Fábio Grezele

SEGURANÇA EM SERVIÇOS DE BANCO DE DADOS EM NUVEM: CONTROLES PARA ACORDOS DE NÍVEIS DE SERVIÇOS

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do Grau de Mestre em Ciência da Computação.
Orientador: Prof. Dr. Carlos Becker Westphall

Florianópolis

2013

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Grezele, Fábio
Segurança em Serviços de Banco de Dados em Nuvem : Controles para Acordos de Níveis de Serviços / Fábio Grezele ; orientador, Carlos Becker Westphall - Florianópolis, SC, 2013.
114 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da Computação. 2. Banco de Dados como Serviço em Nuvem. 3. Segurança de Banco de Dados em Nuvem. 4. Controles Internos. 5. Acordo de Nível de Serviço. I. Westphall, Carlos Becker. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Fábio Grezele

SEGURANÇA EM SERVIÇOS DE BANCO DE DADOS EM NUVEM: CONTROLES PARA ACORDOS DE NÍVEIS DE SERVIÇOS

Esta Dissertação foi julgada adequada para a obtenção do Título de "Mestre em Ciência da Computação", e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Florianópolis, 02 de agosto 2013.

Prof. Dr. Ronaldo dos Santos Mello
Coordenador

Banca Examinadora:

Prof. Dr. Carlos Becker Westphall
Orientador

Prof. Dr. João Bosco Mangueira Sobral
Universidade Federal de Santa Catarina

Prof. Dra. Carla Merkle Westphall
Universidade Federal de Santa Catarina

Prof. Dr. Elias Procópio Duarte Júnior
Universidade Federal do Paraná

Sem medo algum da repetição ou quiçá costume inveterado, incluindo ainda uma pitada de irreverência e outra de reverência, este trabalho é dedicado a Inês Grezele, Nossa Mãe; se está lendo isto, saiba que, sem esses suportes e essa luz, nada seria possível...

AGRADECIMENTOS

Existe uma quantidade grande de pessoas a agradecer pela realização deste trabalho, pois, por menor que seja a contribuição de cada um, ela, ainda, é muito importante.

Alguns tiveram destaque grande e ressaltam-se os Professores Carlos Becker Westphall, Carla Merkle Westphall. Especialmente, grande gratidão ao Professor João Bosco Mangueira Sobral pelas imensas horas dedicadas, além de finais de semana. Também agradeço ao Professor Elias Procópio Duarte Júnior pelas sugestões e contribuições realizadas para o aperfeiçoamento deste trabalho.

Além disso, não se pode esquecer os diversos professores da UFSC que apoiaram durante todo o trajeto e realização de atividades de pós-graduação, os vários funcionários da Universidade que sempre foram diligentes, em especial, a Katiana de Castro Silva, o apoio dos colegas de curso, notadamente, Pedro Vitti.

Traz à memória o que nunca pode ser dispensado, o apoio incondicional da família, de sua afetividade, carinho, de momentos de lazer e, também, invocação e convocação ao exercício de pensar e escrever. Destacam-se Joabel Moia, Antonio Carlos Espit e Vania Inês Grezele.

Que ninguém se engane, só se consegue a simplicidade através de muito trabalho.

Clarice Lispector

RESUMO

Computação em nuvem surgiu como meio para economia de recursos através do compartilhamento de estruturas em sistemas distribuídos. Dentre os diversos modelos de entrega de serviços em nuvem estão os bancos de dados. No entanto, em ambientes corporativos, a segurança das aplicações com bancos de dados em nuvem, torna-se uma preocupação. Desde 1997, trabalhos de pesquisa vêm sendo desenvolvidos com o objetivo de minimizar alguns dos diversos problemas de segurança apontados, principalmente os relativos aos requisitos de confidencialidade. Esta dissertação focaliza o problema de segurança que pode ser encontrado, quando se celebram acordos de níveis de serviço (SLA) e contratos de serviço para bancos de dados em nuvem. No sentido de averiguar a segurança e tratar riscos, é proposto a utilização de um *framework* conceitual construído com um conjunto de controles internos para orientar clientes e provedores no estabelecimento de níveis de segurança. Com a utilização deste *framework*, controles internos foram implantados em ambientes de laboratório para nuvens públicas e privadas. Estudos de caso e análise de vulnerabilidades foram realizados para verificação da segurança, permitindo obter importantes resultados, tais como: viabilizar a escolha de provedores de serviços que possuem os controle desejados; criar métricas para o monitoramento de serviços; adequar e utilizar o PCMONS (*Private Cloud MONitoring System*) para realizar o monitoramento; integrar controles aos contratos de serviços e fiscalizar acordos de níveis de serviços.

Palavras-chave: Computação em Nuvem. Banco de Dados como Serviço em Nuvem. Segurança de Banco de Dados em Nuvem. Controles Internos. Acordo de Nível de Serviço. Framework Conceitual

ABSTRACT

Cloud computing enables resource savings through IT infrastructure sharing in distributed systems. Databases are one of cloud service delivery models. However, application security in cloud databases is a concern in enterprise environments. Since 1997, scientific researches have been developed in order to minimize some of these security problems, especially those relating to confidentiality. This master thesis focuses on the security problem, which can be found when entering into service level agreements (SLA) and service contracts. In order to investigate the security levels and risk treatment, we have proposed the use of a conceptual framework built with a set of internal controls to guide clients and providers for establishing acceptable security levels. By using this framework, internal controls were implemented in laboratory environment for public and private clouds. Case studies and vulnerabilities analysis were executed in order to investigate the security assurance. Important results were achieved, such as: to guide the choice of service providers holding the desired controls; create metrics for monitoring services; adapt and use of PCMONS (Private Cloud MONitoring System) monitoring tool; include controls into service contracts and manage service level agreements.

Keywords: Cloud Computing. Database as a Service. Database Security. Internal Controls. Service Level Agreement. Conceptual Framework.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

Este trabalho trata sobre segurança de banco de dados em ambientes de computação em nuvem. Tal segurança é baseada, essencialmente, sobre a aplicação de controles internos em um Sistema de Gerenciamento de Banco de Dados, definidos no contexto de um acordo de nível de serviço (do Inglês, SLA – *Service Level Agreement*) ou, mais abrangentemente, de um contrato de prestação de serviço. SLA é o único documento legal entre o provedor e o cliente, fazendo desse documento uma peça chave para o serviço, a melhor maneira de mitigar e gerenciar riscos, compreender as garantias disponíveis, descobrir e lidar com inseguranças (WEIS; ALVES-FOSS, 2011). Ainda, SLA é frequentemente referenciado como tempo de disponibilidade de um serviço. Alguns dos termos do acordo de nível de serviço e alguns controles internos serão verificados ou medidos utilizando a ferramenta PCMONS (*Private Cloud MONitoring Systems*) (CHAVES, 2010).

Do ponto de vista do crescimento da quantidade de informação gerada em um ambiente de nuvem computacional, associado aos procedimentos para administrar um banco de dados ou realizar desenvolvimento, fez com que surgisse um novo paradigma que é o de fornecer banco de dados como um serviço. Da sigla em Inglês, "DBaaS" ou "Database as a Service" compreende-se o compartilhamento de recursos de banco de dados para um ambiente de nuvem. Ainda pode ser caracterizado como uma especialização do paradigma "SaaS" ou "(Software as a Service)" (FERRARI, 2009). Alguns autores, ainda, citam essa especificação como DaaS (SAKR et al., 2011; WEIS; ALVES-FOSS, 2011; ANSTETT et al., 2009).

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 podem ser incluídas em um contrato de prestação de serviço. Do contrato, ainda consta o acordo de nível de serviço que comumente representa o tempo de disponibilidade de um serviço. Outros benefícios desse modelo seriam elasticidade, melhor qualidade de serviço, alocação interna de recursos mais efetiva. Uma das desvantagens de um DBaaS é a percepção da perda de controle sobre os dados. A transparência, que é uma propriedade de um sistema distribuído, reforça essa característica do modelo. Soma-se ainda que são necessários esforços maiores para evitar

manipulação, perda e alteração não autorizada de dados nesse novo ambiente.

Relativo à segurança da informação no banco de dados na nuvem, existem requisitos primordiais como confidencialidade e disponibilidade. Neste trabalho, a criptografia será verificada, através de controles internos, como garantia da privacidade dos dados, no sentido de que a informação poderá ser decifrada para a instituição proprietária dos dados, ou outros que ela venha a definir. Porém, os esquemas de criptografia podem ser mantidos pelos provedores de serviço e compartilhados com seus clientes, estabelecendo assim uma relação de confiança entre provedor e cliente. Já o requisito de disponibilidade do banco será verificado através da ferramenta que verificará a métrica de SLA. Outros requisitos de segurança, como autenticação, autorização e controle de acesso serão verificados através de controles internos. Com relação ao não repúdio, poderá ser verificado através de controles de auditoria. Entretanto, o requisito de integridade não será abordado, dado a capacidade de alteração que um banco de dados possui, tornando bastante dispendioso a verificação da integridade. Atualmente, fornecedores de Sistemas Gerenciadores de Banco de Dados possuem ferramentas internas para essa verificação. No entanto, controles de verificação de integridade de cópias de segurança são propostos.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Num ambiente de computação em nuvem, à medida em que o número de aplicações e sistemas cresce, o risco de exposição de bases de dados também cresce. Nesse sentido, a proteção de informações sensíveis passa a ser de suma importância. Organizações diferentes podem sofrer de maneiras diferentes com a exposição não autorizada de dados. Dependendo da sensibilidade da informação, o valor agregado a ela justifica que contratos de serviços sejam melhor elaborados, prevendo retorno financeiro baseado no valor da informação descoberta. Além disso, métricas para SLA deveriam ser bem definidas nos contratos e verificadas através de ferramentas.

Ademais, ao migrar uma base de dados para a nuvem, alguns desafios devem ser analisados. Dentre eles, devem ser levados em conta os canais de comunicação que estão na Internet; compartilhamento de recursos de armazenamento e memória num *data center*; uso de novas tecnologias; questões legais como contratos com provedores de serviços, legislações locais e internacionais. Nesse caso, deve-se verificar as leis das regiões do planeta onde os dados serão trafegados ou armazenados.

Vulnerabilidades de segurança são tipicamente categorizadas como: visualização não autorizada de dados, modificação incorreta de dados e indis-

ponibilidade de dados (BERTINO; SANDHU, 2005). Conforme a sensibilidade que um dado possui em uma organização, pode-se dar prioridade para qual ou quais dos três requisitos da segurança da informação sejam considerados: confidencialidade, integridade e disponibilidade. Neste trabalho, será dado prioridade à confidencialidade e disponibilidade.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Propiciar meios, através de controles internos no ambiente do cliente de um serviço de bancos de dados em nuvem, para garantir a segurança de bancos de dados nesse ambiente. Pode-se observar que empresas transferem seus dados para a nuvem, sem fazer a verificação adequada da segurança da informação, nem dos níveis de contrato de serviço. Um provedor deve garantir privacidade, robustez, completude e isolamento necessários para o andamento dos negócios dos clientes.

1.2.2 Objetivos Específicos

Em meio a uma variedade de tecnologias e diferentes fornecedores, é preciso trazer à mente e rever a importância de se ter um *framewok* 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 framework reconhecidos internacionalmente, boas práticas e guias, pretende-se implementar framework apropriado para DBaaS. Assim, tem-se como objetivos:

- Avaliar e analisar estruturas e serviços de banco de dados em nuvem;
- Definir e declarar objetivos de controles internos;
- Fornecer subsídios para gerenciar e monitorar acordos e contratos de serviço e
- Estabelecer períodos para verificação de controles internos.

1.3 HISTÓRICO DA PESQUISA

Esta seção mostra um histórico da pesquisa sobre bancos de dados como serviço em ambiente de nuvem, abordando os aspectos de segurança e de contratos de níveis de serviço.

Em 1997, com relação à escalabilidade de serviços em rede, (FOX et al., 1997) identificaram três requisitos fundamentais: escalabilidade incremental, disponibilidade durante 24 horas por dia com mascaramento de falhas e custo efetivo. Propuseram uma arquitetura para construir serviços de rede escalável em que dão prioridade para alta-disponibilidade e menor consistência, uma semântica de dados mais fraca do que ACID (Atomicidade, Consistência, Isolamento e Durabilidade). Em contexto de base de dados em nuvem, esse modelo permite que a atualização de dados entre bases distribuídas em redes distintas seja temporariamente tolerada até que todas as cópias fiquem idênticas. Os autores argumentaram que respostas baseadas em dados desatualizados ou regerada podem ter mais valor do que respostas entregues com espera por consistência.

