. O teste de vulnerabilidade deverá ser feito diariamente por 3 diferentes fornecedores, realizados na periodicidade de: 24 horas, 7 dias da semana e 365 dias do ano;
4. Monitoramento de alerta de eventos: A provedora da cloud deverá fazer o envio de notificações em real-time sobre vulnerabilidades e incidentes no sistema de ticketing, e o time necessário deverá ter disponibilidade de ser acionado para resolver o problema. Além disso, todas as ações realizadas para resolver o problema deverão ser documentadas, permitindo rastreabilidade;
5. Monitoramento do abastecimento de energia e nobreak: A provedora da cloud deverá ter dois provedores de energia elétrica, bateria adicional, fontes de backup e geradores a diesel de backup. Além disso, as baterias precisam ser sempre carregadas, portanto, devem ser testadas continuamente e se a capacidade máxima das baterias decai excessivamente as mesmas deverão ser trocadas.

## **REDE E ACELERAÇÃO**

1. A camada de apresentação deverá ser isolada dos dados: Os administradores de um determinado equipamento ou área de rede não será administrador de outras áreas, por exemplo, administradores que gerenciam bancos de dados não possuem acesso aos servidores web;
2. O acesso ao conteúdo hospedado deverá ser dimensionado para o acesso global;
3. O ambiente de datacenter deverá satisfaz os requisitos e normas da ISO 27001/27002 e PCI-DSS conformidade: Para isso a provedora da cloud deverá passar por processos de auditoria e poderá realizar auditorias independentes a fim de validar que as medidas e controles de proteção de segurança e dados são estabelecidos e mantidos.

## **PLANO DE CONTINUIDADE DO NEGÓCIO**

1. Sistema para recuperação de desastres:
   1. Manter duas instalações distintas de data center em cada grande região geográfica (ou seja, Américas, Europa, Ásia), cada um configurado como um failover warm-site para outro em caso de desastre;
   2. Backups de banco de dados devem ser criptografados e armazenados em ambas as instalações para fins de redundância e recuperação de desastres.
2. Não deverá haver diferenças entre os ambientes produtivos e os centros de dados para recuperação de desastres. O data center primário poderá ser mantido em uma localização de escolha do cliente e o data center secundário alinhado para backup e continuidade dos negócios deverá ser mantido criptografado em outra determinada região;
3. O tempo para a recuperação dos serviços em caso de desastre deve ser no máximo 3 horas;
4. O período para a realização de testes de Recuperação de Desastres: O teste de DR deve ser realizado uma vez ao ano, e o plano de DR deve ser revisado conforme a necessidade com base nos resultados dos testes;
5. Processo de backup:
   1. Deve haver sempre um data center alinhado ao data center principal;
   2. Backups do banco de dados devem ser criptografados (AES 256-bit) e armazenadas no local "primário", bem como no local "secundário" para fins de redundância e recuperação de desastres;
   3. Quanto aos tipos de backup, deverá ocorrer snapshots a cada hora, backup incremental diário, e backups completos semanais;
   4. Os backups não devem ser enviados a provedores externos para evitar brechas em segurança da informação;
   5. Os backups devem ser armazenados por 30 dias.

