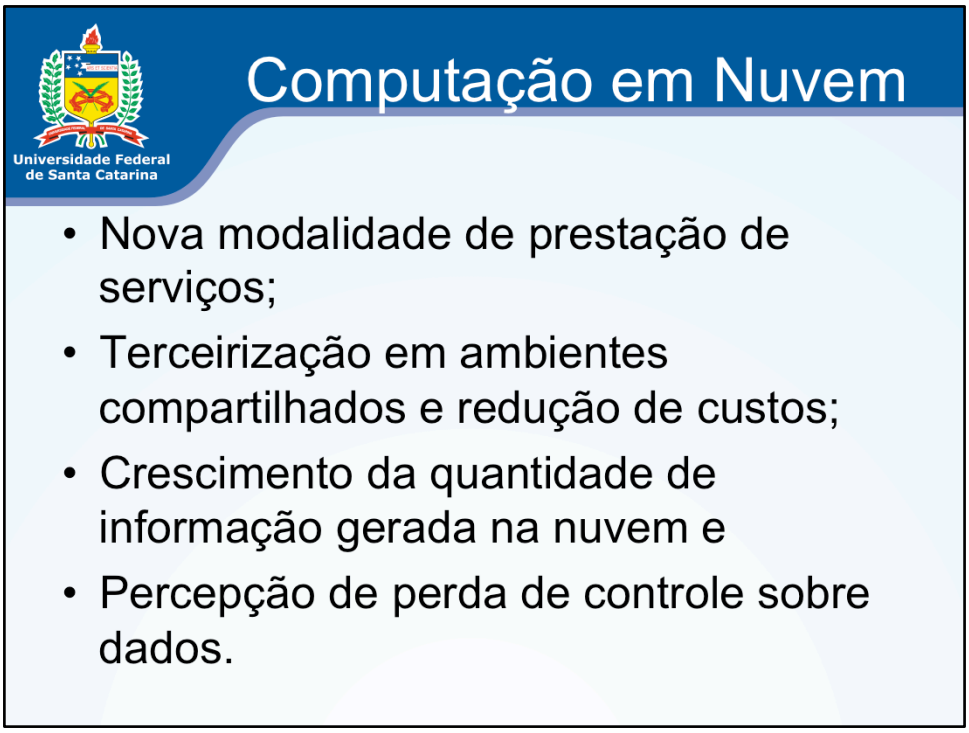
Imagem Gustavo Santos.
Observe Bombinhas – SC.

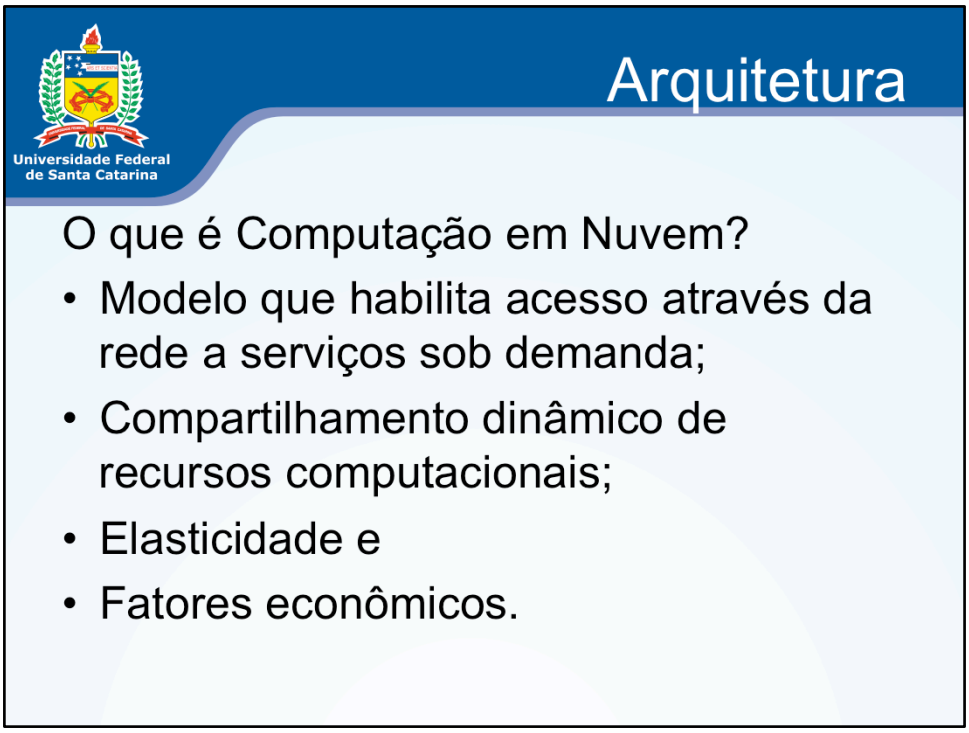
Universidade Federal de Santa Catarina

Agenda

Sumário
Computação em Nuvem: motivação, arquitetura, modelos
Problema de Pesquisa e Objetivos
Bases de Dados em Nuvem e Segurança da Informação
Framework Conceitual: Controles Internos
Resultados Obtidos
Métricas e Análise de Vulnerabilidades



1. Uma nova modalidade de prestação de serviços computacionais está em uso desde que a computação em nuvem começou a ser idealizada. As empresas norte-americanas são as que mais se destacam na comercialização mundial desses serviços de “data center”;
2. Seguindo a ideia de redução de custos, proporcionando economia com aquisição de equipamentos e licenças de programas, praticidade e menor tempo para utilizar um ambiente completamente operacional, incorporações têm terceirizado diversos serviços. Além desses pontos, empresas de qualquer tamanho podem, dependendo de suas necessidades e prioridades, desonerar gastos de contratação de profissionais especializados, antes necessários para suprir demandas pequenas. Assim, tarefas rotineiras de gerenciamento, manutenção e atualização de programas são incluídas no contrato de prestação de serviço. Outros benefícios seriam elasticidade, melhor qualidade de serviço e alocação interna de recursos mais efetiva.
3. O crescimento da quantidade de informação gerada na nuvem associado à inteligência para administrar ou consultar fez com que surgisse um novo paradigma que é o de fornecer banco de dados como serviço.
4. Uma das desvantagens desse modelo é a percepção da perda de controle sobre os dados. No entanto, as próprias características de um sistema distribuído reforçam a transparência.



1. Segundo definição do NIST: Computação em nuvem é um modelo que habilita acesso à rede sob demanda, conveniente e ubíqua para o compartilhamento de recursos computacionais tais como redes, servidores, armazenamento, aplicações e serviços.
2. Esses recursos podem ser facilmente fornecidos ou removidos com esforço mínimo de gerenciamento ou mínima interação do provedor de serviços.
3. É um paradigma de computação distribuída em larga escala determinado por fatores econômicos, surgindo de uma derivação de Computação em Grid.