Em 2002, a Universidade da Califórnia e a IBM (HACIGUMUS; IYER; MEHROTRA, 2002) publicaram o artigo *Providing Database as a Service*. Nesse artigo, os autores exploraram um novo paradigma para gerenciamento de dados, no qual um provedor de serviços hospedava "base de dados como serviço", Assim, fornecia aos clientes mecanismos para criar, armazenar e acessar suas bases de dados num local de hospedagem. Esse modelo desonerava a necessidade de organizações na aquisição de software e hardware caros, lidar com atualizações de software, contratar profissionais para tarefas de administração e manutenção, as quais ficariam a cargo do provedor desse serviço. Entre os primeiros desafios introduzidos pelo bancos de dados como serviço são: a sobrecarga de acesso a dados remotos, uma infraestrutura para garantir a privacidade dos dados e uma interface para o usuário acessar tal serviço. Os autores identificaram que a privacidade dos dados era um problema particularmente vital e propuseram soluções alternativas baseadas em criptografia.

Em 2008, o serviço de armazenagem da *Amazon Simple Storage Service (S3)* foi abordado em (BRANTNER et al., 2008). O propósito do artigo foi demonstrar as oportunidades e limitações de usar S3 como um sistema de armazenamento de aplicações de bancos de dados de propósito genérico que envolviam pequenos objetos e atualizações frequentes. S3 proporcionou escalabilidade "infinita" e alta disponibilidade a baixo custo. Além disso, o custo, o desempenho e propriedades de consistência também foram estudados.

Em 2008, a organização Gartner (BRODKIN, 2008) publicou um relatório sobre os sete riscos associados à computação em nuvem, orientando

clientes na escolha de fornecedor de serviços em nuvem. Foram citados os riscos: 1. Acesso de usuário privilegiado; 2. Conformidade com regulamentação; 3. Localização dos dados; 4. Segregação dos dados; 5. Recuperação; 6. Suporte à investigação e 7. Viabilidade dos termos de contrato de longo prazo.

Em 2009, foi publicado um artigo que discutia as limitações e oportunidades de implantação de gerenciamento de dados sobre as plataformas emergentes de computação em nuvem (ABADI, 2009). Os autores inferiram que bases de dados analíticas são melhor adaptadas a um ambiente de nuvem do que bases de dados transacionais e expressaram a necessidade de criação de um ambiente de base de dados específico para nuvem.

Artigo publicado em 2009 (KANDUKURI; PATURI; RAKSHIT, 2009), os autores baseando-se nos sete riscos identificados pela organização Gartner, propuseram a padronização de SLA, como garantia ao cliente de maior segurança no serviço de nuvem.

Em 2009, na Universidade de Insubria, Itália (FERRARI, 2009), a autora expõe a análise sobre as mais importantes brechas de segurança e privacidade, as quais podem surgir num modelo de banco de dados como um serviço, revendo o estado da arte na visão dos requisitos identificados de privacidade e segurança. Tal análise mostra que existem ainda muitos problemas em aberto, permanecendo não resolvidos.

Em 2010, no Instituto Federal de Tecnologia de Zurique, uma tese de doutorado foi defendida (KRASKA, 2010) com o propósito de explorar como aplicações de bases de dados na web com requisitos de consistência alta ou baixa podem ser desenvolvidas e implementadas em diferentes provedores de infraestrutura na nuvem. Isso foi motivado pelo fato de que não existe consenso em serviços de provedores de nuvem. Diferentes provedores oferecendo funcionalidades e interfaces diferentes, o que dificulta a portabilidade de uma aplicação de uma provedor para outro. O autor argumenta que a consistência é comprometida para garantir escalabilidade e disponibilidade.

Ainda em 2010, a Cloud Security Alliance (CSA) (ALLIANCE, 2010) criou uma matriz de controles com o objetivo de guiar provedores na garantia de princípios de segurança da informação para clientes de serviços genéricos de nuvem –não sendo específico para banco de dados. Propuseram um *framework* de controles que detalhava sobre conceitos e princípios de segurança em 13 domínios. Eles se basearam em padrões de segurança aceitos pela indústria, além de regulamentações e outros *frameworks* de controles como ISO 27001/27002, ISACA COBIT, PCI, NIST. A matriz fornece a organizações detalhamentos e clareza relativos à segurança em nuvem. Diferentemente da CSA, a proposta deste trabalho é a criação de um *framework* com controles de segurança relativos especificamente ao serviço de banco de dados em nuvem.

Em 2011 (WEIS; ALVES-FOSS, 2011), os autores levantam diversas questões relevantes e preocupações relativas a DBaaS, incluindo segurança, confiança, expectativas de clientes, regulamentações e problemas de desempenho. Algumas soluções de propostas incluem gerenciamento de risco e melhores acordos contratuais antes da discussão de uso de uma solução específica de DBaaS. A maioria das soluções cobrem técnicas de autenticidade e criptografia de base de dados. O objetivo é a educação do leitor para a adoção de uma solução quando os problemas e insegurança são entendidos.

Em 2011, (FRANK, 2011) propõe o uso de ACID menos restritivo para consistência de múltiplas bases de dados em ambientes distribuídos. Um modelo de transações é proposto para reduzir ou prevenir as consequências da falta de consistência.

Em 2012 (BUTLER, 2012), novamente o Gartner mostra que fornecedores de serviços de nuvem são relutantes na inclusão de cláusulas contratuais (SLA) sobre a perda de dados, ocasionados por problemas diversos. Alguns provedores podem não divulgar informações porque poderiam representar um ameaça de segurança. Provedores, muitas vezes, alegam um alto nível de disponibilidade e confidencialidade dos dados do usuário, mas fornecem poucas evidências para verificar essas afirmações.

Ainda em 2012, (PAL et al., 2012), focando na falta de considerações sobre segurança em contratos de prestadoras de serviços de nuvem, propõem a criação de um *frawework* para garantir segurança para ambientes genéricos em nuvem. Subdividiram-no em oito domínios: 1. Segurança física; 2. Segurança de Rede e Perímetro; 3. Segurança de imagem virtual; 4. Gerenciamento de identidade e acesso; 5. Segurança de dados e segurança de armazenamento; 6. Transmissão; 7. Monitoramento e 8. Segurança em nível do cliente.

Diferentemente dos trabalhos citados acima, este trabalho apresenta um conjunto significativo de controles internos, para obtenção de segurança da informação em banco de dados em ambientes de nuvem. Eles podem ser verificados através das ferramentas de monitoramento e também através da aplicação desses controles por um *framework* produzido para este fim. Como parte adicional, é mostrado como a segurança, através de controles, pode ser verificada por auditoria através de análise de vulnerabilidades.

1.4 ORGANIZAÇÃO DO TRABALHO

No capítulo 1 está a introdução deste trabalho, apresentando a área de pesquisa, contextualização e os desafios. Também estão expostos os objetivos pretendidos com uma hipótese que será averiguada ao longo da desta

dissertação.

Já no capítulo 2 está a revisão bibliográfica, apresentando a arquitetura de computação em nuvem, definições comumente aceitas e modelos de serviços. Traz ainda mais detalhes sobre serviços de banco de dados na nuvem e suas características. Mostra diferenças e propriedades de bancos de dados e como elas podem alterar a implementação do serviço.

O capítulo 3 apresenta a proposta, um *framework* conceitual para organizar e auxiliar organizações a avaliar banco de dados entregues como serviço. Será introduzido um método baseado em controles internos para avaliação dos serviços de nuvem e requisitos de negócio. Enfim, é exposto um conjunto reduzido de controles, porém significativo, que poderá ser estendido com controles comuns para bancos de dados.

É exibida, no capítulo 4, a validação da proposta. São avaliados alguns controles e a aderência de fornecedores de serviços de banco de dados em nuvem. Além disso, são analisados documentos, contratos e acordos para estabelecimento de serviços. Ainda, são propostas métricas para verificação de alguns controles internos através de ferramenta de monitoramento. Comentários sobre resultados obtidos estão na seção 4.4.

Enfim, no capítulo 5 se exibe a conclusão do trabalho e propostas para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo aborda sucintamente os conceitos relativos à computação em nuvem utilizados neste trabalho, contendo as seções sobre computação em nuvem, modelos de serviços, segurança da informação relativa ao ambiente de bancos de dados em nuvem, além de propriedades e características relativas a esse ambiente. Ainda, será dado um enfoque sobre como as áreas de armazenamento podem ser disponibilizadas.

2.1 O QUE É COMPUTAÇÃO EM NUVEM?

Computação em nuvem é um modelo de computação distribuída em larga escala que habilita acesso à rede sob demanda, conveniente e ubíqua para o compartilhamento de recursos computacionais tais como redes, servidores, armazenamento, aplicações e serviços (MELL; GRANCE, 2011). Esses recursos podem ser facilmente fornecidos ou removidos com esforço mínimo de gerenciamento ou mínima interação do provedor de serviços. É ainda determinado por fatores econômicos, evoluindo a partir da computação em *grid* (FOSTER et al., 2008), utilizando muitas tecnologias, aplicações e infraestruturas, conforme necessidades do cliente. A figura 1, baseada em

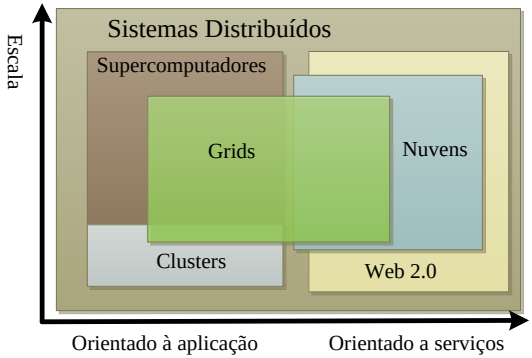


Figura 1 – Relacionamentos entre Sistemas Distribuídos

(FOSTER et al., 2008), mostra os relacionamentos dessas tecnologias, no contexto de sistemas distribuídos.

Grids e nuvens possuem diversas semelhanças como arquitetura e tecnologia, no entanto, diferem em outros aspectos como modelo de negócios, segurança, aplicações e programação, modelo para computação de dados e armazenamento.

O modelo de nuvem é composto pelas seguintes características:

Serviços sob demanda Clientes podem unilateralmente requisitar serviços automaticamente conforme suas necessidades sem a interação de pessoal técnico do 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. Existe transparência de localização em que não se tem controle ou conhecimento da localidade do recurso. No entanto, é possível especificar a localização em um nível mais alto de abstração, por exemplo, país, estado, *data center*.

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, além de processamento. A cobrança geralmente é baseada pelas medidas de uso.

Computação em nuvem pode ser implementada seguindo os seguintes modelos:

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.

A evolução da computação em nuvem ocorreu devido ao uso combinado de recursos de infraestrutura e armazenamento distribuídos como se pode ver na computação em grid. A computação em nuvem expande o conceito de sistemas distribuídos agregando fatores econômicos, criando novos modelos (FOSTER et al., 2008).

2.2 MODELOS DE SERVIÇOS DA COMPUTAÇÃO EM NUVEM

Segundo (MELL; GRANCE, 2011), os serviços de nuvem podem ser divididos em três principais modelos: Infraestrutura, Plataforma e Software como Serviço.

2.2.1 Software como Serviço

Do Inglês, *Software as a Service (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. Dentre os provedores de computação em nuvem, destacam-se como fornecedores de softwares como serviço Google Apps, Salesforce, Amazon Web Services, Amazon Relational Database Service, Microsoft Office 365 e Oracle Cloud.

2.2.2 Plataforma como Serviço

Platform as a Service (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. São exemplos de plataforma com serviço Google App Engine, Windows Azure, Salesforce Heroku.

2.2.3 Infraestrutura como Serviço

Infrastructure as a Service (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. São exemplos de infraestrutura como serviço Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3), Simple Queue Service (SQS).

2.2.4 *Multi-tenancy*

Um quarto elemento identificado para computação em nuvem, conforme (BRUNETTE; MOGULL, 2009), chama-se *multi-tenancy* –traduzido como "inquilinos múltiplos". Sob a perspectiva do provedor, diferentes clientes podem compartilhar a mesma infraestrutura, aplicações, dados, metadados e serviços. Isto implica na necessidade de aplicar políticas para segmentação, isolamento, governança, níveis de serviço, modelos de cobrança e restituição para diferentes clientes. A forma como o *multi-tenancy* é aplicado varia de provedor para provedor.