## **SEGURANÇA**

1. Segurança física da instalação:
   1. Os data centers devem ter um sistema de gestão de segurança integrada, que inclui fotos eletrônicas, crachá de identificação, controle de acesso do titular do cartão, biometria, vigilância por vídeo digital gravado, e monitoramento de alarme e alarmes silenciosos, que notificam automaticamente o pessoal de segurança para aplicação da lei se ocorrer uma violação.
   2. Acompanhamento contínuo;
   3. Múltiplos circuitos de alimentação redundantes protegidas por UPS com gerador reserva;
   4. Detecção de fumaça e sistemas de extinção de incêndios 24 horas;
   5. Paredes à prova de balas e colunas de concreto.
   6. Monitoramento de umidade, e projetos terremoto-safe.
2. Acesso aos dados: Todo e qualquer acesso requisitado por autoridade necessita ser precedido de uma autorização judicial;
3. Firewalls redundantes e camada DMZ;
4. Controladores de domínio para garantir que todas as solicitações sejam autenticadas de modo seguro:
   1. Os dados devem ser criptografados em trânsito e em repouso, e para acessá-los deve-se utilizar SSL como chave pública e privada, gerando uma chave única para a sessão, garantindo assim privacidade da mensagem e integridade. Além disso, todos os usuários devem fazer autenticação centralizada no Active Directory e as permissões gerenciadas através do AD em combinação com as demais tecnologias de cada plataforma.
5. Para manutenções deve ser utilizado o sistema de identificação de usuário:
   1. Física: descrita anteriormente;
   2. Digital: todos os usuários devem ser autenticados via AD (ID único) através da ferramenta de Gestão de Acesso IDM+IGA, cujas permitem não apenas a autenticação, mas também a autorização de acesso e log de acessos.
6. Senhas de usuários:
   1. Colaboradores/terceiros com acesso a plataforma: O algoritmo utilizado para armazenar o hash de senhas é o SHA-1;
   2. Autenticação para usuários de sistemas que se integram à plataforma: SSO utilizando o protocolo SAML 1.1 e 2.0, seguindo as propriedades do modelo de autenticação do cliente.
7. Acesso:
   1. Acesso a plataforma via internet: Os navegadores dos clientes devem utilizar protocolo HTTPS / SSL v3, cujos são suportados nativamente pelos browsers de internet.
   2. Para clientes que acessam a plataforma de forma restrita através de seus portais deve ser estabelecido um range de IPs para os quais a aplicação possa ser acessada e a integração pode ser feita através do protocolo LDAP, tokens (MD5, SHA-1, HMAC encryption, DES, 3DES); Security Assertion Markup Language (SAML 1.1, 2.0) ou Active Directory;
   3. Acesso limitado por funcionalidade de usuário (IDM + IGA).
8. Política de senha adotada e processos de troca e recuperação de senhas:
   * 1. Criação de senhas:
        + Tamanho máximo
        + Tamanho mínimo
        + Letras maiúsculas e minúsculas (Caso Misto)
        + Caracteres numéricos não alfa
     2. Período máximo de troca: 30 dias;
     3. Número máximo de tentativas incorretas: 3;
     4. Esquecimento da senha: uma nova senha é gerada - o funcionário receberá um e-mail automático para redefinir a senha.
9. Sistema de proteção contra incêndio:
   1. Os data centers devem possuir proteção contra incêndio, desastres naturais e mudanças meteorológicas com sistemas de extinção de incêndio;
   2. Os data centers devem ter monitoramento de temperatura, fluxo de ar, umidade e terremoto;
   3. Os data centers devem ter unidades de detecção de fumaça, sistemas de extinção de incêndio e alarmes de incêndio para a área segura;
   4. Cilindros de Gás Inerte devem ser mantidos em um determinado nível de pressão específico. Um indicador eletrônico de pressão presente em cada cilindro de gás transmite desvios do valor padrão para a central de distribuição de gás, ou seja, o sistema deve ser testado continuamente;
   5. Detectores de fumaça devem ser testados a cada três meses utilizando um dispositivo que emite fumaça para verificar se o sistema está funcionando corretamente;
   6. Os equipamentos utilizados em cada datacenter devem ser distintos, de acordo com a sua localidade, porém obedecer aos requerimentos das certificações.
10. Procedimento de descarte de discos rígidos em caso de manutenção devem atender os requisitos de Controles NIST SP800-53 de segurança.