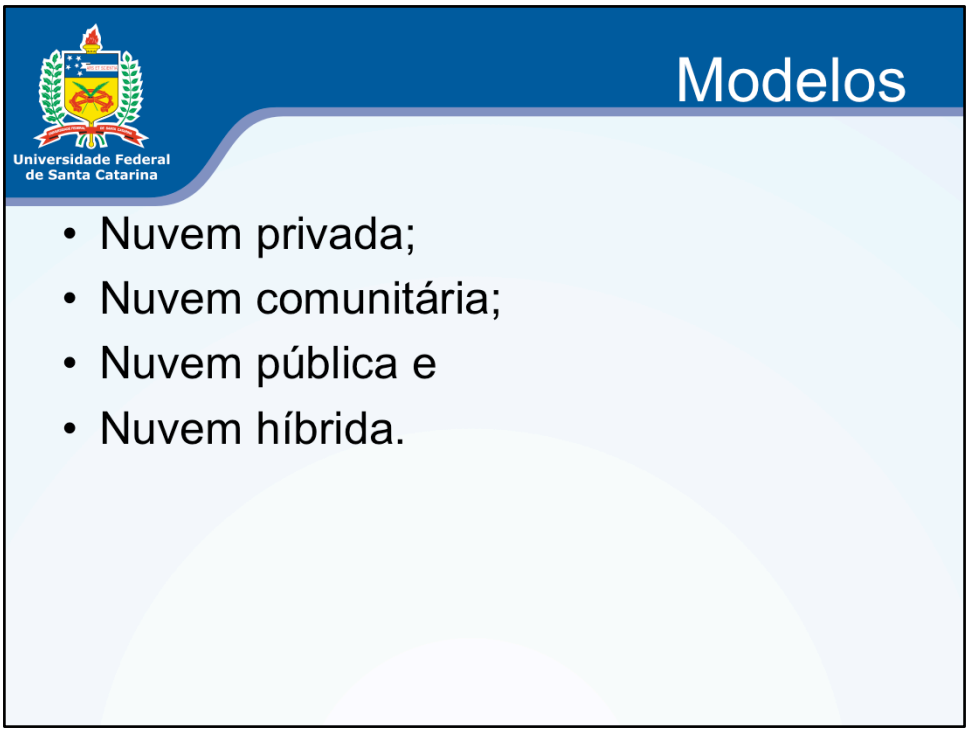
Serviços sob demanda: O próprio consumidor pode fornecer recursos computacionais tais como servidores de sincronização de tempo ou armazenamento em rede sem interação com pessoal de cada provedor.

Acesso através da rede: Recursos da nuvem estão disponíveis através da rede e por mecanismos heterogêneos como telefones celulares, tablets, laptops ou estações de trabalho.

Alocação dinâmica de recursos: Os recursos computacionais do provedor são colocados em pool para atender a diversos consumidores diferentes ao mesmo tempo. Recursos físicos e virtuais são alocados e realocados dinamicamente, conforme a necessidade do consumidor.

Elasticidade: Capacidade de crescimento ou decrescimento feito de maneira rápida e, em alguns casos, automática, conforme a demanda. Para o consumidor a capacidade de crescimento parece ser ilimitada.

Cobrança: Medidas de uso de recursos são feitas em níveis de abstração conforme o tipo de serviço, por exemplo, uso de espaço de armazenamento ou banda de rede, processamento. A cobrança geralmente é baseada pelas medidas de uso.

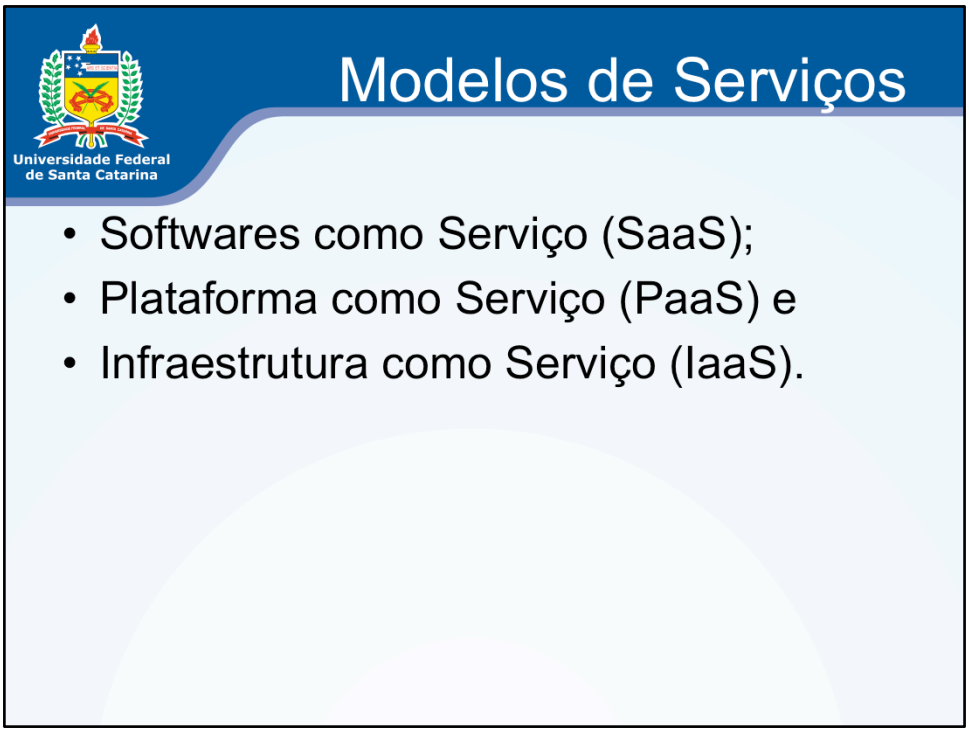


Nuvem privada A infraestrutura de nuvem é fornecida para uso exclusivo de uma única organização que poderá ter diversos consumidores (por exemplo, departamentos de uma empresa). Ela pode ser de propriedade, gerenciada e operada pela organização ou por terceiros ou ainda por ambos.

Nuvem comunitária É utilizada por uma comunidade específica de consumidores de organizações com interesses comuns, por exemplo, missão, requisitos de segurança. Ela pode ser de propriedade, gerenciada e operada por uma ou mais organizações da comunidade, por terceiros ou alguma combinação de terceiros e organizações.

Nuvem pública A infraestrutura de nuvem é fornecida para uso do público em geral. Ela pode ser de propriedade, gerenciada e operada por organizações de governo, empresas privadas, instituições acadêmicas ou uma combinação delas.

Nuvem híbrida Composta pela composição de duas ou mais infraestruturas distintas de nuvem (privada, comunitária ou pública). É limitada a padrões ou tecnologias proprietárias que habilitem a portabilidade de dados e aplicações entre as partes da infraestrutura com, por exemplo, balanceamento de carga entre nuvens.



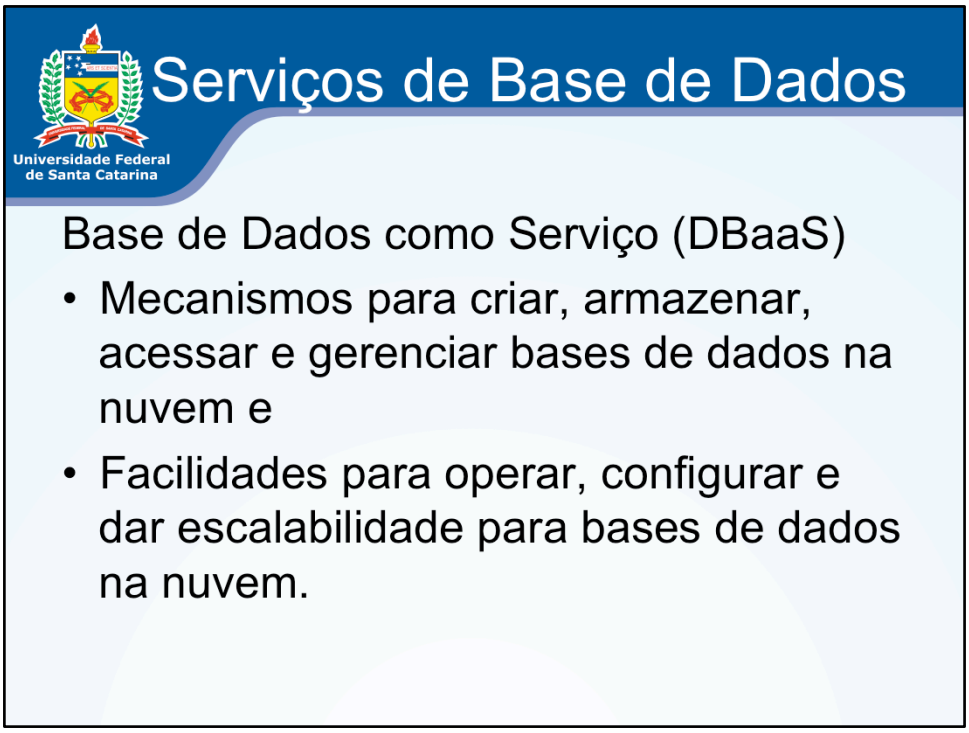
Segundo definição do NIST

SaaS Capacidade de os clientes utilizarem aplicações rodando na infraestrutura de provedores. As aplicações podem ser acessadas através de diversos dispositivos do cliente incluindo navegadores ou programas específicos. A infraestrutura, incluindo rede, servidores, sistemas operacionais ou área de armazenamento não é controlada pelo cliente. Google Apps, Amazon RDS, Office 365