2.2.5 Base de Dados como Serviço

Database as a Service (DBaaS) – O armazenamento de dados em computação em nuvem considera a utilização de bancos de dados, os quais são

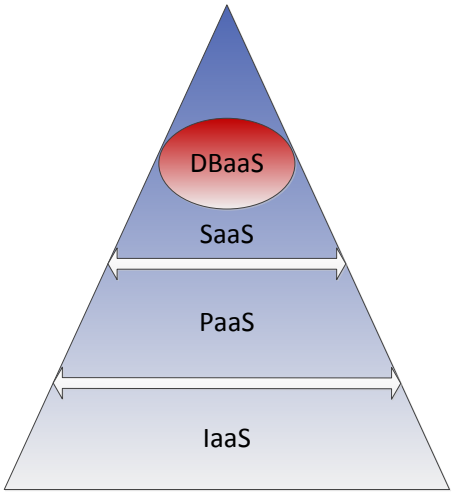


Figura 2 – Modelos de Serviço da Computação em Nuvem

disponibilizados como serviço. Banco de Dados como Serviço é uma especialização de Software como Serviço, como mostrado na figura 2. Nesse caso, os clientes possuem acesso a mecanismos para criar, armazenar, acessar e gerenciar seus bancos de dados localizadas no provedor (HACIGUMUS; IYER; MEHROTRA, 2002; FERRARI, 2009). O modelo DBaaS facilita a configuração, a operação e a escalabilidade para bancos de dados na nuvem. No entanto, outros desafios surgem concernentes à confidencialidade, uma vez que mecanismos de proteção da informação podem ser usados em determinados níveis de granularidade sobre o banco ou partes dele. Isso acarreta a preocupação sobre a segurança dos dados, posto que, embora um provedor possa não revelar, ele possui a custódia de chaves criptográficas utilizadas pelo cliente. E mais ainda, as chaves privadas podem nem ser de conhecimento do cliente, sendo gerenciadas apenas pelo provedor. No que tange a proteção de dados, o cliente é dependente dos serviços de confidencialidade do provedor.

2.3 SEGURANÇA DA INFORMAÇÃO NA NUVEM

No sentido de abordar a segurança de banco de dados na nuvem, pode-se ressaltar que a interoperabilidade entre equipamentos ou até mesmo *data centers* heterogêneos gerou diversos desafios. Apesar de *grids* serem construídos em ambientes heterogêneos, existe a centralização para administração e operação dos recursos. A segurança deve ser profundamente analisada ao se utilizar os serviços de nuvem. Segundo (BRODKIN, 2008; CARROLL; MERWE; KOTZE, 2011; BUTLER, 2012), alguns riscos devem observados:

- Serviços de provedores e gerenciamento de níveis de serviço: os clientes devem analisar cuidadosamente os provedores contratados para os serviços de nuvem 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. Outro fator relevante é a possibilidade de haver impacto para o negócio do cliente por falhas de segurança. Deveria ser de responsabilidade do provedor a criação de mecanismos de defesa ou mitigação, além de se responsabilizar por eventuais perdas ou indisponibilidade ou descoberta de dados dos clientes;

- Interrupção de serviços: Associado aos serviços e seus níveis, a perda de dados relacionada à interrupção deles tem sido um fator preocupante. Organizações tem trabalhado para criar padronizações e certificações para no sentido de evitar a interrupção e garantir a continuidade do negócio;

- Gerenciamento e controle: clientes devem estabelecer requisitos para que as ferramentas de gerenciamento e controle dos ambientes heterogêneos sejam satisfeitos. Devem-se ressaltar os métodos de autorização, autenticação e controle de acesso, além da privacidade de dados e intercomunicação entre os componentes das nuvens;

- Acesso de usuários privilegiados: necessidade de assegurar que dados sensíveis estando fora da empresa sejam acessados e propagados apenas por usuários privilegiados. Pode existir, ainda, a necessidade de assegurar que somente os clientes tenham acesso a esses dados, incluindo modelos para garantir a confidencialidade;

- Conformidade com legislações e regulamentações: provedores precisam ter certificados de segurança, auditoria externa e estar em conformidade com regulamentações, legislações e padronizações locais dos

países em que estão localizados. Clientes precisam estar cientes de que o provedor deverá seguir os requisitos legais sob autorização deles;

- Localização de dados: provedores devem fornecer a localização dos dados dos clientes e se estão em conformidade com a jurisprudência local;

- Segregação de dados: ambientes compartilhados são usados para armazenamento e clientes podem requerer como detalhes de como a segregação dos dados é feita. Mecanismos de criptografia podem ser utilizados, no entanto, acidentes podem ocorrer e perda de todos os dados. Além disso, a disponibilidade pode estar comprometida com o tratamento da informação criptografada;

- Recuperação: Mesmo não havendo a possibilidade de saber onde se localização os dados, o provedor deve fornecer um serviço de recuperação em caso de desastre;

- Rastreabilidade e perícia: Como muitos clientes utilizam ambientes em colaboração, investigação de atividades ilegais ou inapropriadas pode não ser possível. Assim, provedores devem fornecer meios para levantar evidências, investigar e responder a pedidos de autoridades. Os provedores também deveriam responder e ressarcir os clientes por perdas ou indisponibilidade ou ainda descoberta de dados dos clientes e

- Portabilidade e interoperabilidade de provedores: Clientes devem verificar a possibilidade de portar os dados de um provedor e realocá-los em infraestrutura própria ou de terceiros. Para a portabilidade podem ser consideradas quebras de contrato, aquisições de provedores ou criação de políticas diferenciadas.

Observando-se os riscos acima, percebe-se que a transparência contratual e informações mais precisas sobre a configuração da nuvem acaba, de certa forma, contrariando os próprios conceitos de nuvem em que a implementação não deveria ser relevante para os clientes. A transparência nas implementações de nuvem é necessária por motivos de regulamentação e também os contratuais em que se especifica a perda ou descoberta de dados (CHOW et al., 2009).

Os controles de segurança utilizados na nuvem não diferem, em sua maior parte, dos controles em outros ambientes de Tecnologia da Informação (TI). Entretanto, devido ao modelo diferenciado, surgiram riscos diferenciados dos tradicionais (BRUNETTE; MOGULL, 2009). A responsabilidade para a segurança pode variar muito entre clientes e provedores, conforme

modelos de serviço. Por exemplo, o IaaS do Amazon AWS EC2 dá foco à responsabilidade do provedor até a camada de virtualização do ambiente, ou seja, controles sobre a segurança física do provedor e controles sobre a segurança lógica do ambiente que envolve essa virtualização. Já o cliente é responsável pela instância virtual, incluindo sistema operacional, aplicações e dados. Para os clientes de SaaS CRM da Salesforce (BRUNETTE; MOGULL, 2009), o provedor é responsável pela segurança física, controles do ambiente e, também, infraestrutura, aplicação e dados.

Em suma, nos ambientes SaaS, os controles de segurança e seus escopos são negociados em contratos, níveis de serviço, privacidade e conformidade com legislações. Em IaaS, infraestrutura e níveis de abstração são de responsabilidade do provedor e o restante é do cliente. Um equilíbrio entre as responsabilidades de clientes e provedores pode-se observar em PaaS. Enquanto a segurança da plataforma propriamente dita pertence ao provedor, a de aplicações desenvolvidas na plataforma pertence ao cliente.

(CHOW et al., 2009) propõem o uso de *Trusted Computing Base (TCB)* e técnicas de criptografia para avaliar os problemas de segurança da informação em que a nuvem está sujeita. Esquematicamente, foram criadas três categorias que devem ser levadas em consideração:

- Segurança tradicional: ataques em nível de máquinas virtuais, vulnerabilidades associadas ao provedor de nuvem, *phishing*, ataque à rede de conexão e interconexão entre clientes, usuários e a nuvem, autenticação e autorização, perícia forense na nuvem;

- Disponibilidade: tempo em que serviços não estão indisponíveis, ponto único de falha, garantia de integridade computacional e

- Controle de dados de terceiros: se diligências e ações policiais podem ser executadas em tempo hábil, auditoria, obrigações contratuais, espionagem no provedor, portabilidade, quarteirização dos serviços de nuvem.

Em suma, as tecnologias de nuvem podem ser concebidas sem a devida atenção à segurança da informação. Para auxiliar em melhor garantia de segurança, um cliente pode incluir ou verificar a existência de cláusulas de contrato, tais como:

- Segurança física, lógica e de comunicação;

- Cópia de segurança (*backup*) e recuperação;

- Como são feitos os acesso de usuários privilegiados;

- 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.

Com relação a chaves criptográficas, um problema de gerenciamento delas é relatado: se a criptografia é necessária, então as chaves não poderiam ficar na nuvem. Esse problema seria resolvido caso houvesse um dispositivo de uso e controle exclusivo do cliente. Esse dispositivo seria responsável por decifrar os dados (WEIS; ALVES-FOSS, 2011). No entanto, essa solução, além de aumentar os custos, torna esse dispositivo um novo ponto de falha. O problema pode ser parcialmente resolvido caso se usem chaves criadas para durarem um período de tempo. Esse novo conjunto de chaves seria usado para criptografar a chave privada do banco. Um novo conjunto de chaves seria gerado periodicamente e poderia ser armazenado na nuvem. Já a chave privada deve ficar armazenada com o cliente e apenas levada criptograficamente à memória dos servidores na nuvem (WEIS; ALVES-FOSS, 2011).

A escolha de um Sistema Gerenciador de Banco de Dados (SGBD) como motor do ambiente de nuvem pode delinear a escolha dos clientes. Muitos motores possuem funcionalidades nativas, bastando sua customização para obtenção da segurança necessária. Dentre as funcionalidades, podem-se destacar: 1. Controle de usuários, papéis e atribuições; 2. Criptografia de todos os dados ou parte deles; 3. Classificação de dados; 4. Gerenciamento de identidade e 5. Auditoria.

2.3.1 Banco de Dados em Nuvem

Devido ao alto custo envolvido na aquisição de software e hardware para dar suporte a aplicações de gerenciamento de dados, o uso dos serviços de nuvem passa a ser atrativo (ABADI, 2009). Para empresas pequenas e médias, a forma de cobrança em que se paga conforme o uso, pode ser considerado fonte de economia de recursos. Os principais desafios estão na

confidencialidade onde a sensibilidade da informação e problemas de performance devem ser analisados. A competição entre empresas e furto de base de dados fez com que as corporações procurassem técnicas para preservar a privacidade e a segurança de dados (AGRAWAL et al., 2009). Nesse sentido, propriedades gerais de banco de dados (ACID – Atomicidade, Consistência, Isolamento e Durabilidade) também são levadas em conta. Além disso, propriedades relativas ao ambiente de nuvem (Teorema CDP – Consistência, Disponibilidade e Particionamento de Rede) são analisadas no que segue.

2.3.1.1 Propriedades ACID

Para garantir que as transações de um banco de dados sejam confiáveis é necessário seguir as propriedades *ACID* (RAMAKRISHNAN; GEHRKE, 2003). Assim, as transações devem ter os seguintes atributos:

- *A*tomicidade: Todas as tarefas são desempenhadas ou nenhuma delas. Ela é implementada no Sistema Gerenciador de Banco de Dados (SGBD) através dos arquivos de registro com todas as alterações feitas pelas transações;
- *C*onsistência: Os dados permanecem consistentes antes do começo da transação e depois dela;
- *I*solamento: O resultado de transações concorrentes é o mesmo que se poderia obter com elas sendo executadas em ordem serializada. Em outras palavras, dados sendo manipulados por uma transação não podem ser vistos por outras até o término (concluído com sucesso ou retorno de valores originais) da primeira e
- *D*urabilidade: Modificações feitas por transações devem persistir, mesmo em casos de falhas, defeitos ou erros (AVIZIENIS et al., 2001; WEBER, 2002). Num SGBD, a durabilidade é garantida pelos arquivos de registro com as alterações efetuadas.

Para garantir a segurança da informação em banco de dados em nuvem, os requisitos de disponibilidade, integridade e confidencialidade da informação devem ser considerados.

