

Estratégia para Adoção de Nuvem – Sefaz/SP



GOVERNO DO ESTADO DE SÃO PAULO
SECRETARIA DA FAZENDA

COORDENADORIA DE SERVIÇOS E TECNOLOGIA
COMPARTILHADOS - CSTC

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO - DTI

Sumario Executivo



- A computação em nuvem pode proporcionar:
 - Agilidade no atendimento às demandas de negócio ;
 - Maior racionalidade na ocorrência de desembolsos
 - Alocação das equipes de TI em tarefas de maior valor agregado
 - Utilização de escalabilidade horizontal
 - Migração de custos de investimentos para custeio
 - Maior transparência na apresentação dos custos de projetos de TI

Sumário Executivo



- Desafios:
 - Necessidade de desenvolver uma equipe com sólidos conhecimentos em Nuvem
 - Implantação de um modelo de governança
 - Manutenção dos níveis de qualidade de serviço - disponibilidade, desempenho e segurança;
 - Integração entre datacenters internos e de Nuvem
 - Estratégia de proteção e classificação de dados
 - Plano de gestão de riscos;
 - Gerenciamento operacional centralizado → recursos da nuvem e internos

Sumário Executivo



- Benefícios esperados:
 - Redução no tempo de implantação de um novo ambiente;
 - Redução de custos de investimento;
 - Redução do uso do datacenter próprio;
 - Pagamento pelo uso efetivo.

Sumário executivo



- Objetivos estratégicos atendidos pela Iniciativa:
 - **Objetivo Estratégico A** – Aproximar a Fazenda das Pessoas, Empresas e Servidores;
 - **Objetivo Estratégico: J** - Ser Mais Justo e Eficaz na Relação com o Contribuinte e Agentes Públicos;
 - **Objetivo Estratégico R** – Ampliar os Recursos para a Sociedade por Meio da Redução do Custo de Servir;
 - **Objetivo Estratégico S** – Reduzir a Burocracia, Simplificando, Integrando e Informatizando Processos.

Sumário Executivo



- Escopo da iniciativa:
 - Elaboração da Estratégia de uso de nuvem da Sefaz
 - Criação de um framework de adoção de nuvem
 - Definição de cenários indicados para adoção de nuvem

Requisitos Estratégicos - Nuvem



- **Requisitos Legais**

- **Lei federal 12.527/2011 - LAI**
- **Decreto Estadual nº 58.052/2012**
- **Deliberação COETIC 1-2017**
- **Resolução SF Nº 20 - 2012**
- **Resolução SEFAZ SF-57 - 2009 e Portaria Conjunta CGA/CPM-1 - 2012**