PaaS Capacidade de os clientes instalarem aplicações na infraestrutura da nuvem. As aplicações podem ser adquiridas ou criadas pelos clientes usando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor. A rede, servidores, sistemas operacionais ou área de armazenamento não são gerenciados pelos clientes, mas eles possuem o controle das aplicações e configurações delas. Windows Azure

IaaS Capacidade de os clientes provisionarem processamento, área de armazenamento, rede e outros recursos computacionais relevantes para instalação e execução de programas arbitrários, incluindo sistemas operacionais e aplicações. O cliente não tem controle sobre a infraestrutura da nuvem, mas pode controlar sistemas operacionais, armazenamento, aplicações instaladas e controle limitado sobre componentes de rede como firewalls. Amazon EC2, S3.

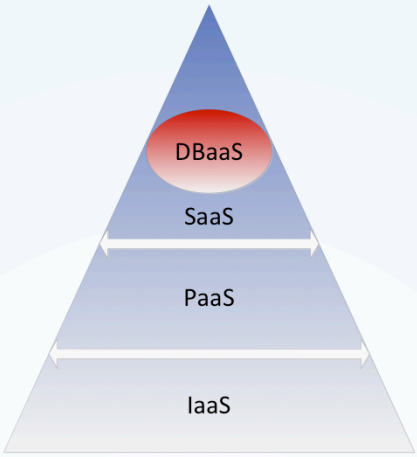
Multi-Tenancy Ele implica na necessidade de aplicar políticas para segmentação, isolamento, governança, níveis de serviço, modelos de cobrança e restituição para diferentes clientes compartilhando recursos.

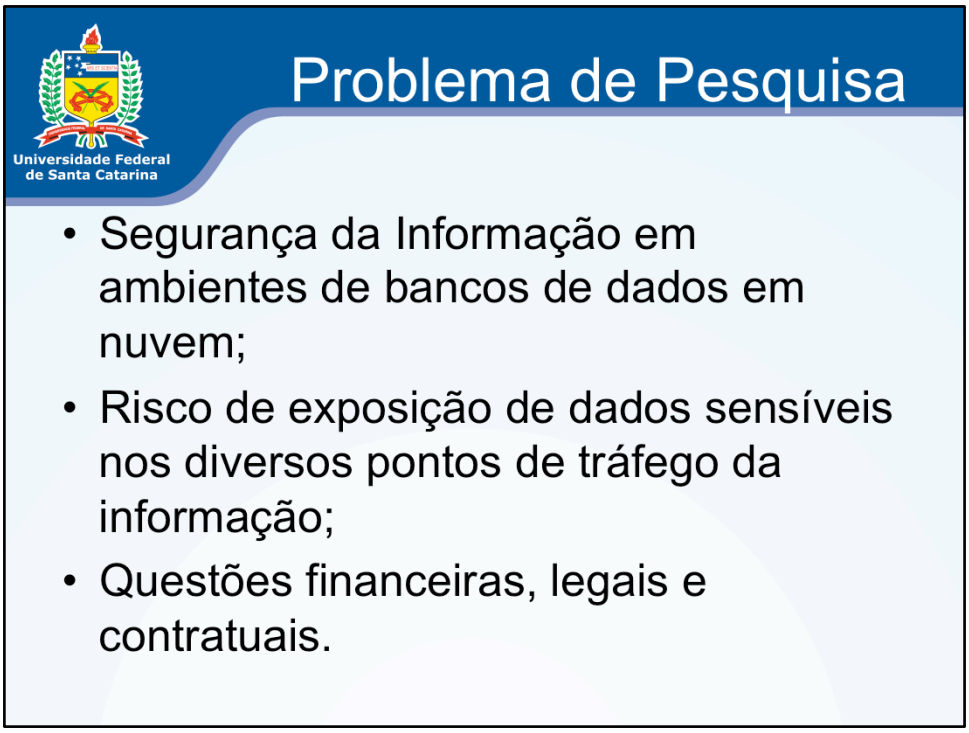


Introduz um modelo que facilita a operação, configuração e a escalabilidade para uma base de dados. No entanto, gera outros desafios como a privacidade, criptografia de dados e em qual granularidade, como o acesso aos dados deve ser, considerando a confidencialidade nos canais de comunicação. Além disso, devem-se criar mecanismos para garantir que dados não sejam alterados inadvertidamente e controle de acesso mais rigoroso.

Universidade Federal de Santa Catarina

Modelos de Serviços





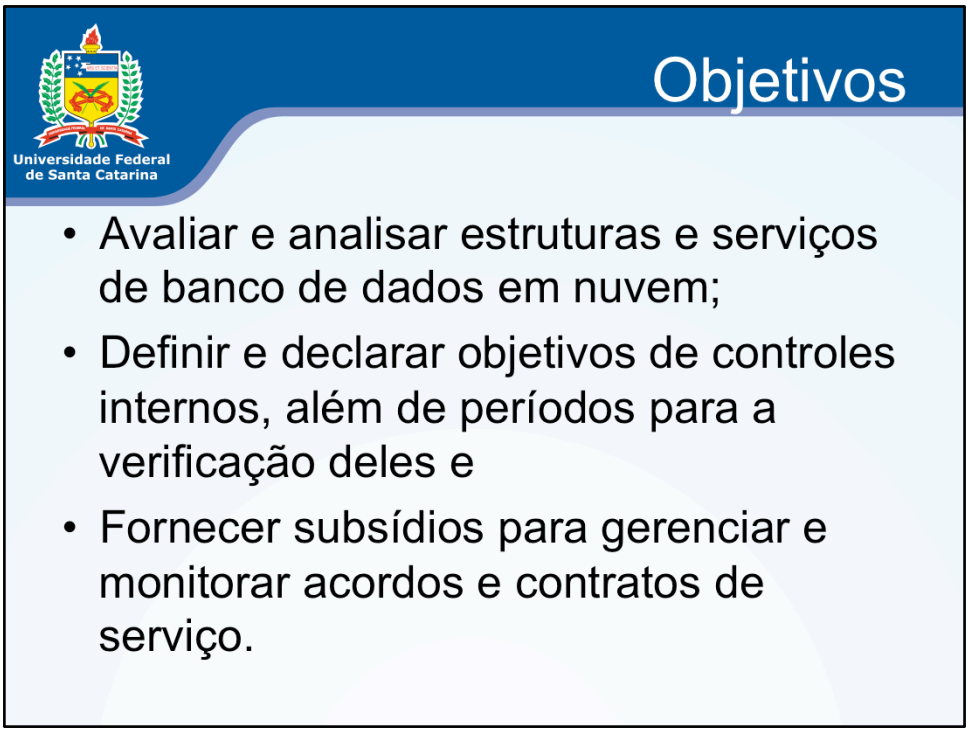
Confidencialidade O caminho mais comum para a privacidade de dados é o uso de criptografia. Surgem novos desafios como a granularidade da informação, escolha de algoritmos e formas de implementação, uso de chaves criptográficas e esquemas utilizando software ou hardware.