2.3.1.2 A Importância do Teorema CDP

Em inglês, para o teorema é utilizada a sigla CAP que significa *Consistency, Availability, Partition-tolerance*. Em (GILBERT; LYNCH, 2002)

o teorema é provado. É dito que para um serviço distribuído é impossível prover as seguintes garantias:

- *C*onsistência: relativo à atomicidade das operações web. Para garantir consistência, deverá haver uma ordem para que todas as operações se realizem tal que cada operação deve se comportar como se somente ela tivesse rodado. Isso equivale a dizer que um ambiente de memória distribuída compartilhada deve se comportar como se estivesse rodando em apenas um nó, respondendo uma operação por vez;

- *D*isponibilidade: para um sistema distribuído estar continuamente disponível, cada requisição recebida por um nó deve resultar em uma resposta. Isto é, qualquer algoritmo usado pelo serviço deve eventualmente terminar e

- *P*articionamento de rede: num modelo tolerante a partições, a rede estaria apta a perder arbitrariamente uma quantidade de mensagens enviadas de um para outro nó. Quando a rede é particionada, todas as mensagens enviadas de um nó em um componente da partição para nós em outro componente são perdidas.

Com o objetivo de diminuir o particionamento de rede, servidores únicos ou servidores num mesmo *rack* poderiam ser usados (KRASKA, 2010). Ambas as soluções não são escaláveis nem poderiam ser usadas em nuvem. Assim, para manter a disponibilidade e a consistência de dados de um DBaaS, um provedor poderia montar sua estrutura física em uma mesma partição de rede.

2.3.1.3 Características de BD em Nuvem

Estão dispostas abaixo algumas características específicas para bancos de dados em nuvem.

Dentre as características da nuvem, há a preocupação de que, usando elasticidade de processadores, um comando escrito utilizando a linguagem "Structured Query Language" (SQL) pode ser distribuído para execução entre diversos processadores concorrentemente. Caso contrário, um incremento de CPU pode não refletir em ganho de tempo. Além disso, em caso de falha, a maioria dos Sistemas Gerenciadores de Banco de Dados (SGBD) reiniciam o comando SQL, já que em ambientes locais esse evento é raro. Já na nuvem, os equipamentos costumam ser mais baratos, menos confiáveis, menos potentes, mais numerosos e falhas mais comuns (ABADI, 2009).

O armazenamento de dados pode ficar em servidores não confiáveis, podendo violar as normas de privacidade de uma empresa. Além disso, os dados podem estar fisicamente alocados em diversos países, estando sujeitos a regras e regulamentações locais de cada país. Por exemplo, nos EUA, o *US Patriot Act* permite acesso do governo a dados de qualquer computador (ABADI, 2009).

Outra característica que deve ser ressaltada é a replicação de dados para garantir disponibilidade e durabilidade (WIESMANN et al., 2000). Devido a isso e ao teorema de CDP, a consistência do banco sendo garantida em cada instante torna-se mais difícil.

2.3.1.4 Gerenciamento de dados transacionais

Para limitar o escopo de estudo de SGBD, alguns tipos de bancos de dados podem ser avaliados com enfoque diferenciado. Assim, (ABADI, 2009) propôs uma separação entre bancos transacionais e analíticos. Para bases de processamento transacional, ressaltaram-se os seguintes desafios:

- Compartilhamento de arquitetura: dados transacionais podem ser compartilhados inclusive entre *storages* diferentes em localidades diferentes. Para manutenção da consistência e disponibilidade desses dados através da rede, é necessária a implementação de protocolos avançados para bloqueio de transações que pretendem alterar dados ao mesmo tempo e protocolos que permitam gravar as alterações com sucesso;

- Manutenção de ACID torna-se difícil quando exige-se a replicação de dados entre localidades distantes. O teorema CDP mostra que sistemas que compartilham dados precisam escolher até duas das propriedades de consistência, disponibilidade ou tolerância a particionamentos de rede. Geralmente, a consistência é comprometida para garantir razoável disponibilidade;

- Riscos em armazenamento de dados: bases transacionais armazenam tipicamente dados relativos à missão crítica de uma empresa, podendo conter informação sigilosa ou restrita. Possíveis descobertas ou vazamento dessas informações não são aceitáveis.

Por fim, (ABADI, 2009) conclui que o gerenciamento de bases transacionais não está suficiente desenvolvido para a nuvem.

2.3.1.5 Gerenciamento de dados para análise

Entende-se como bases de dados de processamento analítico aquelas que são usadas para inteligência de negócio, solução de problemas ou suporte a decisões, usadas mais frequentemente para consultas. Consequentemente, o aumento do número de nós de *clusters* de banco de dados em nuvem não oferece tantos desafios quanto em bases transacionais. Isso se deve pelo fato de alterações ao banco serem menos frequentes, logo garantias de consistência são mais fáceis de serem obtidas.

- Compartilhamento de arquitetura: com aumento da quantidade de dispositivos associados a *clusters* de bancos de dados, o paralelismo e a concorrência podem ser utilizados para entregar respostas mais rápidas às análises sendo executadas. Assim, o compartilhamento de dados em localidades diferentes é vantajoso. Como a alteração de dados não é frequente, manter a consistência e a disponibilidade entre as partições da rede torna-se mais fácil;

- Manutenção de ACID: além de haver pouca alteração de dados, as consultas nem sempre precisam das informações mais atualizados para fazer a análise necessária. Assim, atomicidade, consistência e isolamento tornam-se mais fáceis de serem obtidos;

- Riscos em armazenamento de dados: Dados sensíveis à missão da empresa podem ser retirados da análise, tornando assim mais seguro o transporte deles pela nuvem.

Por fim, (ABADI, 2009) conclui que o gerenciamento de bases para análise pode ser executado mais facilmente e com menos desafios na nuvem.

Em outras palavras, (CURINO et al., 2011) citam os desafios para bases de dados relacionais na nuvem. O primeiro é *multi-tenancy* eficiente, em que mais bases de dados podem usar um número menor de servidores. Uma proposta para garantir uso individual de recursos seria o uso de máquinas virtuais. O segundo é escalabilidade com elasticidade em que o processamento poderia ser particionado em mais de um nó. Esse particionamento traz além da vantagem de processamento distribuído, balanceamento de carga e alta disponibilidade. O último desafio é a privacidade de dados e uma das propostas é o uso de criptografia.

2.3.2 Armazenamento de Dados em Nuvem

2.3.2.1 Serviços de Armazenamento

Há uma variedade substancial de serviços, técnicas e produtos para o fornecimento de armazenamento de dados na nuvem, dos quais podem-se ressaltar os seguintes:

- Serviços de Armazenamento da Amazon: Amazon Simple Storage Service (Amazon S3) fornece armazenamento através de interface web (AMAZON, 2012d). Os dispositivos de segurança oferecidos são políticas de gerenciamento de identidade e acesso, listas de acesso, outras políticas de segurança e autenticação. Os dados podem ser trafegados através de canais usando *Secure Socket Layer* (SSL) . Além disso, o cliente pode gerenciar suas próprias chaves de criptografia antes de enviar os dados para o servidor ou passar o gerenciamento das chaves para a Amazon. A replicação de dados pode ser feita entre múltiplos dispositivos, mas numa mesma região geográfica.

  Amazon Elastic Compute Cloud (Amazon EC2) é um serviço para prover capacidade computacional na nuvem com elasticidade (AMAZON, 2012b). Para aumentar os níveis de segurança são oferecidos ferramentas para configuração de firewall, possibilidade de uso de número dedicado de IPs e máquinas virtuais dedicadas. Existe uma variedade grande de sistemas operacionais, SGBDs e aplicações oferecidos. Amazon Elastic Block Store (EBS) (AMAZON, 2012a) permite a criação de volumes de armazenamento em níveis de bloco para serem montados como dispositivos de instâncias de EC2. Os volumes podem ter de 1 GB a 1 TB e a cobrança é feita pelo espaço de armazenamento e pela quantidade de I/O utilizada.

  O serviço de banco de dados relacional é fornecido pelo Amazon Relational Database Service (Amazon RDS) (AMAZON, 2012c). É um serviço web para criar, operar e configurar a escalabilidade de bancos de dados relacionais na nuvem. Os produtos disponíveis são MySQL, Oracle e Microsoft SQL Server. O serviço ainda atualiza automaticamente o software e faz backup com retenção definida pelo usuário. Para entregar mais performance de I/O, uma opção de armazenamento com maior *Input/Output Operations Per Second* (IOPS) é oferecida. Além do RDS, ainda existe o Amazon DynamoDB (AMAZON, 2013a) que é um serviço de base de dados NoSQL que automaticamente separa os dados e tráfego das tabelas para um número suficiente de servido-

res para tratar a capacidade de armazenamento requisitada pelo cliente mantendo consistência eventual e alta performance. Todos os dados são armazenados em discos de estado sólido e automaticamente replicados entre três zonas em uma mesma região.

Internamente, a Amazon utiliza a arquitetura do Dynamo delegando à aplicação do cliente a escolha entre consistência, durabilidade, disponibilidade e performance. A garantia de consistência é eventual, ou seja, consistência causal, consistência ao ler suas próprias escritas, consistência de sessão, consistência de leituras serialmente ou escritas serialmente (VOGELS, 2009);

- Serviços de Armazenamento do Google: Dentre os serviços destacam-se Cloud Storage, BigQuery e Cloud SQL. Google Cloud Storage permite o armazenamento e gerenciamento de qualquer quantidade de dados com escalabilidade quase ilimitada. Inclui ferramentas para análise de dados como o Google Prediction API e BigQuery. A replicação de dados é feita em múltiplos *data centers* nas regiões dos EUA ou Europa. Google BigQuery é a implementação de uma tecnologia do Google chamada Dremel e com ela é possível fazer uma varredura em bilhões de linhas em dezenas de segundo (GOOGLE, 2013). Banco de dados orientado a colunas e arquitetura em árvore possibilita a utilização de paralelismo em dezenas de milhares de servidores para a execução de consultas SQL. Google Cloud SQL é uma base de dados MySQL alocada na infraestrutura de nuvem do Google dos EUA ou da Europa;

- Serviços de Armazenamento do Yahoo: PNUTS (Platform for Nimble Universal Table Storage) é uma plataforma de serviço de dados descrita primeiramente em 2008. Deve ser ressaltado neste tópico, como os dados são armazenados: utilizando tabelas ordenadas ou tabelas hash. Assim, além de ser usado como armazenamento de tabelas com chave e valor, também habilita algumas funcionalidades com tabelas ordenadas. Isso possibilita organizar fisicamente registros pela chave e fazer varreduras por subconjuntos de dados ou utilização de índices secundários. Tabelas hash permitem propriedades de balanceamento de carga e escalabilidade. As tabelas ordenadas ou hash são particionadas horizontalmente. O que difere uma tabela hash de uma ordenada é como os registros de chaves são armazenados. Uma tabela ordenada é particionada pela chave e uma hash é particionada pelo valor do hash. Para prover consistência mais forte entre as partições de rede, degradando a disponibilidade, PNUTS se baseia numa linha de tempo de consistência por tupla. Cada tupla deve ter a mesma sequência de transformações

para réplica particionada (SILBERSTEIN et al., 2012; SHIM, 2012; COOPER et al., 2008; YAHOO!, 2013);

- Serviços de Armazenamento da Microsoft: Windows Azure Storage (WAS) é um sistema de armazenamento escalável nas formas de arquivos, tabelas estruturadas e filas (entrega de mensagens). Provê a combinação de alta disponibilidade com garantias de consistência forte o que violaria o Teorema CDP, descrito na subseção 2.3.1.2. Ressalta-se o método adotado para garantir a consistência. São criadas camadas de particionamento de rede separando alterações de dados síncronas e assíncronas. Para simplificar, nesse sistema, as alterações síncronas são feitas no mesmo *rack* onde estão os nós de armazenamento. Já as assíncronas são feitas entre *racks* diferentes, possivelmente em localidades diferentes (CALDER et al., 2011). Observa-se que, com alterações assíncronas, a consistência não é forte, sendo garantida somente após a sincronização das áreas de armazenamento. Outro serviço da Microsoft é o SQL Azure para base de dados relacional. Ele suporta transações com propriedades ACID, confira 2.3.1.1, em escala controlada ou consistência mais relaxada para escalas maiores (CAMPBELL; KAKIVAYA; ELLIS, 2010).

Apesar de todos os recursos e benefícios, o controle sobre os dados não fica sob responsabilidade do cliente, sendo proposto auditoria e verificação dos dados na nuvem. Isso é desejado para evitar problemas de indisponibilidade e segurança tais como os observados no caso da Amazon S3 e da deleção de e-mails do GMail (WANG et al., 2010).

São muitos os sistemas de armazenamento de código aberto, no entanto, nem todos estão estáveis ou não possuem um leque abrangente de funcionalidades. Podem ser ressaltados os seguintes: Cassandra, CouchDB, HBase, Redis, Scalaris, Project-Voldemort (KRASKA, 2010).