Requisitos Estratégicos de Segurança



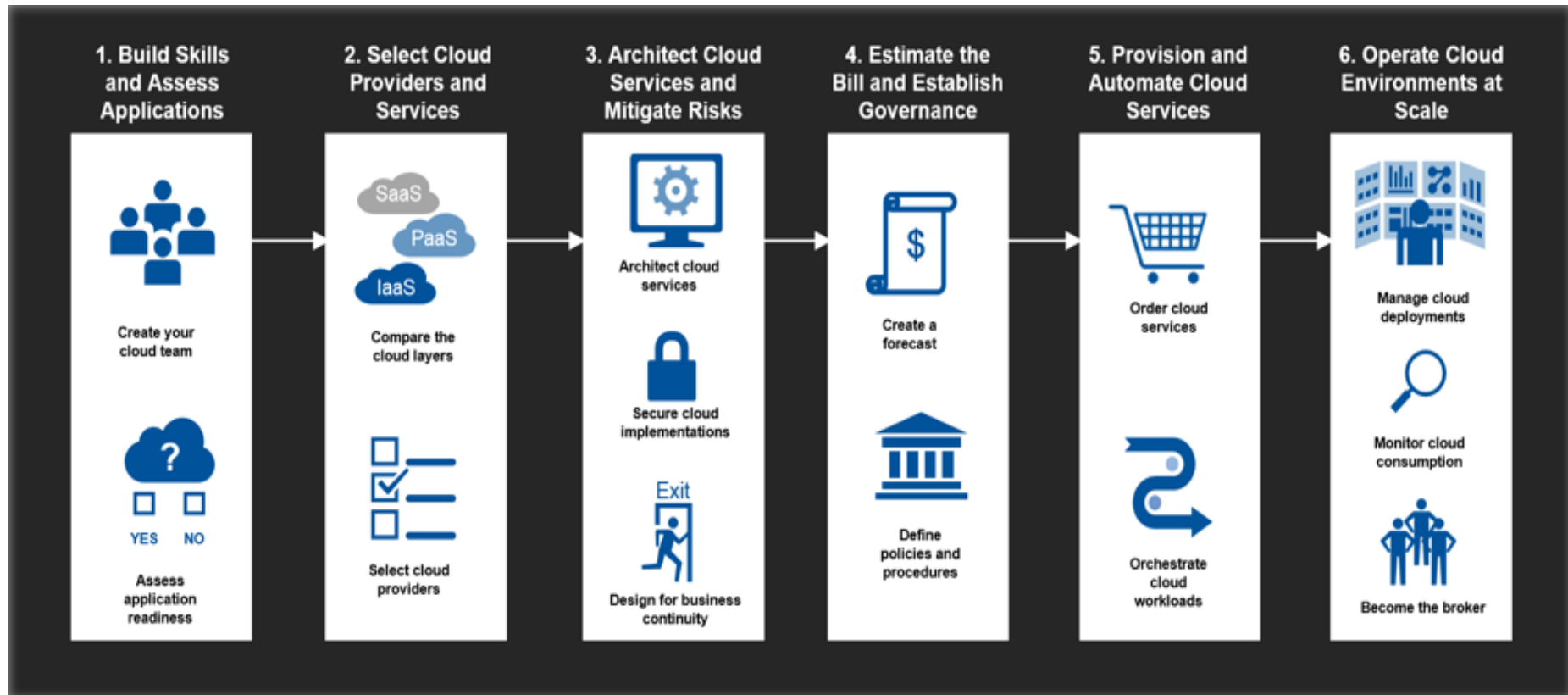
- **Restrição ao uso de Nuvem**
- **Análise de Riscos**
- **Governança**
- ***Confiança/Garantia***
- ***Geolocalização***
- ***Monitoramento do ambiente***
- ***Gestão de Acesso e Gestão de Identidades***
- ***Gerenciamento de Chaves e Uso de Recursos Criptográficos***
- ***Transição contratual***
- ***Dependência do Fornecedor***

Uso de Nuvem na Sefaz



- Estratégia: mover/criar um subconjunto de aplicações para a nuvem pública
- Dinâmica:
 1. demanda recebida
 2. Avalia-se o enquadramento em um dos cenários de uso
 3. caso a demanda se enquadre em um dos cenários, a demanda poderá ser implantada na nuvem.

Framework de adoção de Nuvem



Cenários de uso - Nuvem



- Solução de TI como resposta a uma necessidade imediata
- Falta de recursos próprios
- Ambiente de testes de sistemas/aplicações
- Bibliotecas na nuvem para diminuir o tráfego de dados
- Demandas sazonais elásticas
- Uso de ferramentas de telemetria/monitoramento
- Uso de aplicações disponíveis na nuvem
- Desenvolvimento de provas de conceito
- Infra interna com custo/benefício pior que a nuvem;

Papéis e Responsabilidades



- O grupo de arquitetos de Desenho de Solução
 - responsável por avaliar e coordenar os aspectos de desenho de solução
 - Recomendações
 - detalhes de implantação e
 - decisões para os projetos relacionados à Nuvem.

Comitê Gestor da Nuvem Sefaz



Área	Pessoas
CIA	Gerente de Desenho de Solução, Diretor do CIA e Controller de Nuvem
CDS	Arquiteto de Desenvolvimento
COI	Arquiteto de Infraestrutura
CSI	Arquiteto de Segurança da Informação
CAS	Arquiteto de Atendimento e Suporte
CGC	Arquiteto de Gestão de Contratos
DTI-Gabinete (Gestor do Contrato de Nuvem)	Diretor do DTI

Investimentos Necessários



- Capacitação de recursos humanos
- Link de Internet
- Ferramenta de gerenciamento de contratos
- Ferramenta de gerenciamento de despesas
- Ferramenta de gerenciamento operacional único: datacenter próprio e ambiente de nuvem;
- Processos de governança
- Ferramenta para rotular as informações quanto à classificação
- Licenças de ferramentas específicas para a nuvem

Visão Arquitetural



- Forma de implantação: **Nuvem Híbrida**
 - Composição de nuvem privada e nuvem pública,
 - interligação por tecnologias padronizadas
 - Permite a portabilidade de aplicações e de dados entre as nuvens