Integridade Tem-se usada assinaturas digitais como maneira para se obter completude e autenticidade de dados. Uma proposta é a de prover metadados (geralmente uma hash) que permita ao usuário a verificação do dados.

Cliente deve verificar se estão previstos em contrato:

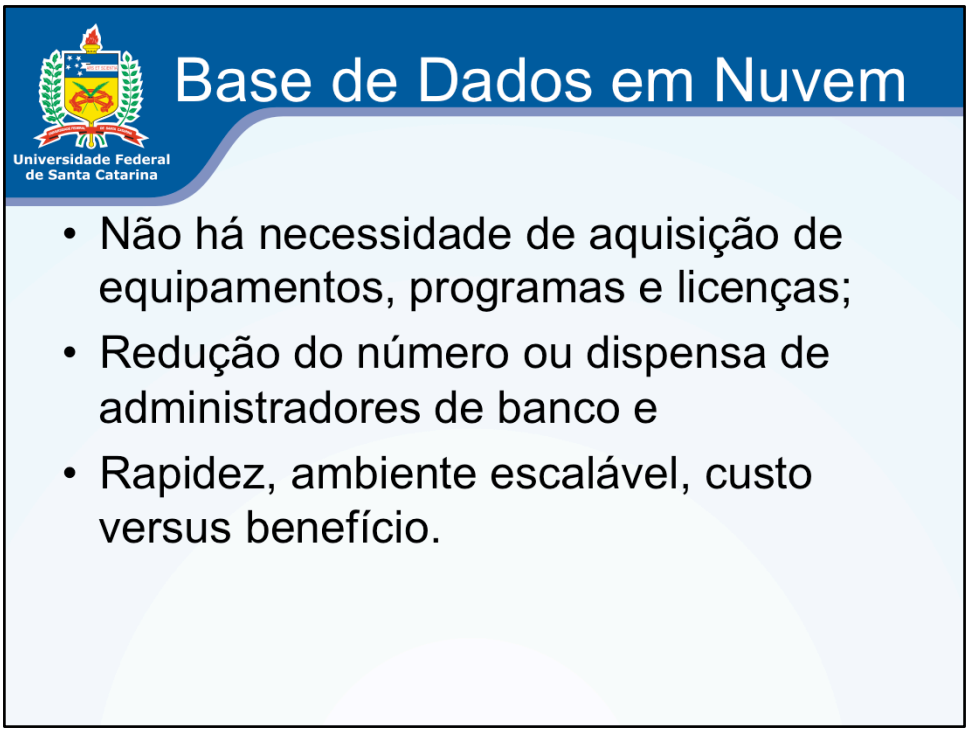
Segurança física e lógica; Cópia de segurança (backup) e recuperação; Como são feitos os acesso de usuários privilegiados; Aplicar restrições na localização de dados; Segregação dos dados dos clientes; Auditoria de dados e usuários; Auditoria do cliente e do provedor; Suporte à investigação; Conformidade com regulamentações e leis; Métodos para destruição ou eliminação de dados; Gerenciamento de chaves criptográficas e Segurança da rede.

Os SGBDs devem dar suporte a Controle de usuários; Criação de papéis ou atribuições para usuários ou grupos; Criptografia transparente de dados; Classificação de dados através do uso de rótulos; Customizar a segurança para os níveis de linha ou coluna; Gerenciamento de identidade e Auditoria.

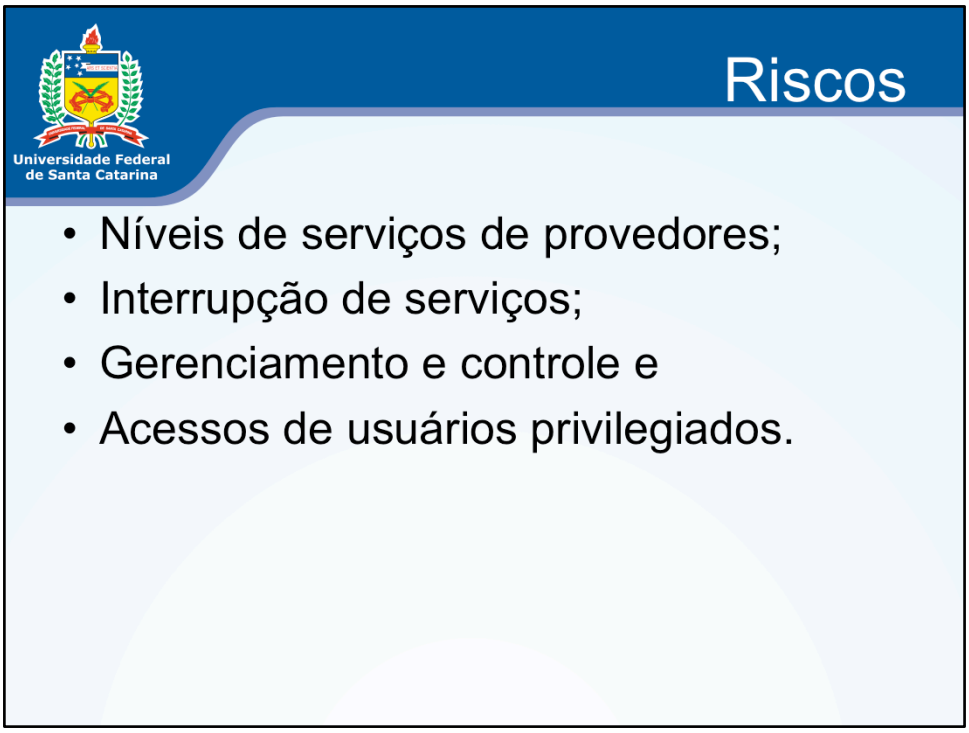


Em meio a uma variedade de tecnologias e diferentes fornecedores, é preciso trazer à mente e rever a importância de se ter um modelo de dados conceitual para organizar aquilo tudo que se pretende obter com um DBaaS e ter sucesso na sua implementação ou certificar-se de sua impossibilidade.

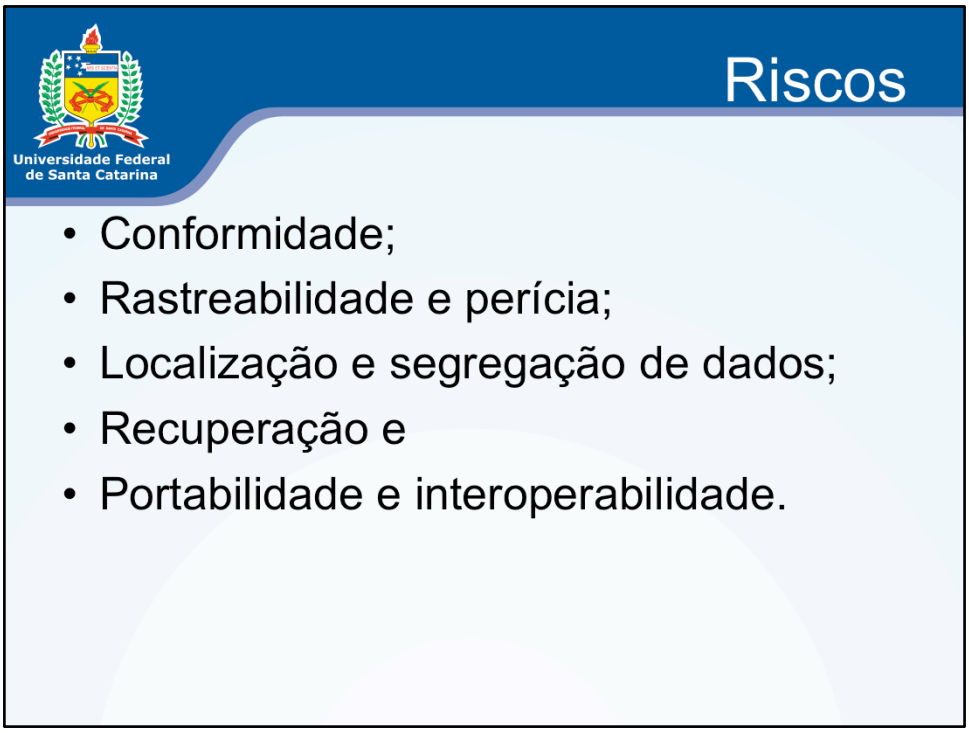
Com base em modelos de dados conceituais conhecidos internacionalmente, boas práticas e guias pretende-se implementar um modelo de dados conceitual apropriado para DBaaS.