2.3.2.2 Fatores Relevantes

Deve ser ressaltada a segurança existente em servidores de armazenamento, pois, no modelo de DBaaS, ele deverá ficar completamente transparente ao cliente. Certamente, os riscos de segurança aumentam e igualmente deveria ser a preocupação dos clientes, pois dependem desse armazenamento. Assim, as garantias de completude –em que dados não são omitidos em um resultado– devem ser especificadas e avaliadas nos contratos e acordos de serviços. A completude está relacionada com a autenticidade em que se tem garantias de que os dados não foram alterados inadvertidamente (WEIS;

ALVES-FOSS, 2011). Alguns estudos propõem auditoria em servidores de armazenamento para garantir a integridade e a completude (WANG et al., 2012, 2011).

Outro fator relevante é a continuidade do negócio e a proposta de (ARMBRUST et al., 2010) é usar fornecedores múltiplos. No entanto, essa solução não é viável para nuvem pública para DBaaS, pois não existe uma ligação direta entre os provedores. Caso fosse feita, seriam ainda maiores os desafios para a segurança.

3 UM FRAMEWORK PARA AVALIAR CONTROLES INTERNOS

Dar segurança aos ativos de software e hardware e da própria informação trafegada na nuvem torna-se um grande desafio, especialmente, em ambientes públicos em que os dados não são controlados por seus detentores. Em nuvens privadas ou comunitárias existe a possibilidade de controle maior sobre ativos e informações, no entanto, deve-se lembrar que dados críticos ou sensíveis devem estar restritos, conforme políticas ou normas, entre departamentos ou organizações.

Para obter mais confiança e consequente sucesso nos processos de implementação de banco de dados em nuvem, a partir de requisitos de negócio e segurança da informação, este trabalho apresenta a criação de um modelo de dados, um *framework* de processos, o qual descreve um conjunto de controles internos (termo utilizado pelo COBIT, ver seção 3.2.1) e práticas para auxiliar usuários finais a:

- Definir objetivos de controles internos;
- Integrar e analisar *Service Level Agreement* (SLA) e
- Estabelecer períodos para verificação desses controles internos.

Este trabalho pode ser executado em conjunto com aplicações que verifiquem a performance e a disponibilidade de serviços na nuvem, monitorando (LEITNER et al., 2010) e controlando a elasticidade e proporcionando a economia de recursos (ZHAO; SAKR; LIU, 2013; SOUSA; MACHADO, 2012; ZHAO; SAKR; LIU, 2012). Neste trabalho, será usada a ferramenta PCMONS (*Private Cloud MONitoring Systems*) (CHAVES, 2010).

Um SLA é parte de um contrato de serviço onde um serviço é formalmente definido e é um documento legal entre o provedor e o cliente, é utilizado aqui como fonte para definição de controles com o objetivo de mitigar e gerenciar riscos, no que tange a segurança do serviço de banco de dados em nuvem. SLA é frequentemente referenciado como tempo de disponibilidade de um serviço e, dessa maneira, poderá ser medido através de métricas do PCMONS.

3.1 PRÁTICAS DE SEGURANÇA

3.1.1 Princípio do Menor Privilégio

As bases de dados empresariais poderão estar sujeitas a acessos de diversas aplicações ou módulos dessas. Uma boa prática de segurança é limitar o acesso dessas aplicações ao menor nível possível, garantindo assim que dados fiquem disponíveis àqueles de direito, evitando que permissões desnecessárias sejam delegadas. No entanto, na prática, a implementação baseada em menor privilégio é trabalhosa, pois inclui a classificação de dados, conhecimento de dados sensíveis, gerenciamento de acesso e manutenção periódica. Usuários e aplicações teriam acesso a dados somente para desempenho de suas funções. Além disso, o controle de acesso deve ser acompanhado com auditoria periódica nos sistemas (SANDHU; SAMARATI, 1994).

3.1.2 Ataques e Camadas de Proteção na Nuvem

A rapidez em que as mudanças ocorrem em ambientes de nuvem é proporcional à medida que ataques aparecem (VENGURLEKAR, 2012). Essas mudanças e alterações nos modos de operação devem ser tratados nos processos e controles internos de uma organização.

Outras ameaças, surgem quando múltiplos clientes alocam um mesmo espaço (memória, unidade de processamento ou armazenamento) ou estarem próximos (compartilhando conexões de rede), fazendo com que riscos para os dados e sistemas aumentem. Além disso, ameaças podem afetar muitos clientes ao mesmo tempo. Um exemplo é o ataque distribuído por negação de serviço – da sigla, em Inglês, DDoS (*Distributed Denial of Service*) –ou um DoS (*Denial of Service*). Desta forma, políticas de segurança e controles internos mais robustos devem ser analisados e implementados para remediar ou eliminar esses riscos.

Idealmente, todas as camadas que comporiam a estrutura da nuvem precisariam de controles, desde o acesso físico, sistemas operacionais, o ambiente de virtualização, armazenamento, bases de dados, servidores de aplicação, redes, interfaces de gerenciamento e automação da nuvem.

3.2 METODOLOGIA

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 mitigar os possíveis riscos associados ao ambiente de banco de dados. Para dar suporte ao método de construção do *framework*, serão utilizadas como referência algumas padronizações. 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), criado pelo *IT Governance Institute* (ITGI) e *Information Systems Audit and Control Association* (ISACA) nos anos 90 (RIDLEY; YOUNG; CARROLL, 2004; NWAFOR et al., 2012).

Uma segunda padronização utilizada neste trabalho é a do NIST (*National Institute of Standards and Technology*), em *Special Publication* 800-53 (NIST, 2009), que tem o propósito de prover meios para selecionar e especificar controles para sistemas de informação.

3.2.1 Modelo Genérico de Processos

Para definir em qual fase de maturação de um processo interno, é utilizado o COBIT (ITGI, 2007), que define atividades em um modelo de processos genérico em quatro domínios. São eles:

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.

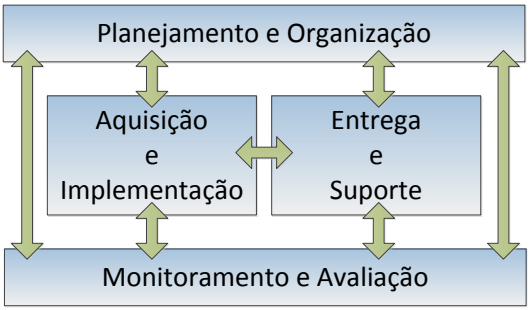


Figura 3 – Inter-relacionamento entre os domínios do COBIT

A figura 3 mostra o inter-relaciomento entre os quatro domínios do COBIT. Por exemplo, Planejamento e Organização direciona entrega de soluções (Aquisição e Implementação) e serviços (Entrega e Suporte).

A partir deste ponto, foram depurados controles e fases para melhor identificar em que momento e maturação do processo, os controles selecionados devem ser avaliados. Assim, onde o controle indicar a fase, deve-se entender que ele se refere a esses domínios. Alguns controles deverão ser avaliados durante todo o ciclo de vida de um projeto de DBaaS.

3.2.2 Prioridades e Melhorias

Uma ordem em que os controles devem ser avaliados deve ser seguida, pois implica em tomada de decisões diferentes e variedade de maneiras de implementação. Assim, baseando na padronização NIST 800-53, criaram-se as seguintes prioridades para os controles:

Alta Os controles com prioridade Alta devem ser avaliados ou implementados primeiramente dentro de cada família de controles comuns;

Média Os controles devem ser avaliados ou implementados depois dos de prioridade Alta e antes dos de prioridade Baixa;

Baixa Devem ser avaliados ou implementados após os controles de prioridades Alta e Baixa e

Documentação Devem ser utilizados apenas para gerar documentação para futuras consultas ou análises.

Diferentemente da especificação 800-53, preferiu-se gerar uma documentação onde os controles não possuíam prioridade definida.

Entretanto, após selecionados os controles, tais prioridades foram atribuídas empiricamente, com base em experiência de trabalho profissional no CIASC (Centro de Informática e Automação do Estado de Santa Catarina).

Já as melhorias que podem ser aplicadas ao controle são especificadas em um campo de cada controle. Entre elas podem ser a automatização de processos, desmembramento em diversas etapas ou até uma ampliação para dar suporte a outras necessidades.

3.3 MÉTODO

Problemas de segurança são, num nível mais alto de visualização, semelhantes entre os diversos SGBDs. Assim, alguns controles foram obtidos de (FINNIGAN, 2004; ORACLE, 2008; NATAN, 2005). Nesses trabalhos é possível observar o que se deve aplicar à bases de dados, de uma forma geral. Para o tratamento específico de SGBD numa nuvem, foi usado como referência (VENGURLEKAR, 2012). Com base nestes trabalhos foi possível organizar um subconjunto de controles relevantes aos ambientes de bases de dados em nuvem. Diversos outros controles que são usados normalmente para gerar processos internos para serviços locais podem ser adaptados para a nuvem.

Para exemplificar, os controles de sistema operacional e do ambiente de virtualização não são possíveis de verificação em um DBaaS, mas podem ser utilizados com objetivo de documentação. Além disso, devido à essa restrição, se existirem atributos do SGBD que só poderiam ser alterados utilizando o sistema operacional, o provedor de DBaaS deveria fornecer meios para que os clientes possam fazer essas alterações através de outras interfaces.

Abaixo, estão apresentados um subconjunto relevante de controles para criação de um framework. Eles estão subdivididos em famílias ou domínios de controles comuns.

(A) Planejamento e Avaliação de Risco

(1) Identificar e aplicar correções conhecidas e reportadas para vulnerabilidades

Descrição: Para o SGBD, verificar se:

(a) As versões de programas e componentes de programas são as mais recentes;

(b) Está aplicado o último pacote de atualizações;

(c) Estão aplicadas atualizações de segurança;

(d) São homologadas e suportadas versões mais antigas, caso necessário por questões de compatibilidade de aplicativos.

Melhorias ao controle: Criar um procedimento automatizado para verificação do controle.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Alta.

(2) Identificar e gravar versões de software (banco de dados e aplicações) e de pacotes de correções no sistema

Descrição: Armazenar informações de versões de software para documentação.

Fase: Aquisição e Implementação.

Prioridade: Documentação.

(3) Utilizar somente as funcionalidades necessárias

Descrição: Verificar a possibilidade de instalação e exclusão de funcionalidades tais como pacotes de aplicativos, bibliotecas auxiliares e ferramentas para execução de tarefas específicas.

Melhorias ao controle: Criar processo para analisar periodicamente se as funcionalidades instaladas estão sendo usadas regularmente.

Fase: Aquisição e Implementação, Monitoramento e Avaliação.

Prioridade: Baixa

(4) Rever procedimentos e políticas de segurança

Descrição: Revisar as políticas de segurança utilizadas pelo DBaaS e implementar procedimentos para focar o princípio do menor privilégio.

Fase: Planejamento e Organização, Aquisição e Implementação, Monitoramento e Avaliação.

Prioridade: Média.

(5) Verificar localização física dos servidores e conformidade com o Teorema CDP

Descrição: Os provedores de serviços geralmente oferecem como opção a escolha da região onde os recursos de DBaaS estarão disponíveis. O Teorema CDP, conforme subseção 2.3.1.2, detalha a impossibilidade de se obter consistência e disponibilidade em ambientes particionados. Assim, para evitar que sincronizações entre partições depreendam considerável tempo, aconselha-se o uso de um mesmo segmento de rede. Verificar a necessidade de os ambientes

de uma mesma região geográfica suportarem transações ACID (ver subseção 2.3.1.1), conforme estabelecido pela regra de negócio do cliente. Além disso, devido problemas relativos à localização como legislações e adversidades climáticas devem ser considerados.

Melhorias ao controle: Verificar a possibilidade de criação de serviços espelhados em, pelo menos uma, região geográfica distinta.

Fase: Planejamento e Organização, Aquisição e Implementação.

Prioridade: Alta para SGBD com suporte a transações ACID e média para outros.

(6) Definir arquitetura de acesso da aplicação

Descrição: Mapear o acesso das aplicações ao SGBD.

Melhorias ao controle: Mapear o acesso de aplicações em desenvolvimento e mapear o acesso direto à base para administração e desenvolvimento.

Fase: Planejamento e Organização.

Prioridade: Baixa.

(7) Infraestrutura de Chave Pública (ICP)

Descrição: Verificar a possibilidade de uso de uma infraestrutura de chaves públicas para que a criptografia de dados seja feita com chaves gerenciadas e administradas pelo cliente.