## **CRIPTOGRAFIA**

1. Chave de criptografia:
   1. Todos aplicativos serão baseados 100% em navegador da Web, com todo o acesso via HTTPS \ Port 443 exclusivamente e TLS versão 1.2. Todos os dados em trânsito também serão criptografados por criptografia AES de 256 bits;
   2. No caso de transferência de arquivos os mesmos devem ser enviados para importações em lote agendadas, passando por uma conta SFTP específica do cliente e com o uso recomendado da criptografia de arquivo PGP antes da transferência;
   3. Todas as senhas dos usuários finais serão armazenadas no banco de dados do cliente com um hash salgado unidirecional. O algoritmo de hash usado deverá ser baseado em PBKDF2 e HmacSHA256. Todos os backups de banco de dados serão armazenados apenas em disco e criptografados usando o protocolo AES de 256 bits;
   4. Os dados em repouso também devem ser criptografados por meio de uma abordagem baseada em hardware e sempre que os dados forem gravados no disco, eles serão gravados e salvos no formato criptografado utilizando criptografia AES de 256 bits. A criptografia no nível do hardware fornece desempenho superior à criptografia no nível do software, como na camada de software \ banco de dados da memória do banco de dados;
   5. O gerenciamento da chave de criptografia deve ser automatizado \ agendado por meio das Ferramentas Administrativas;
   6. Os dados trafegados entre os servidores da solução também serão criptografados utilizado SSL/TLS (HTTPS) como default através da porta 443 para todas as interações. Nenhum tráfego na porta 80 (HTTP) deverá ser permitido;
   7. E-mails ou notificações também devem ser criptografadas usando TLS/SSL. Adicionalmente observamos os itens abaixo para uma comunicação eficiente:
      1. Clientes devem adicionar os domínios da nossa plataforma em sua White list de e-mail para prevenir marcação como junk e-mail;
      2. Clientes que precisam de DomainKeys (DKIM) como protocolo de autenticação devem notificar a área de serviços durante a implementação;
      3. Para prevenir sobrecarga, o envio de e-mails deve ser agendado para cada 5 minutos e enviados em lotes de 100 por default.

## **TESTE DE VIOLAÇÃO DO AMBIENTE**

1. Processo de teste de violação de ambiente:
   1. Os seguintes fornecedores para teste de vulnerabilidade podem ser usados além da nossa própria equipe de infraestrutura e segurança de ti:
      1. HP Fortify On Demand, teste de vulnerabilidade no nível do aplicativo, TRIMESTRALMENTE;
      2. ERNW, teste de penetração no nível da rede e no nível da infraestrutura, BI-ANUALMENTE;
   2. Os relatórios de resumo do teste devem ser produzidos de acordo e disponíveis para clientes existentes, mediante solicitação;
   3. Os clientes da nossa plataforma podem enviar uma solicitação para realizar seu próprio teste de penetração em seu próprio banco de dados de testes, uma vez por ano e todos os testes de penetração patrocinados pelo cliente devem ser aprovados e agendados em conjunto com nossa equipe de infraestrutura.

## **SEGURANÇA DE ACESSO**

1. Perfil dos funcionários ou indivíduos que poder ter acesso interno a dados sobre produção:
   1. Os funcionários e terceiros que atuam na corporação deverão ter perfil de acesso gerenciado através da solução de Gestão de Acesso (IDM + IGA), cuja autenticação e autorização são feitas através do AD e geram registro de log para auditoria.
2. Prevenção ou mitigação de Negação Distribuída de Serviço (DDoS):
   1. Utilizar um DNS externo fornecendo em uma infra-estrutura DNS escalável, com tolerância a falhas global que é resistente contra uma grande escala distribuída de ataques DoS;
   2. Monitoramento para ataques DoS em roteadores e interface de firewall;
   3. Roteadores ACL para faixas de entrada endereço IP inválido e portas TCP não utilizadas;
   4. Relatório de ataque DoS;
   5. Todos os servidores de centro de dados e estações de trabalho devem ser bloqueados e protegidos;
   6. Filtragem de saídas; ou seja, verifica se o endereço IP de origem varia para impedir duplicação;
   7. Desabilitar o tráfego direcionado / multicast para evitar ataques Smurf.

## **AUDITORIA**

1. Certificações e os órgãos avaliadores:
   1. Atender a norma ISO27002 – internacional;
   2. Auditoria SSAE16 – SOC2 a cada 6 meses;
   3. Auditoria SAS 70 Tipo II;
   4. Auditorias independentes duas vezes por ano;
   5. Certificação Swiss Safe Harbor;
   6. Data centers certificados na ISO27001, ISO9001 e em conformidade com PCI-DSS;
   7. Clientes podem solicitar visita ao datacenter e realização de pen-testings através da abertura de um ticket. Os testes podem ser realizados pela equipe de TI ou por uma empresa terceirizada.

## **REQUISITOS DE SISTEMA**

1. Formas possíveis de conexão com os sistemas legados:
   1. Através de serviços REST/SOAP e também podem ser feitas através de arquivos utilizando o SFTP.
2. Largura de banda de rede mínima: 128kbps por usuário concorrente.