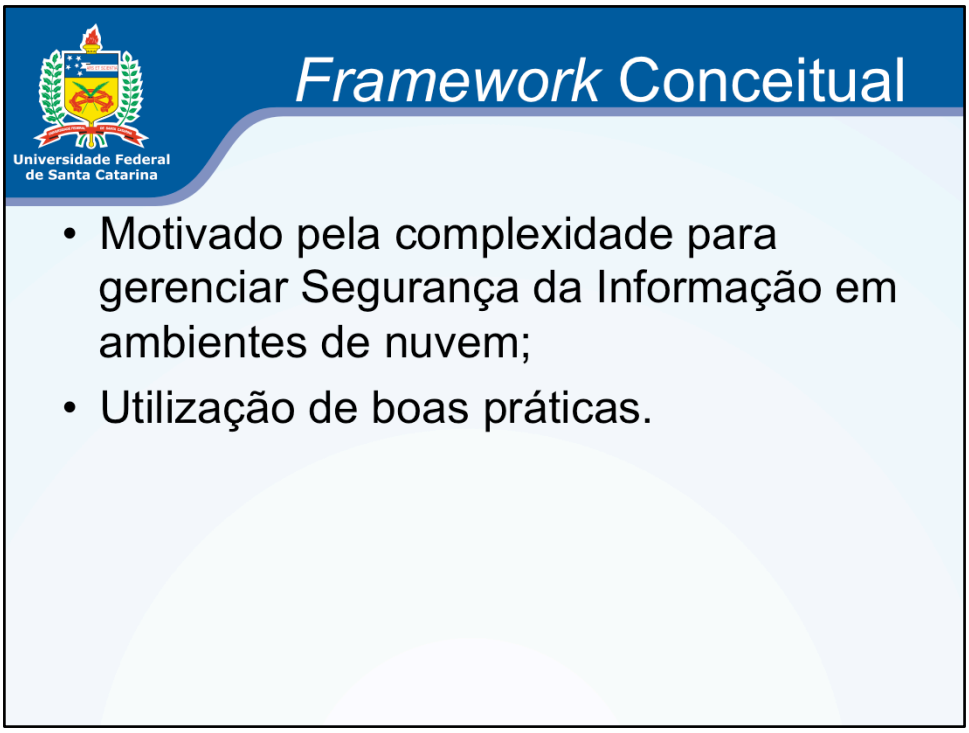
1. Seguindo a ideia de redução de custos, proporcionando economia com aquisição de equipamentos e licenças de programas, praticidade e menor tempo para utilizar um ambiente completamente operacional, incorporações têm terceirizado diversos serviços.
2. Empresas de qualquer tamanho podem, dependendo de suas necessidades e prioridades, desonerar gastos de contratação de profissionais especializados, antes necessários para suprir demandas pequenas. Assim, tarefas rotineiras de gerenciamento, manutenção e atualização de programas são incluídas no contrato de prestação de serviço.
3. Outros benefícios seriam elasticidade, melhor qualidade de serviço e alocação interna de recursos mais efetiva.



1. **Serviços de provedores e gerenciamento de níveis de serviço**: analisar cuidadosamente os contratos e fiscalizar meticulosamente a prestação e a satisfação das cláusulas contratuais. Devem ser previstas multas ou créditos nos casos de indisponibilidades superiores ao níveis de serviço acordados. A possibilidade de haver impacto para o negócio do cliente por falhas de segurança.
2. **Interrupção de serviços**: a perda de dados relacionada à interrupção tem sido uma grande preocupação. Organizações tem trabalhado para criar padronizações e certificações para endereçar a continuidade do negócio.
3. **Gerenciamento e controle**: Devem-se ressaltar os métodos de autorização, autenticação e controle de acesso, além da privacidade de dados e intercomunicação entre os componentes das nuvens;
4. **Acesso de usuários privilegiados**: necessidade de assegurar que dados sensíveis sejam acessados e propagados apenas por usuários privilegiados. Pode existir a necessidade de assegurar que somente os clientes tenham acesso a esses dados;



1. **Conformidade com legislações e regulamentações**: provedores precisam ter certificados de segurança, auditoria externa e estar em conformidade com regulamentações, legislações e padronizações locais. Clientes precisam estar cientes de que o provedor deverá seguir os requisitos legais sob autorização deles;
2. **Rastreabilidade e perícia**: provedores devem fornecer meios para levantar evidências, investigar e responder a pedidos de autoridades. Deveriam responder e ressarcir os clientes por perdas ou indisponibilidade ou ainda descoberta de dados dos clientes .
3. **Localização de dados**: provedores devem fornecer a localização dos dados dos clientes; **Segregação de dados**: clientes podem requerer como a segregação dos dados é feita. Mecanismos de criptografia podem ser utilizados, no entanto, acidentes podem ocorrer e perda de todos os dados;
4. **Recuperação** em caso de desastre**.**
5. **Portabilidade e interoperabilidade**: podem ser consideradas quebras de contrato, aquisições de provedores.