Melhorias ao controle: Criar procedimentos para armazenamento e cópia de segurança para uma ICP.

Fase: Planejamento e Organização.

Prioridade: Alta.

(8) Gerenciamento de Incidentes

Descrição: Gerenciamento de incidentes permite ao cliente monitorar e resolver problemas relativos ao banco de dados de maneira rápida e eficiente. Os problemas podem ser origem externa como ataques ou exploração de vulnerabilidades. Ainda, de origem interna como sobrecarga, estouro de áreas de armazenamento e até problemas de configuração.

Melhorias ao controle: Configuração de alertas que podem ser enviados através de eventos, conforme a criticidade.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Média.

(B) Segurança de Sistema Operacional e Ambiente de Virtualização

(1) Segurança e criptografia nas conexões de rede
Descrição: Numa estrutura de DBaaS, controles relativos ao sistema operacional ou ao ambiente de virtualização não são administrados pelo cliente. No entanto, no que for possível a verificação desta Segurança, ela deve ser feita. A garantia de segurança não deve se limitar ao DBaaS, pois falhas em níveis mais baixos podem ocasionar quebra de contrato.
Fase: Planejamento e Organização.
Prioridade: Documentação.

(2) Troca segura de senhas entre servidores e clientes
Descrição: Verificar se as senhas trocadas entre servidores e clientes alocados total ou parcialmente no ambiente de nuvem estão sendo feitas de maneira segura.
Melhorias ao controle: Impedir conexões com troca de senhas inseguras.
Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.
Prioridade: Baixa.

(3) Auditoria nas máquinas clientes para evitar arquivos de configuração com usuários e senhas
Descrição: Verificar se não existem senhas armazenadas de maneira insegura nas máquinas de usuários, operadores, desenvolvedores e administradores.
Fase: Aquisição e Implementação, Monitoramento e Avaliação.
Prioridade: Baixa.

(4) Detecção e prevenção de intrusos
Descrição: Ferramentas de detecção e prevenção de intrusos devem ser utilizadas pelos provedores de serviços na nuvem criando mais camadas para proteção de dados.
Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.
Prioridade: Baixa.

(5) Assegurar privilégios mínimos de conexão
Descrição: Verificar se, ao conectar no banco, o usuário possui privilégios para modificar parâmetros de sessões ou configurações do sistema.
Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.
Prioridade: Baixa.

(6) Auditoria sobre arquivos de exportação e de registros de alteração da base

Descrição: Os arquivos de exportação da base podem ser usados com forma alternativa de backup. Eles podem conter toda a base de modo não criptografado ou protegido. Os arquivos de registro podem conter, além das instruções para recuperação da base, códigos utilizados para alterar dados.

Fase: Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Baixa.

(7) Troca de senhas após importação de dados

Descrição: A criação de usuários e importação de dados podem ser feitas por equipes diversas, sendo necessário reconfigurar novas senhas para uso exclusivo a quem se destina.

Fase: Planejamento e Organização, Aquisição e Implementação.

Prioridade: Baixa.

(8) Auditoria sobre tabelas externas

Descrição: Tabelas externas podem ser usadas como fontes de dados. No entanto, não seguem os padrões, parâmetros e políticas implementadas no banco.

Fase: Monitoramento e Avaliação.

Prioridade: Baixa.

(9) Restringir acesso para compilação de código no banco

Descrição: Para dar mais performance, a inteligência de uma aplicação pode ser desenvolvida diretamente no banco de dados. Usuários com a permissão de compilação e execução devem ser bem mapeados.

Melhorias ao controle: Inclusão de fluxo para publicação de código em ambientes de produção.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Baixa.

(10) Firewall e antivírus

Descrição: Assim como detecção e prevenção de intrusos, firewall e antívirus pode ser desejável no tráfego de dados que ocorre entre servidores e clientes.

Melhorias ao controle:

Fase: Planejamento e Organização, Aquisição e Implementação.

Prioridade: Documentação.

(11) Virtual Private Network (VPN)

Descrição: Conexões privadas são necessárias para garantir acesso exclusivo ou limitado aos dados.

Melhorias ao controle: Garantir acesso somente através de redes virtuais privadas.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Documentação.

(C) Autenticação e Autorização

(1) Auditoria de usuários ativos da base e de usuários de aplicação

Descrição: Auditar usuários da base e usuários da aplicação conforme sensibilidade e classificação da informação.

Fase: Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Baixa.

(2) Auditoria de senhas da base

Descrição: Verificar se a segurança das senhas está compatível com a sensibilidade do dados armazenado.

Melhorias ao controle: Criar políticas restritivas como tamanho, complexidade, tempo para troca e histórico de senhas.

Fase: Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Baixa.

(3) Auditoria de contas padrão

Descrição: As contas padrão de um SGBD são as prováveis contas a serem exploradas no caso de tentativa de acesso a um sistema.

Melhorias ao controle: Bloqueio de senhas conforme o número de tentativas de acesso subsequente sem sucesso. Se possível, eliminar contas padrão ou renomear.

Fase: Monitoramento e Avaliação.

Prioridade: Baixa.

(4) Incluir gerenciamento de senhas para contas por padrão

Descrição: O gerenciamento de senhas deve dar suporte a complexidade, histórico, tamanho, idade e forma de armazenamento de senhas.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Alta.

(5) Alterar senhas de usuários privilegiados de sistema

Descrição: Usuários privilegiados do sistema devem ser restritos.

Fase: Planejamento e Organização, Aquisição e Implementação.

Prioridade: Alta.

(6) Inclusão de senhas para todos os componentes da base

Descrição: Proteção de pontos como ligações entre bancos, gerenciador de conexão, servidor de páginas ou serviços.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte.

Prioridade: Baixa.

(D) Controle de Acessos

(1) Segurança granular: controle de acessos a partes de tabelas, visões, parte de procedimentos e funções

Descrição: O desenho de uma base de dados pode ser amplo e complexo. Por exemplo, uma tabela com dados de Gestão de Pessoas pode ser composta por diversas informações como nome, sobrenome, endereço, telefone, salário etc. Aplicações e usuários com perfis e papéis diferentes podem ter acesso a somente um subconjunto de dados garantindo o menor privilégio para o desempenho de suas funções, evitando a descoberta de informações privilegiadas mesmo àqueles com grande conhecimento do desenho da base.

Melhorias ao controle: Aquisição de ferramentas específicas para auxiliar na configuração de segurança granular.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Média.

(2) Checar usuários com permissão de operação e administração da base

Descrição: Usuários com permissão para operação e administração de um banco deve ser utilizados somente para essas finalidades. Por conveniência ou facilidade, é comum utilizar essas permissões para usuários de desenvolvimento ou aplicação. Isso deve ser evitado.

Fase: Aquisição e Implementação, Monitoramento e Avaliação.

Prioridade: Alta.

(3) Revisar permissões de sistema garantida a usuários

Descrição: Durante as diversas fases de um projeto pode-se requerer diferentes permissões para usuários de desenvolvimento ou de aplicação. Eles devem ser avaliados para utilizar os menores privilégios.

Melhorias ao controle: Utilizar auditoria desses usuários.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Média.

(4) Verificar acessos através de ligações permitidas entre bases

Descrição: Obter dados de diversas bases para compor um resultado faz com que sejam feitas ligações entre elas. O acesso pode ser feito com usuários específicos para isso.

Melhorias ao controle: Inserir ferramentas de firewall para controlar conexões.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Média.

(5) Controle de usuários, papéis e gerenciamento de identidade

Descrição: O rotacionamento de funções, contratações e desligamentos são rotinas de uma empresa. Assim, os controle de acessos de usuários deve ser revisto periodicamente. Esse controle também tem o objetivo de identificar os usuários relativos a contas de sistema.

Melhorias ao controle: Criar procedimento ou ferramenta para controle de usuários nos casos de alteração de seus estados juntamente à Gestão de Pessoas da corporação do cliente.

Fase: Monitoramento e Avaliação.

Prioridade: Baixa.

(6) Classificação de dados

Descrição: A classificação de dados é uma das atividades mais importantes para Segurança da Informação. No entanto, a execução desse controle envolve custos e tempo que devem ser emparelhados com o negócio da corporação do cliente.

Melhorias ao controle: Aquisição de ferramentas e contratação de consultoria para realização desta atividade e verificações periódicas.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Variável conforme o negócio do cliente.

(E) Auditoria

(1) Configurar auditoria

Descrição: A auditoria em banco de dados deve ser estudada a fundo, pois implica em perda de performance e uso de recursos de

armazenamento. Assim, deve ser bem meticulosa e suficiente, auditando somente o necessário. Auditoria deve ser acompanhada ao processo de classificação de dados.

Melhorias ao controle: Criação de procedimentos para auxiliar na escolha de métodos e processos de auditoria.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Variável conforme a sensibilidade dos dados.

(2) Auditoria em falhas de inserção em objetos

Descrição: Esta especificação de auditoria permitirá obter mais rapidamente informações sobre eventuais falhas no desenho de código ou tipificação de dados. Pode auxiliar na prevenção de inserção maliciosa ou inadvertida de dados. Esta auditoria também está acompanhada com a classificação de dados, no entanto, restrita a inserções.

Melhorias ao controle: Criação de processo para validação e auditoria em tempo de desenvolvimento de código.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Baixa.

(3) Auditoria de acesso à base

Descrição: Esta especificação de auditoria deve reforçar o controle de acessos, refinando seu ajuste.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Baixa.

(F) Camada de Rede

(1) Não utilizar portas padrão para conexão

Descrição: Evitar o uso de portas padrão incrementa a segurança do sistema. Para um ambiente de nuvem, esse dado pode não ser verificável, pois está implementado no *core* do sistema.

Fase: Planejamento e Organização.

Prioridade: Documentação.

(2) Segurança do servidor de conexão e ligações entre bases

Descrição: Um sistema pode utilizar diversas bases de dados e estas podem se comunicar entre si ou ainda diversos sistemas podem usar uma única base. O servidor que permite a conexão à base deve ser analisado para verificar se não há problemas de configuração ou

suscetibilidade a ataques. As ligações entre bancos de dados devem ser evitadas.

Fase: Planejamento e Organização, Monitoramento e Avaliação.

Prioridade: Baixa.

(3) Auditoria e criação de políticas para definir ligações entre bases

Descrição: As conexões ao banco devem ser auditadas para observação de anomalias e futuras consultas. Políticas devem ser geradas para estabelecer regras e níveis de acessos para ligações entre bases.

Fase: Planejamento e Organização, Monitoramento e Avaliação.

Prioridade: Baixa.

(4) Usuários de conexões entre bases não pode ser usuário privilegiado

Descrição: Durante o estabelecimento de conexões entre bases de dados deve-se usar o princípio do menor privilégio.

Fase: Planejamento e Organização, Monitoramento e Avaliação.

Prioridade: Baixa.

(5) Transferência de dados com criptografia entre servidores e clientes

Descrição: Possivelmente existam clientes ou servidores locais fazendo conexão com as bases. Como o ambiente da nuvem é compartilhado e haja tráfego entre servidores inclusive pela Internet, requer-se que essas conexões sejam criptografadas.

Melhorias ao controle: Configurar sistema para recusar conexões que não sejam criptografadas.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Variável conforme sensibilidade da informação.

(G) Disponibilidade, Cópia de Segurança e Recuperação

(1) Revisar e documentar procedimentos de backup e recuperação

Descrição: Os procedimentos de backup e recuperação são de vital importância durante o ciclo de vida de um projeto. Assim, eles devem ser documentados e revistos com frequência. Com a execução periódica, podem-se extrair métricas de tempo, corrigir eventuais problemas e aplicar melhorias.

Melhorias ao controle: Criar procedimentos automáticos para efetuar periodicamente backup e recuperação.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Alta.

(2) Armazenamento de mídias em localização distinta

Descrição: Armazenar mídias de backup em localização distinta faz com que a probabilidade de perda em caso de desastre seja diminuída. Para o caso em que o fornecedor não entregue a informação de mídias para o seu cliente, uma adaptação pode ser feita: exportar os dados da nuvem e armazenar no local do cliente dando garantias da posse do dado.

Melhorias ao controle: Criar procedimento automatizado para a exportação de dados para o local do cliente.

Fase: Monitoramento e Avaliação.

Prioridade: Baixa.

(3) Validar mídias de backup regularmente

Descrição: Tão considerável quanto trazer os dados é a validação deles. Ademais, esse procedimento ainda pode ser incluído como uma das opções para a continuidade do negócio em caso de ruptura.