## **EVOLUÇÃO TECNOLÓGICA E QUALIDADE**

1. Metodologia de Garantia de Qualidade:
   1. Testes:
      1. Teste unitário;
      2. Teste integrado;
      3. Teste de segurança usando as ferramentas de escaneamento de código da Fortify e Burp;
      4. Testes de Performance/Carga/Stress usando HP Mercury LoadRunner;
      5. Testes de Release Readiness (prontidão);
      6. Teste de Aceitação.
   2. Treinamento de equipe:
      1. Equipes de Programadores e Qualidade devem receber treinamento avançado, especificamente para como desenvolver e testar o código visando segurança.
   3. Toda evolução sistêmica/tecnológica deverá fazer uso de procedimentos formais de controle de mudanças: documentação, especificação, testes, controle de qualidade e implementação gerenciada, avaliação de riscos, análise dos impactos das mudanças, e especificação de controles de segurança necessários;
   4. Os programadores devem ter acesso apenas às partes do sistema necessário para o seu trabalho e um acordo formal registrado nas soluções de gestão de acesso;
   5. Todos os novos códigos devem ser testados pelo time de qualidade;
   6. A área de Qualidade deve:
      1. Envolver-se com projeto de desenvolvimento para entender as próximas melhorias;
      2. Elaborar planos de teste no JIRA;
      3. Elaborar de casos de teste automatizados quando aplicável;
      4. Verificar novos recursos e correções de bugs;
      5. As vulnerabilidades de segurança devem ser incluídas na lista de verificação de itens.
   7. Solução para teste de segurança:
      1. WhiteHat Security - verifica a aplicação web regularmente e de forma contínua (24x7x365 dias por ano) e deve ter integrado o reporte vulnerabilidade diretamente no sistema interno de rastreamento de bugs. Uma vez que as vulnerabilidades estão localizadas, deverá ser aberto um ticket ao grupo de engenharia;
      2. Host and Network Based Intrusion Detection” e in-line “Web Application Firewalls”.
   8. Versão dos módulos da solução: devem ser atualizados sempre na mesma versão.

**ESTRATÉGIA MULTICLOUD**

Todo workload da solução será executado no provedor de Cloud publica Amazon Web Services (AWS) e o ambiente de Disaster Recovery ficará hospedado no provedor de Cloud publica Microsoft Azure.

A infraestrutura planejada para produção (site primário) hospedada na AWS foi desenhada utilizando como base a documentação do próprio provedor, onde recomenda as melhores práticas para operações de cartão de crédito atendendo a norma PCI DSS. Os recursos de produção ficarão hospedados em duas zonas de disponibilidade para redundância contra falhas e distribuição de tráfego, em localidades próximas a maior massa de usuários.

Será criado uma infraestrutura de Disaster Recovery no provedor Microsoft Azure, sendo um ambiente stand by, com uso de recursos mínimos e preparado para atender com alta escalabilidade uma demanda emergencial caso algum problema generalizado aconteça nas zonas de disponibilidade primarias na AWS. O banco de dados primário na AWS será replicado de forma síncrona para o banco de dados standby na Azure, de forma a manter uma consistência de dados entre os provedores.

O serviço de DNS Route 53 hospedado na AWS ficará responsável em rotear o tráfego de entrada dos clientes, apontando como caminho principal os recursos na AWS. O mesmo serviço irá monitorar a retorno de sucesso da aplicação e em caso de falha, o mesmo irá redirecionar o tráfego para os recursos na Azure.

**ESTRATÉGIA E ARQUITETURA PENSADA PARA A RESOLUÇÃO DO CASO**

A arquitetura proposta para o case consiste em disponibilizar os recursos de produção e Disaster Recovery via provedores de Cloud pública.