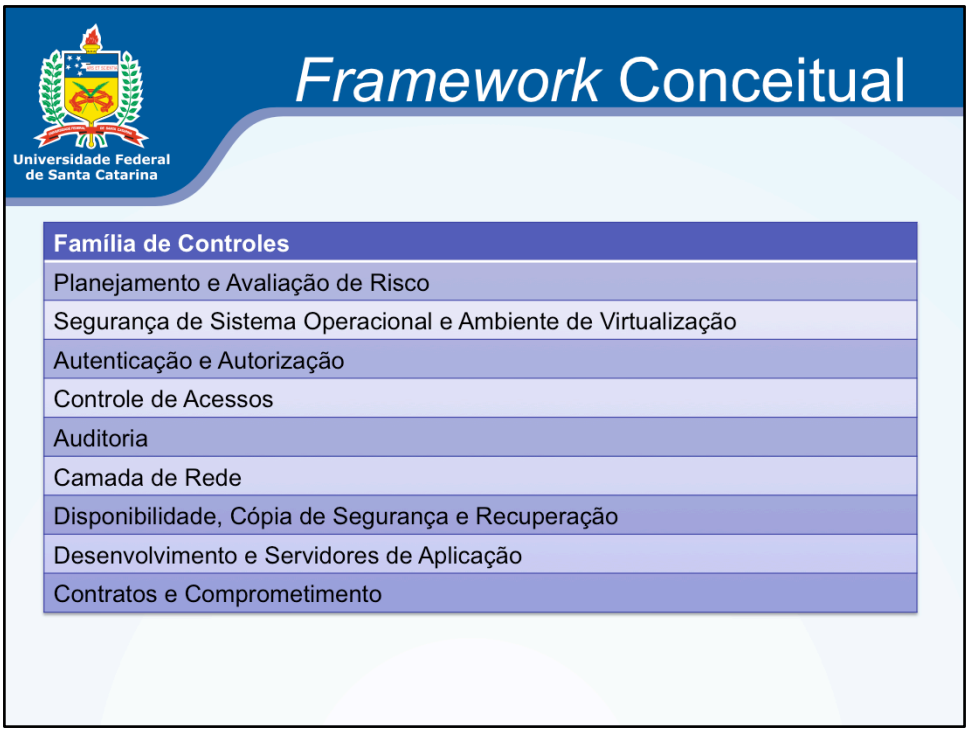


1. Em face à complexidade que está posta para gerenciar a Segurança da Informação em ambientes privados e, ainda mais complexos, públicos ou híbridos na nuvem, existe a necessidade de implementar processos para ajudar a endereçar os possíveis riscos associados ao ambiente de banco de dados. Para dar suporte ao método serão utilizados como referência algumas padronizações e boas práticas em Tecnologia da Informação.
2. Para prover boas práticas para um framework de processos e apresentar atividades numa estrutura lógica e gerenciável pode-se utilizar o Control Objectives for Information and related Technology (COBIT).
3. A padronização NIST Special Publication 800-53 tem o propósito de prover meios para selecionar e especificar controles para sistemas de informação para o governo federal dos EUA.
4. COBIT: Há mais foco em controles e menos em execução. Foi criado pela IT Governance Institute (ITGI) e Information Systems Audit and Control Association (ISACA) nos anos 90

Universidade Federal de Santa Catarina

Controles

- Modelo conceitual é apresentado através de um conjunto de controles relevantes aos bancos de dados em nuvem;
- Sugerem períodos para serem verificados e
- Estabelecem prioridades para serem analisados.



1. Planejamento e Avaliação de Risco: Versões de software, procedimentos de segurança, localização, acesso da aplicação, incidentes e chaves públicas.
2. Segurança de SO e hyper: conexões de rede entre servidores, clientes, arquivos com senhas, IDS e IPS, privilégios de conexão, exportação de dados, firewall, antivírus e VPN.
3. Autenticação e autorização: auditoria de usuários, aplicação e senhas.
4. Controle de acessos: segurança granular, permissões de DBA, permissões de sistema, controle de usuário e classificação de dados.
5. Auditoria: Auditoria em falhas de inserção, de acessos.
6. Camadas de rede: portas padrão, conexões seguras, transferência de dados.
7. Disponibilidade, backup e recover: documentar processos de backup e recuperação, armazenamento de mídias, validar procedimentos.
8. Desenvolvimento e Servidores de aplicação: ambientes de produção isolados, procedimentos de replicação, segurança de usuários de portal, controle de vulnerabilidades
9. Contratos: fiscalizar SLA e suporte, ferramentas de monitoramento, treinamento, suporte à investigação, conformidade com legislações e regulamentações, término contratual, eliminação de dados.

Universidade Federal de Santa Catarina

Controles

Cada controle contém:

Campo	Descrição
Identificador	Numerados conforme a família de controles
Descrição	Foco de atenção do controle
Melhorias	Atividades desenvolvidas para melhorias
Fase	Quatro domínio de processos genéricos
Prioridade	Alta, média, baixa e documentação

Universidade Federal de Santa Catarina

Controles

Exemplos:

Controle	Família	Descrição
A5	Planejamento e Avaliação de Risco	Verificar localização física de servidores e conformidade com teorema CDP
B5	Segurança de SO e Virtualização	Assegurar privilégios mínimos de conexão
C5	Autenticação e Autorização	Alterar senhas de usuários privilegiados de sistema
D3	Controle de Acessos	Revisar permissões de sistema garantida a usuários
I7	Contratos e Comprometimento	Término contratual, migração e eliminação de dados

Planejamento e Organização Provê direções para entrega de solução e entrega de serviço. A realização da visão estratégica precisa ser planejada, comunicada e gerenciada de diferentes perspectivas;

Aquisição e Implementação Adquire ou desenvolve soluções e integra os serviços associados no processo de negócio. Garante que as soluções estão alinhados com os objetivos de negócio;

Entrega e Suporte Recebe as soluções e entrega para os usuários finais, incluindo gerenciamento de segurança e continuidade, suporte aos usuários, gerenciamento de dados e operação e

Monitoramento e Avaliação Monitora todos os processos para assegurar que o direcionamento que foi dado está sendo seguido. Assegura qualidade e conformidade com requisitos de negócio, legislações e regulamentações.

Universidade Federal de Santa Catarina

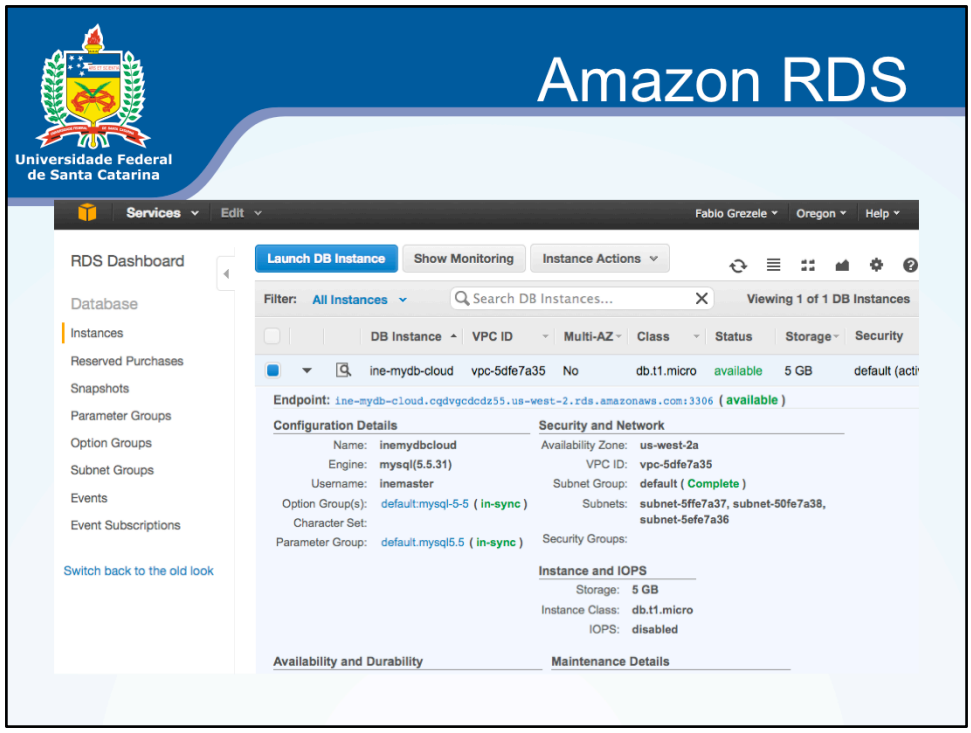
Prioridade

Prioridade	Descrição
Alta	Controles devem ser avaliados ou implementados primeiramente
Média	Devem ser avaliados ou implementados depois dos de prioridade Alta e antes dos de prioridade Baixa
Baixa	Devem ser avaliados ou implementados depois dos de prioridades Alta e Baixa
Documentação	Devem ser utilizados apenas para gerar documentação para consultas ou análises futuras

Avaliação de Controles

Provedores analisados:

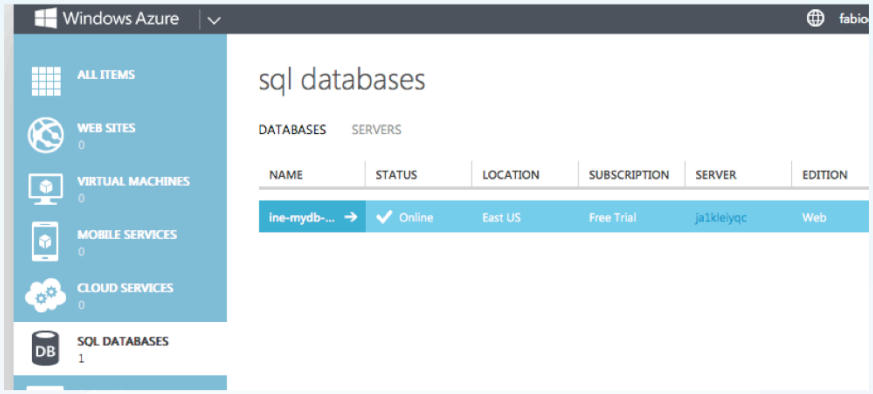
- Amazon Relational Database Service (MySQL);
- Microsoft Windows Azure SQL Database e
- Oracle Database Cloud Service.