Desenho de Solução - Nuvem



Atividades	Notas
Identificação de cenário de uso de Nuvem	A demanda foi analisada e encaixa-se em um dos cenários de uso de Nuvem.
Requisitos de integração com Datacenter próprio	Avalia-se a necessidade de integração entre datacenters próprio e a Nuvem. Os requisitos não funcionais de integração são anotados.
Desenho de Solução	Forma-se o grupo de arquitetos responsável por produzir a solução técnica para a demanda recebida. Requisitos técnicos, de integração e de conformidade devem ser conhecidos por todos os envolvidos.
Validação da Solução proposta pelo CSP	A Solução proposta pelo grupo de desenho de solução é debatida com o CSP e alterações de desenho de solução podem ser necessárias.
Provisionamento de recursos do contrato de Nuvem	Controller de Nuvem recebe o desenho de solução final e avalia se existem recursos financeiros para a implantação proposta.
Implantação da Solução na Nuvem	Após finalizada a etapa de modelagem da solução e a indicação sendo o uso da nuvem, então a solução é implantada na Nuvem.

Atividades Necessárias – Uso da Nuvem



- **Capacitação de Recursos Humanos;**
- **Criação do Comitê Gestor da Nuvem;**
- **Criação do Papel de Controller da Nuvem;**
- **Contratação de Nuvem;**
- **Gerenciamento Unificado de Identidades;**
- **Implementação de VPN;**
- **Desenho e Implantação de Solução na Nuvem.**

Anexos



- **Anexo 1 - Características da Nuvem**
- **Anexo 2 - Requisitos Técnicos para Adoção de Nuvem**
- **Anexo 3 – Tabela de riscos, controles aplicáveis, Análise de Risco – Sefaz/SP**
- **Anexo 4 - Glossário**

Anexo 2 – Requisitos Técnicos



- Os requisitos arquiteturais a seguir foram avaliados como necessários à implantação de soluções na Nuvem pública;
- Os requisitos foram categorizados conforme apresentados nos tópicos a seguir.

Desenvolvimento



- O time de desenvolvimento será responsável por instrumentar os novos serviços, permitindo assim a fácil administração e manutenção pelo time de operação;
- Deverão ser utilizados frameworks de desenvolvimento que aproveitem as funcionalidades disponíveis no provedor de nuvem, para extrair o maior benefício da nuvem.

Rede/Segurança



- Segmentação de Redes (DMZ, APP e BD)
- Segmentação de Ambientes (Produção, Homologação e Desenvolvimento)
- Proteção de Segmento Externo por IPS/IDS
- Proteção contra DDoS
- Antivírus/Antimalware para os Servidores
- Gestão de Patches e Atualizações;
- WAF (Web Application Firewall)
- Gravação e Correlação de Logs de Acesso
- Integração entre os Ambientes do Provedor de Computação em Nuvem e a Sefaz
- Classificação da Informação
- Administração Restrita de Servidores e BDs

Disponibilidade



- Escalabilidade e Elasticidade conforme demanda
- Recursos de Monitoramento e Configurações de Self-healing

Criptografia, Certificados Digitais e Gerência de Chaves



- Serviço de Proteção e Gerência de Chaves Criptográficas;
- Criptografia de Banco de Dados;
- Criptografia de Volumes (Sistemas Operacionais e Dados);

Plano de Continuidade de Negócios



- Estrutura de Backup
- Balanceamento de Carga entre diferentes sites (datacenters)
- Distribuição de Banco de Dados com replicação síncrona em diferentes sites

Gerenciamento de Identidade



- Federação do Active Directory para centralização das contas de acesso;
- Gerenciamento de Credenciais de Acesso ao Provedor de Nuvem
- Utilização de Multi-Factor Authentication
- Política de Acessos Granular

Governança



- Política de Deploy
- Utilização do Recurso de TAGs
- Utilização de recursos de monitoramento e conformidade (*compliance*)

Análise de Riscos - SEFAZ



- **Resultado**
- Calculando a média dos riscos envolvidos, temos:
- PIR Total: $(\sum \text{Riscos}) / 30 \text{ (N. de Riscos)} = 23,5$
(Risco Médio)

Análise de Riscos - SEFAZ



Conclusão

- Adoção da computação em nuvem é viável;
- Há Riscos inerentes à tecnologia de armazenamento e processamento de informações em um CSP (Cloud Service Provider);
- A análise/avaliação de riscos deve servir de subsidio para a adoção de controles de segurança da informação ;
- Atualmente, a infraestrutura provida pelos maiores provedores de serviço de nuvem é robusta e madura, com capacidade de fornecer camadas de proteção aos dados e serviços de clientes, inclusive contando com diversas creditações e certificações internacionais.

Obrigado!