Melhorias ao controle: Criar procedimento automatizado para a importação de dados para o local do cliente.

Fase: Monitoramento e Avaliação.

Prioridade: Baixa.

(4) Validar procedimentos de recuperação regularmente

Descrição: Validar se o procedimento de backup com ferramentas da nuvem está válido. Talvez essa atividade inclua custos adicionais para o cliente, pois requer a criação de um ambiente espelhado.

Melhorias ao controle: Criar procedimento automatizado para provisionar recursos, efetuar a recuperação e liberar os recursos alocados.

Fase: Monitoramento e Avaliação.

Prioridade: Baixa.

(5) Documentar e rever procedimentos de recuperação de desastre

Descrição: Recuperação de desastre inclui custo por vezes enormes. Desse modo, nem todos os clientes prescindem de retorno das atividades em curto tempo. No entanto, a realização dos outros controles desta família, colabora com a realização deste.

Fase: Monitoramento e Avaliação.

Prioridade: Documentação

(H) Desenvolvimento e Servidores de Aplicações

(1) Ambiente de produção isolado e sem acesso para desenvolvedores

Descrição: Boas práticas de desenvolvimento consideram relevante a separação dos ambientes de produção entre outros. Assim, tem-se um sistema estável rodando em produção e outros onde podem ser feitas alterações frequentes para serem testadas e homologadas.

Melhorias ao controle: Criação de ambientes isolados para produção, desenvolvimento, teste e homologação.

Fase: Planejamento e Organização, Entrega e Suporte.

Prioridade: Baixa.

(2) Procedimentos de replicação de ambientes

Descrição: Alguns requisitos podem exigir a replicação de ambientes, dentre eles ressaltam-se alta-disponibilidade, recuperação em caso de falha, isolamento de ambientes para outros fins como desenvolvimento, teste, homologação e extração de relatórios.

Melhorias ao controle: Automatização do procedimento.

Fase: Planejamento e Organização, Entrega e Suporte.

Prioridade: Baixa.

(3) Segurança de usuários de portal na base

Descrição: Usuários da aplicação precisam conectar à base para desempenho de atividades e deve-se aplicar, na medida do possível, o princípio do menor privilégio.

Fase: Planejamento e Organização, Entrega e Suporte.

Prioridade: Média.

(4) Remover programas e dados de exemplo de portal e base

Descrição: Com o objetivo de criar mais conhecimento para o produto adquirido, os fornecedores costumam adicionar opcionais em aplicações e bases de dados. No entanto, isso insere mais variáveis ao ambiente, podendo os opcionais estarem suscetíveis a vulnerabilidades.

Fase: Planejamento e Organização

Prioridade: Baixa.

(5) Controle de vulnerabilidades: injeção de código e SQL, DoS e DDoS, cross-site script

Descrição: As aplicações e bancos de dados estão suscetíveis a diversos ataques com o objetivo de obter acesso aos dados e descobrir informações privilegiadas, sensíveis ou secretas. Assim, deve-se verificar se existem barreiras de proteção e se o código é robusto e criada com boas práticas de segurança.

Melhorias ao controle: Fazer testes periódicos de intrusão para observar o nível de proteção e se é eficaz.

Fase: Planejamento e Organização, Entrega e Suporte.

Prioridade: Alta.

(I) Contratos e Comprometimento

(1) Documentar, verificar e fiscalizar periodicamente os níveis de serviço contratados

Descrição: Contratos podem ser extensos e prolixos, assim, deve-se:

(a) Focar nas regras de negócio como requisitos para o contrato;
(b) Analisar e fiscalizar como é feito o compartilhamento entre os outros hóspedes ou inquilinos, veja subseção 2.2.4;
(c) Verificar gerenciamento de recursos, isolamento e qualidade de serviço;
(d) Verificar planos para recuperação de desastres e retenção de dados;
(e) Observar e documentar latência entre conexões;
(f) Tempo de indisponibilidade: por exemplo, contratos com 90% (um nove) de disponibilidade, permitem indisponibilidade mensal de 72h e, com 99,99% (quatro noves), permitem 52min34s por ano;
(g) Tempo de resposta para solicitações ao suporte;
(h) Verificar se a nuvem é privada, híbrida, pública ou comunitária e se subcontrata fornecedores terceiros;
(i) Observar custos e taxas excepcionais ou adicionais;
(j) Estornos por quebra contratual e
(k) Ruptura e cancelamento contratual.

Melhorias ao controle: Procedimentos para testar periodicamente recuperação de desastre, criar rotinas de backup automatizadas.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Alta.

(2) Fiscalizar e avaliar serviços de suporte

Descrição: Durante o ciclo de vida de um projeto, consultas ao suporte são primordiais. O cliente pode optar por montar uma equipe interna ou usar o fornecedor. Assim, deve-se analisar o tempo de resposta de solicitações ao suporte e também o tempo médio para a resolução de problemas de diversas gravidades. A satisfação do

cliente está diretamente relacionada à qualidade de atendimento do fornecedor. Questões de língua e internacionalização também devem ser analisadas.

Fase: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação.

Prioridade: Alta.

(3) Verificar e avaliar ferramentas de monitoramento e geração de relatórios

Descrição: Ferramentas de monitoramento são de importância para a manutenção de um sistema, pois dão meios para prever e analisar eventos e incidentes. Além disso, com o auxílio de relatório é possível extrair métricas como, por exemplo, para dimensionamento e capacidade de serviços.

Melhorias ao controle: Ferramenta com possibilidade de entregar mensagens de correio eletrônico ou de celular. Criar equipe de respostas a incidentes.

Fase: Monitoramento e Avaliação.

Prioridade: Média

(4) Verificar documentação para treinamento interno de equipes

Descrição: O sucesso da implantação e manutenção de um projeto está relacionado com o treinamento das equipes e usuários. Assim, deve-se verificar se o fornecedor possui material educacional préformatado com os serviços oferecidos.

Melhorias ao controle: Criar ambiente autoexplicativo.

Fase: Entrega e Suporte.

Prioridade: Média

(5) Suporte à investigação

Descrição: Suporte à investigação não se restringe a ferramentas de monitoramento e geração de relatórios. Ele deve possuir meios para, em caso de diligências ou investigação policial, entregar pedidos consistentes e com a informação necessária.

Melhorias ao controle: Criar ferramentas para facilitar o acesso à investigação de uma equipe de respostas a incidentes ou polícia.

Fase: Entrega e Suporte.

Prioridade: Baixa

(6) Conformidade com legislações e regulamentações

Descrição: Provedores e clientes devem estar em conformidade com as legislações dos países em que estão localizados. Assim, o armazenamento e o uso de dados devem estar sujeitos à jurisprudência

dessas localizações. O cliente deve checar se as legislações do país em que os dados serão trafegados estão em conformidade com aquelas que o próprio cliente deve seguir em seu país sede. Por exemplo, nos EUA, todas as empresas com ações na bolsa de valores estão sujeitas à lei Sabarnes-Oxley. Além disso, organizações estão sujeitas a regulamentações diversas conforme o ramo de atividade a que se propõem. Como exemplo, podem ser tomadas as entidades da área da saúde que devem resguardar os dados clínicos de seus clientes e seguir regulamentações específicas.

Fase: Planejamento e Organização.

Prioridade: Varia conforme o negócio do cliente.

(7) Término contratual, migração e eliminação de dados

Descrição: Criou-se um controle específico para o tratamento de término contratual, migração e eliminação de dados, pois sistemas ou até mesmo empresas podem deixar de existir, caso não se verifique com cuidado esses itens. Antecedendo o término contratual, todos os sistemas com ciclo de vida ativo devem ser migrados para outro ambiente. O fornecedor deve dar garantias de que os dados, uma vez eliminado, eles não devem ficar armazenados em mídias, mesmo aquelas que foram arquivadas ou para backup.

Melhorias ao controle: Utilização de um segundo fornecedor para armazenando de cópias de segurança e sincronização de serviços.

Fase: Planejamento e Organização.

Prioridade: Alta.

4 CONTROLES PARA ACORDOS DE NÍVEIS DE SERVIÇOS

Os controles, descritos na seção 3.3, também foram dispostos em tabelas no apêndice A com o objetivo de criar planilhas auxiliares para que eles pudessem ser verificados de maneira melhor estruturada.

Neste capítulo, estão demonstradas análises para ambientes de nuvem privada e outras para nuvem pública. No primeiro, foram criadas métricas, através do PCMONS (*Private Cloud MONitoring Systems*) (CHAVES, 2010), para verificar alguns controles. No segundo, os controles puderam ser analisados em sua totalidade. Finalmente, será feita uma análise de vulnerabilidades para averiguar se existem falhas de segurança nos ambientes.

4.1 DBAAS EM NUVENS PÚBLICAS

Alguns Sistemas de Gerenciamento de Bases de Dados (SGBD) que possuem versões para instalação em ambientes isolados externos à nuvem puderam ser testados. Para construção do serviço na nuvem, muitas restrições foram aplicadas aos SGBDs se comparadas às versões instaladas e customizadas em ambiente próprio.

De acordo com o http://db-engines.com/ (acessado em maio de 2013), os SGBDs mais populares são Oracle, MySQL e Microsoft SQL Server. Ainda, de acordo com o documento do Gartner *Market Share: All Software Markets, Worldwide, 2012*, as empresas comercias líderes em SGBD são Oracle, IBM, Microsoft, SAP e Teradata. Assim, com o objetivo de obter resultados que refletissem a abrangência de ferramentas largamente utilizadas, foram escolhidos três sistemas de gerenciamento para serem analisados neste trabalho. Listadas abaixo, os dois últimos são SGBDs comerciais e o primeiro é de código aberto:

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

Os resultados obtidos foram expostos em tabelas identificadas conforme a família ou domínio de controles. A estrutura utilizada por elas segue a seguinte convenção:

Ctrl: Identificador do controle baseado na listagem da seção 3.3, também repetidos nas tabelas do apêndice A;

OK: Expõe se o controle é atendido ou não ou se atende parcialmente; ainda, existem casos em que a estrutura do ambiente ou a tecnologia ou o próprio SGBD não dá suporte à aplicação do controle;

Observações: Informações relevantes e adicionais de como o controle foi validado.

4.1.1 Amazon Relational Database Service

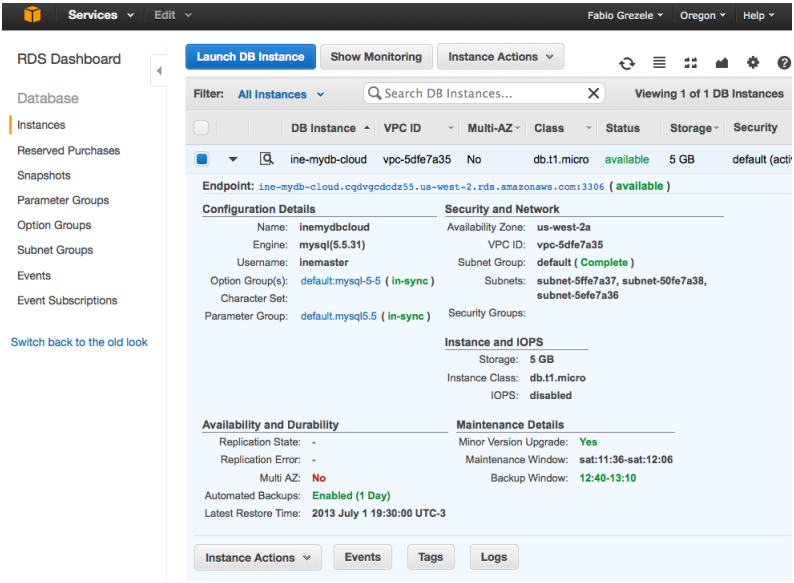


Figura 4 – Painel de Controle dos Serviços AWS

O Amazon *Relational Database Service* (Amazon RDS) é um serviço web que torna simples a criação, configuração, operação e provisionamento de bases de dados na nuvem. A administração da base fica a cargo da Amazon, enquanto o cliente poderá desenvolver aplicações. Estão disponíveis as tecnologias MySQL, Oracle ou SQL Server Database. O fornecedor se compromete a automaticamente atualizar e fazer backup das bases.