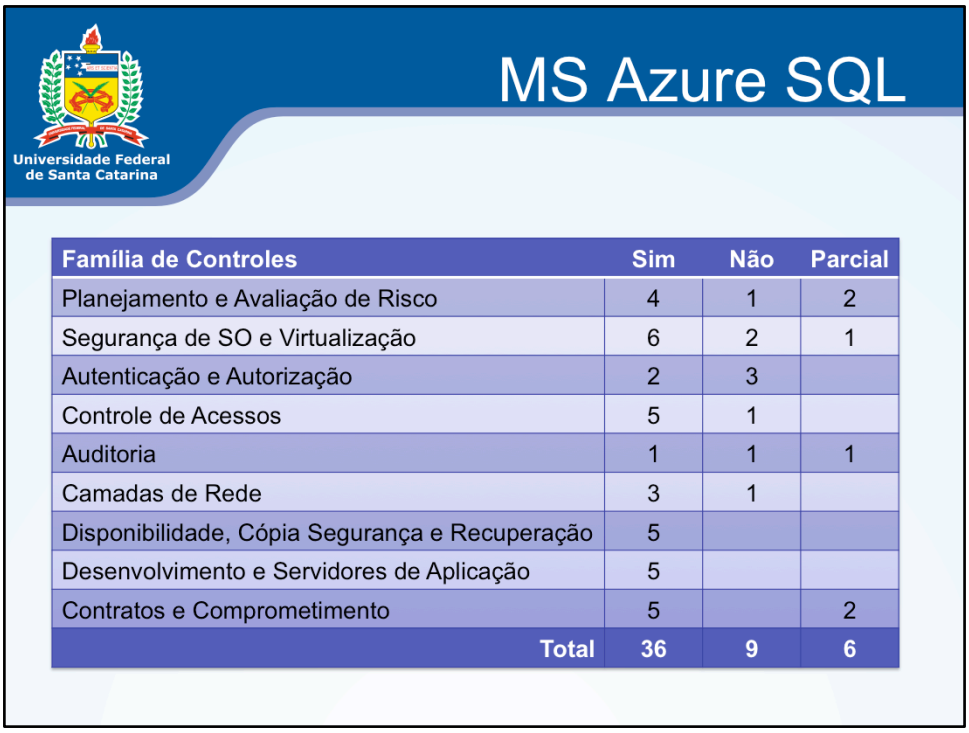

Universidade Federal de Santa Catarina
Amazon RDS
Services
Edit
Fabio Grezele
Oregon
Help
RDS Dashboard
Database
Instances
Reserved Purchases
Snapshots
Parameter Groups
Option Groups
Subnet Groups
Events
Event Subscriptions
Switch back to the old look
Launch DB Instance
Show Monitoring
Instance Actions
Filter: All Instances
Search DB Instances...
Viewing 1 of 1 DB Instances
DB Instance
VPC ID
Multi-AZ
Class
Status
Storage
Security
ine-mydb-cloud
vpc-5dfe7a35
No
db.t1.micro
available
5 GB
default (acti
Endpoint: ine-mydb-cloud.cqdvgcdcdz55.us-west-2.rds.amazonaws.com:3306 (available)
Configuration Details
Name: inemydbcloud
Engine: mysql(5.5.31)
Username: inemaster
Option Group(s): default:mysql-5-5 (in-sync)
Character Set:
Parameter Group: default.mysql5.5 (in-sync)
Security and Network
Availability Zone: us-west-2a
VPC ID: vpc-5dfe7a35
Subnet Group: default (Complete)
Subnets: subnet-5ffe7a37, subnet-50fe7a38, subnet-5efe7a36
Security Groups:
Instance and IOPS
Storage: 5 GB
Instance Class: db.t1.micro
IOPS: disabled
Availability and Durability
Maintenance Details

Família de Controles	Sim	Não	Parcial
Planejamento e Avaliação de Risco	6		2
Segurança de SO e Virtualização	10		
Autenticação e Autorização	6		
Controle de Acessos	6		
Auditoria		1	2
Camadas de Rede	2	1	
Disponibilidade, Cópia Segurança e Recuperação	4		
Desenvolvimento e Servidores de Aplicação	4		1
Contratos e Comprometimento	7		
Total	**45**	**2**	**5**