1. Os usuários (aplicações, chamadas de API) acessam um endpoint (DNS Global) publicado na web.
2. O serviço de DNS Global direciona o tráfego para o provedor de Cloud primário e monitora a aplicação. Em caso de problemas no provedor primário, o DNS redireciona o tráfego de entrada de clientes para o provedor de Cloud stand-by.
3. Existem quatro camadas de rede segregadas logicamente com regras de tráfego definidas entre elas.
4. Dentro do provedor de cloud, a conexão do cliente é encaminhada para um Load Balancer, que irá balancear a carga de entrada e posteriormente redirecionará para o pool de servidores Web. Os servidores de Web são escalados horizontalmente de acordo com a demanda e uso dos recursos.
5. Os servidores Web se conectam no Internal Load Balancer na camada de aplicação e redirecionam o tráfego para o pool de servidores de aplicação. Os servidores de aplicação são escalados horizontalmente de acordo com a demanda e uso dos recursos.
6. A aplicação realiza leitura e escrita no banco de dados principal, localizado na zona de disponibilidade principal. Como o pool de aplicação é escalado em mais de uma zona de disponibilidade, o serviço de banco de dados da Cloud garante que a aplicação seja acessada através de um único endpoint, realizando a leitura e gravação na instancia de produção do Bando de Dados.
7. O Banco de Dados principal é replicado de forma síncrona para outra zona de disponibilidade, pois caso a zona primaria fique indisponível, as instancias de aplicação se conectam na instancia de bando de dados standby.
8. O banco de dados secundário é replicado de forma síncrona para outro provedor de cloud que será utilizado em situação de Disaster Recovery.
9. Os administradores da infraestrutura e aplicação podem utilizar para acesso, tanto o portal do provedor de cloud como também um servidor de bastion host, que possui rotas definidas somente para as subnets internas.
10. Será executado backup do banco de dados com retenções programadas.
11. Os serviços de telemetria e monitoramento serão utilizados para monitorar a saúde da infraestrutura e aplicações.

Diagrama

Descrição gerada automaticamente

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

**EXPECTATIVA DE BUSINESS (NEGÓCIOS).**

O negócio espera que após todo o investimento realizado pela empresa para se adequar as novas tecnologias de mercado e adaptação da infraestrutura para a mullticloud os ganhos sejam significantes, pois através da tecnologia multicloud que será implementada na empresa teremos melhorias em todas as áreas da empresa, gerando uma vantagem competitiva sobre os concorrentes.

Com adoção da multicloud permitiremos que a empresa combine opções de serviços mais competitivas, não se limitando a ser atendida por um único provedor. Dessa forma, será mais fácil encontrar soluções com o melhor custo-benefício.

Além disso, com toda a flexibilidade no uso dos recursos em multicloud, poderemos investir em inovação sem a necessidade de ter um custo alto em compra de máquinas para suportar os ambientes, se preocupando cada vez mais no negócio e menos em Infraestrutura.

Um ambiente multicloud oferece como vantagem a alta disponibilidade, baixa latência e o aumento de recursos aplicados a segurança da informação, além de estarem totalmente aderente as legislações locais evitando assim multas e sanções por não cumprimento das mesmas e isso são requisitos fundamentais para o negócio.

Com a adoção da multicloud conseguiremos lançar a nova funcionalidade de pagamento via celular sem a necessidade do cartão de forma mais rápida, pratica e segura gerando maior credibilidade a empresa e assim atraindo novos clientes a procura pelos nossos serviços.

**EXPECTATIVA FINANCEIRA**

|  |  |  |
| --- | --- | --- |
| **ITEM** | **PROVEDOR** | **VALOR MENSAL R$** |
| Recursos Cloud Mensais AWS | AWS | R$ 142.479,00 |
| Recursos Cloud Mensais Azure | Azure | R$ 99.735,00 |
| Pacote de horas de suporte mensais | Cloud Providers | R$ 4.000,00 |
| Consultoria Arquitetura e implantação | Arquitetos | R$ 200.000,00 |

**SUGESTÕES E RECOMENDAÇÕES**

Iremos realizar o treinamento para equipe atual de infraestrutura da REDE AMES com o objetivo de torná-los aptos à administração e suporte de toda infraestrutura e aplicações.

Sugerimos a contratação de horas técnicas com os vendors de cloud citados no documento para devida tratativa em caso de incidentes onde a equipe técnica local possa utilizar como apoio para resolução de problemas e incidentes.

Também sugerimos a contratação de especialistas:

* + Especialistas em nuvem;
  + Especialista em Banco de Dados;
  + Especialista em aplicações;
  + Especialista em aplicações web.
  + Consultoria para suporte.