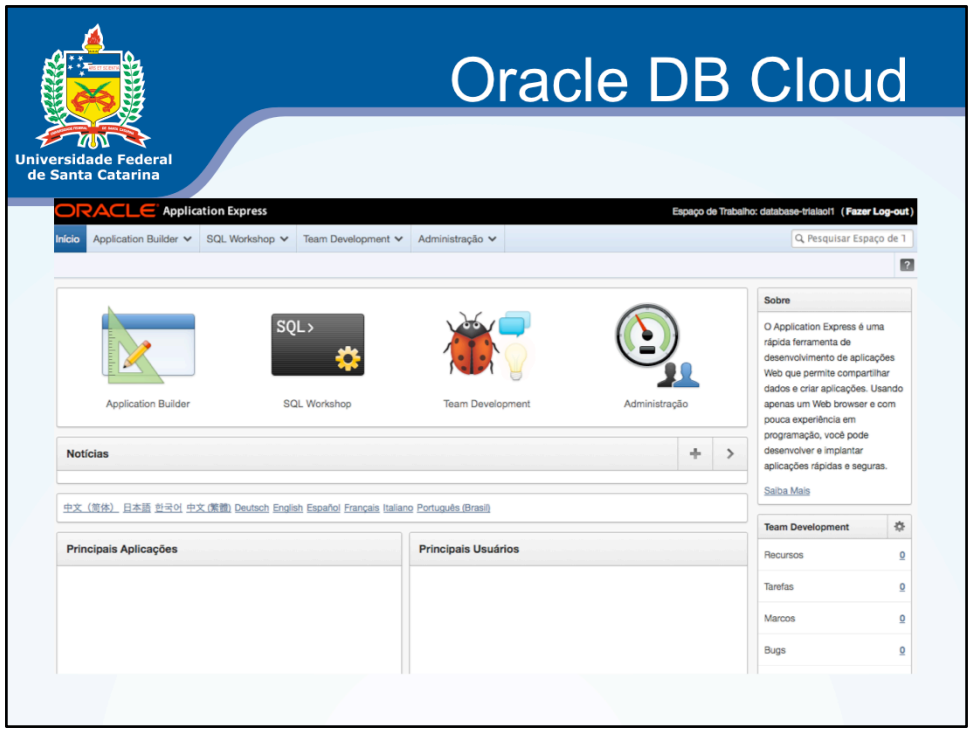
Universidade Federal de Santa Catarina

MS Azure SQL





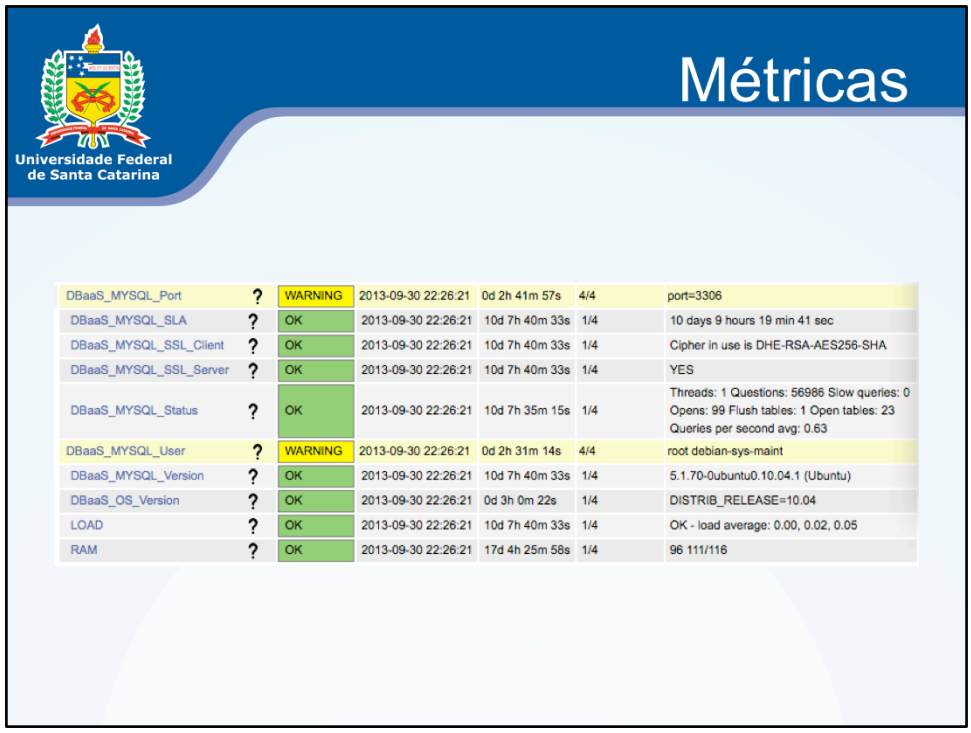
Família de Controles	Sim	Não	Parcial
Planejamento e Avaliação de Risco	4	1	2
Segurança de SO e Virtualização	6	2	1
Autenticação e Autorização	2	3	
Controle de Acessos	5	1	
Auditoria	1	1	1
Camadas de Rede	3	1	
Disponibilidade, Cópia Segurança e Recuperação	5		
Desenvolvimento e Servidores de Aplicação	5		
Contratos e Comprometimento	5		2
Total	**36**	**9**	**6**


Universidade Federal de Santa Catarina
Oracle DB Cloud
ORACLE Application Express
Espaço de Trabalho: database-trialaol1 (Fazer Log-out)
Início
Application Builder
SQL Workshop
Team Development
Administração
Pesquisar Espaço de T
Application Builder
SQL Workshop
Team Development
Administração
Sobre
O Application Express é uma rápida ferramenta de desenvolvimento de aplicações Web que permite compartilhar dados e criar aplicações. Usando apenas um Web browser e com pouca experiência em programação, você pode desenvolver e implantar aplicações rápidas e seguras.
Saiba Mais
Notícias
中文（简体） 日本語 한국어 中文 (繁體) Deutsch English Español Français Italiano Português (Brasil)
Principais Aplicações
Principais Usuários
Team Development
Recursos 0
Tarefas 0
Marcos 0
Bugs 0

Universidade Federal de Santa Catarina

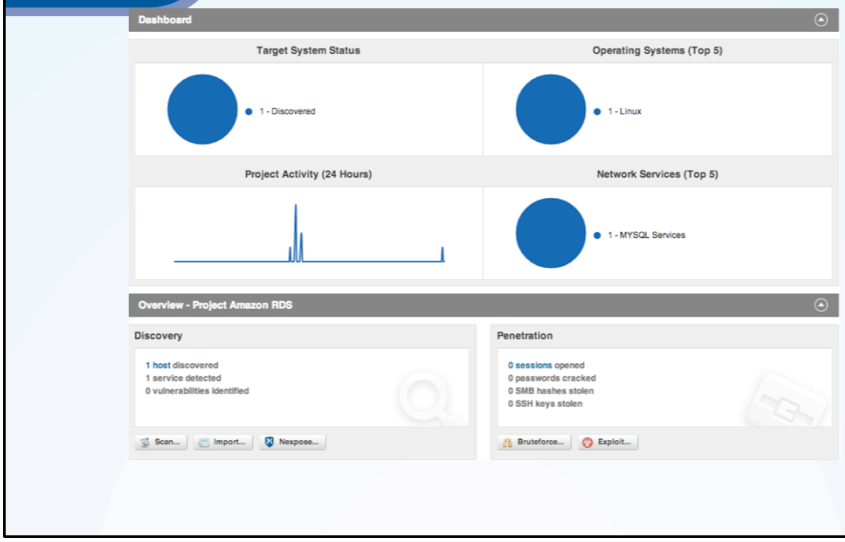
Oracle DB Cloud

Família de Controles	Sim	Não	Parcial
Planejamento e Avaliação de Risco	6	1	1
Segurança de SO e Virtualização	9		
Autenticação e Autorização	4	1	1
Controle de Acessos	4	1	
Auditoria	2		1
Camadas de Rede	2		
Disponibilidade, Cópia Segurança e Recuperação	3	2	
Desenvolvimento e Servidores de Aplicação	3		2
Contratos e Comprometimento	5		2
Total	**38**	**5**	**7**


Universidade Federal
de Santa Catarina
Métricas
DBaaS_MYSQL_Port ? WARNING 2013-09-30 22:26:21 0d 2h 41m 57s 4/4 port=3306
DBaaS_MYSQL_SLA ? OK 2013-09-30 22:26:21 10d 7h 40m 33s 1/4 10 days 9 hours 19 min 41 sec
DBaaS_MYSQL_SSL_Client ? OK 2013-09-30 22:26:21 10d 7h 40m 33s 1/4 Cipher in use is DHE-RSA-AES256-SHA
DBaaS_MYSQL_SSL_Server ? OK 2013-09-30 22:26:21 10d 7h 40m 33s 1/4 YES
DBaaS_MYSQL_Status ? OK 2013-09-30 22:26:21 10d 7h 35m 15s 1/4 Threads: 1 Questions: 56986 Slow queries: 0 Opens: 99 Flush tables: 1 Open tables: 23 Queries per second avg: 0.63
DBaaS_MYSQL_User ? WARNING 2013-09-30 22:26:21 0d 2h 31m 14s 4/4 root debian-sys-maint
DBaaS_MYSQL_Version ? OK 2013-09-30 22:26:21 10d 7h 40m 33s 1/4 5.1.70-0ubuntu0.10.04.1 (Ubuntu)
DBaaS_OS_Version ? OK 2013-09-30 22:26:21 0d 3h 0m 22s 1/4 DISTRIB_RELEASE=10.04
LOAD ? OK 2013-09-30 22:26:21 10d 7h 40m 33s 1/4 OK - load average: 0.00, 0.02, 0.05
RAM ? OK 2013-09-30 22:26:21 17d 4h 25m 58s 1/4 96 111/116

Análise de Vulnerabilidades

Universidade Federal de Santa Catarina




Universidade Federal
de Santa Catarina
Fábio Grezele
fgrezele@inf.ufsc.br