Foi criada uma conta no Amazon Web Services (AWS) que dá o direito de uso por um ano sem custos de uma micro instância de banco com até 20 GB de armazenamento e mais 20 GB de backup. Conforme especificação,

uma micro instância possui 630 MB de memória, até 2 cores de CPU, plataforma de 64 bits, baixa capacidade de interrupções E/S. Além disso, deve ser usado uma zona única de disponibilidade, sem redundância para outras regiões. A tecnologia utilizada poderia ser MySQL ou, exclusivamente, SQL Server Express Edition.

A utilização de MySQL foi preferida, pois já se haviam feito escolhas de Oracle Database e SQL Azure para outras validações utilizando os próprios desenvolvedores e fornecedores do conjunto de pacotes.

A figura 4 mostra o painel de controle para a base de dados MySQL no serviço de DBaaS da Amazon. Podem ser observadas informações relevantes nesta tela como data do último backup, redes e conexão. Além disso, pode-se efetuar ações como reiniciar, modificar, apagar, criar réplicas para somente leitura e recuperar a base.

Tabela 1: Verificação de Controles para Amazon RDS

Verificação de Controles para Amazon RDS		
Ctrl	**OK**	**Observações**
Planejamento e Avaliação de Risco		
A1	Sim	No painel de controle estão indicados detalhes de manutenção como janelas de backup e manutenção e também se atualizações menores de versão podem ser aplicadas automaticamente. Uma atualização menor, para o caso do MySQL, é efetuar atualização de uma versão 5.5.x para outra 5.5.y.
A2	Parcial	A versão utilizada para os testes foi a 5.5 do MySQL. Durante os testes foi lançada a versão 5.6 e incluída no portfólio de produtos. É possibilitado ao cliente a atualização daquela para esta versão e o provedor chama de "atualização maior". Nesse caso, ela deve ser agendada e é necessário efetuar parada do sistema, causando indisponibilidade. Existe a ressalva de que, uma vez atualizada, não se pode retroceder para a versão anterior. Um problema ocorreu quando foi solicitada a atualização: o sistema informou que não era possível atualizar o MySQL da versão 5.5.31 para a 5.6.12. No entanto, existe documentação à parte informando o procedimento manual de atualização que consiste em exportar os dados da versão antiga e importar na 5.6.

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
A3	Sim	As funcionalidades opcionais do banco podem ser observadas no painel de controle. No caso do MySQL 5.5, existe apenas uma opção padrão. No caso da versão 5.6, existe a opção memcached que permite que aplicações usem tabelas de maneira similar a chave-valor do NoSQL.
A4	Sim	Procedimentos e políticas de segurança podem ser alinhados e customizados para garantir maior privacidade. Existe documentação acessória para apoiar decisões e implementações. Amazon informa que o gerenciamento de usuários e privilégios é feita da mesma maneira que numa base independente, autônoma de MySQL.
A5	Sim	Os testes foram efetuados com a base no Oeste dos EUA, em Oregon. As propriedades ACID são mantidas. Não há particionamentos de rede na mesma localização. A consistência e a disponibilidade de dados são mantidas.
A6	Sim	O acesso à base de dados pode ser feito através do que a Amazon chama de "Virtual Private Cloud" (VPC). Habilita assim o isolamento da instância por um range de IPs específicos da própria rede da Amazon ou através de VPN com IPSec.
A7	Parcial	A utilização de chaves públicas está associada à autenticação para criptografar conexões. É possível ainda forçar os usuários a conectarem utilizando uma chave. No entanto, não é oferecida funcionalidade de criptografia nativa de dados do banco.
A8	Sim	Conforme exposto no sítio sobre conformidade, em *http://aws.amazon.com/compliance/*, AWS gerencia investigações forenses, conforme requisitos do "Payment Card Industry" (PCI) "Data Security Standard" (DSS). A equipe de respostas a incidentes do cliente pode entrar em contato com a Amazon. Além disso, estão em conformidade com DSS também na região do Brasil.
Segurança de Sistema Operacional e Ambiente de Virtualização		
B1	Sim	Conforme exposto nos controles A6 e A7, existe segurança e criptografia em conexões de rede.

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
B2	Sim	A troca de senhas entre servidores e clientes pode ser feita conforme exposto no controle A7.
B3	Sim	Pode se realizada auditoria em máquinas cliente para evitar arquivos de configuração com senhas. Inclusive deve ser ressaltada que as chaves criptográficas utilizadas para conexão devem ser armazenadas em locais seguros.
B4	Sim	Segundo (AMAZON, 2013b), todo tráfego de rede entrando ou saindo através de conexões IPSec VPN podem ser inspecionadas pelas próprias ferramentas de IDS/IPS do cliente.
B5	Sim	Como os usuários podem ser gerenciados pelo cliente, incluindo permissões e autorizações, privilégios mínimos podem ser definidos.
B6	Sim	Amazon RDS faz backups diários da base e eles podem ser manipulados pelo cliente. Caso deseje, o cliente pode utilizar a ferramenta mysqldump do próprio MySQL para fazer backups da base e armazenar em local de sua preferência. Os registros de alteração da base estão disponíveis, caso necessário, como tabelas da própria base.
B7	Sim	Possível alterar as senhas da base após a importação de dados.
B8	–	O acesso ao sistemas de arquivos não está permitido neste modelo.
B9	Sim	Como o gerenciamento de usuários pode ser feito pelo cliente, privilégios podem ser refinados e alterados conforme a necessidade.
B10	Sim	Dispositivos de rede, incluindo firewall, são utilizados para monitorar e controlar comunicações externas e internas. Não foram encontradas informações sobre antivírus, no entanto, ele também pode ser implementado em VPN com IPSec para filtrar arquivos antes de serem inseridos no canal.
B11	Sim	VPNs com IPSec podem ser configuradas.
Autenticação e Autorização		

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
C1	Sim	A auditoria pode ser feita em usuários normalmente como se faz em uma instalação independente de MySQL.
C2	Sim	Seguem as regras padrão para o SGBD, em que é possível armazenar senhas criptografadas ou não e incluir procedimentos para garantir a complexidade.
C3	Sim	Podem ser feitas normalmente, inclusive contas administrativas podem ser eliminadas pelo banco. Podem ser criadas novamente através do painel de controle do AWS.
C4	Sim	Procedimentos para gerenciamento de senhas podem ser incluídos. Na versão 5.6, existe uma funcionalidade em que políticas para senhas podem ser validadas globalmente. Para mais informações, veja documentação sobre o *plugin* validate_password.
C5	Sim	As senhas de usuários privilegiados podem ser alteradas através da linha de comando ou alguma ferramenta que o cliente possua.
C6	Sim	O servidor de conexões não pode ser configurado pelo cliente, no entanto, todas as conexões ao banco podem ser feitas com uso de senha ou chaves criptográficas.
Controle de Acessos		
D1	Sim	Um modelo de segurança para privilégio granular de objetos é uma das funcionalidades do MySQL, permitindo que usuários tenham acesso somente aos dados que compete a eles.
D2	Sim	Verificações às permissões dos usuários administrativos ou de operação podem ser feitas através de acesso direto ao banco.
D3	Sim	Permissões de todos os usuários podem ser verificadas através de acesso direto ao banco.
D4	Sim	Ligações entre bases não são permitidas nativamente.
D5	Sim	Controle de papéis, usuários e identidade pode ser feito normalmente pelo cliente.
D6	Sim	Classificação pode ser feita conforme a necessidade do cliente.
Auditoria		

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
E1	Parcial	MySQL possui uma opção para configurar auditoria, no entanto, não foram encontradas informações sobre a ativação no RDS. Registros de auditoria podem ser observados em arquivos binários específicos que podem ser tratados pelo cliente, mas não está clara a informação contida neles.
E2	Não	Não foram encontradas informações detalhadas sobre auditoria da base.
E3	Parcial	O número de conexões à base pode ser monitorado através de gráficos que são gerados periodicamente.
Camada de Rede		
F1	Sim	A porta padrão 3306 é configurada para as conexões e ela só pode ser alterada em tempo de criação da base.
F2	Não	Ligações entre bancos não podem ser configuradas e a configuração do servidor de conexão não está liberada para o cliente.
F3	–	Ligações entre bases não são permitidas.
F4	–	Ligações entre bases não são permitidas, no entanto, qualquer usuário de conexão pode obedecer aos critérios de menor privilégio.
F5	Sim	A conexão entre servidores e clientes pode ser feita usando criptografia através de chaves públicas.
Disponibilidade, Cópia de Segurança e Recuperação		
G1	Sim	Procedimentos de backup e recuperação podem ser documentados pelo cliente. Além disso, o cliente pode configurar rotinas autônomas e independentes da nuvem através do mysqldump, podendo proporcionar mais alternativas no Plano de Continuidade de Negócio.
G2	–	A localização de mídias de armazenamento não está disponível. Segundo (AMAZON, 2013b), zonas de disponibilidade são todas redundantemente conectadas.
G3	Sim	Estratégias de recuperação em instâncias isoladas podem ser recuperadas para validar os arquivos de backup produzidos pelo AWS. Além disso, caso seja de interesse do cliente, procedimentos de cópia e recuperação também podem ser executados independentemente da nuvem.

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
G4	Sim	Os procedimentos de recuperação podem ser agendados regularmente pelo cliente.
G5	Sim	Os procedimentos de recuperação documentados em G1 podem ser revistos e executados regularmente pelo cliente.
Desenvolvimento e Servidores de Aplicação		
H1	Sim	O ambiente de produção pode ser completamente isolado de outros ambientes. Cópias para somente leitura podem ser criadas através do painel de controle. Nesse caso, dados de uma base são replicados assincronamente na outra. Detalhe interessante: também é oferecido a possibilidade de configuração de portas de conexão diferentes da padrão.
H2	Sim	O painel de controle do RDS permite a recuperação de bases através de backups ou de um ponto específico no tempo. Essa recuperação deve ser feita em instância separada, possibilitando a criação facilitada de ambientes de desenvolvimento, homologação e testes.
H3	Sim	A segurança de usuários de portal pode ser aprimorada pelo cliente.
H4	Sim	Dados e usuários de exemplo podem ser removidos pelo cliente.
H5	Parcial	Conforme (AMAZON, 2013b), os controles de vulnerabilidades e ataques é feito através de monitoramento e rastreamento periódico das redes da Amazon. O cliente também pode solicitar liberação de janela para efetuar testes de penetração. Apesar disso, controles mais avançados como injeção de código devem ser desenvolvidos pelo cliente.
Contratos e Comprometimento		

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
I1	Sim	O acordo de nível de serviço com relação a tempo de disponibilidade pode ser consultado em *http://aws.amazon.com/rds-sla/*. Ele se refere somente a instâncias disponíveis em regiões múltiplas, o que pode ser configurado com um custo adicional devido à replicação de dados. O cliente pode solicitar estorno de 10% dos valores, caso a disponibilidade mensal seja menor que 99,95% e maior que 99%, ou seja, caso as instâncias fiquem indisponíveis entre 21,56 minutos e 7,2 horas mensais. Nos casos de indisponibilidade maior que 7h12min, o estorno será de 25%.
I2	Sim	Existem modalidades diferentes para o contrato de suporte sendo uma livre, uma para desenvolvedores, uma para negócios e outra empresarial. O que varia, basicamente, entre elas são os meios de contato, horários de atendimento, tempo de resposta e produtos suportados. No caso de suporte livre de pagamento adicional, só é possível a abertura de chamados para problemas de contas e pagamentos.
I3	Sim	O painel de controle possui ferramentas de monitoramento que podem ser customizadas. Relatórios de uso de serviços e componentes são fornecidos.
I4	Sim	Como as alterações nos serviços diferem pouco de um SGBD nativo, podem ser usadas formas de treinamento tradicional. Além disso, existe farta documentação explicativa e educativa sobre os recursos da Amazon.
I5	Sim	A equipe do cliente pode entrar em contato com a Amazon, no entanto, não informam se existem canais diretos com polícias locais de cada região.
I6	Sim	Segundo (AMAZON, 2013b), o cliente deve avaliar cuidadosamente os serviços escolhidos e fica sob sua própria responsabilidade a integração desses serviços com ambientes de TI, leis e regulamentações.

Continua na página seguinte

Tabela 1 – *Continuação da página anterior*

Ctrl	OK	Observações
I7	Sim	Ao término contratual, a Amazon não eliminará os dados por 30 dias, caso haja pagamento à parte. O término do contrato pode ser celebrado por ambas as partes e a migração pode ser feita pelo cliente utilizando a ferramenta mysqldump. Não foram encontradas informações sobre a eliminação ou retenção dos dados do cliente nos servidores da Amazon, após finalizado o acordo entre as partes.

4.1.2 Microsoft Windows Azure SQL Database

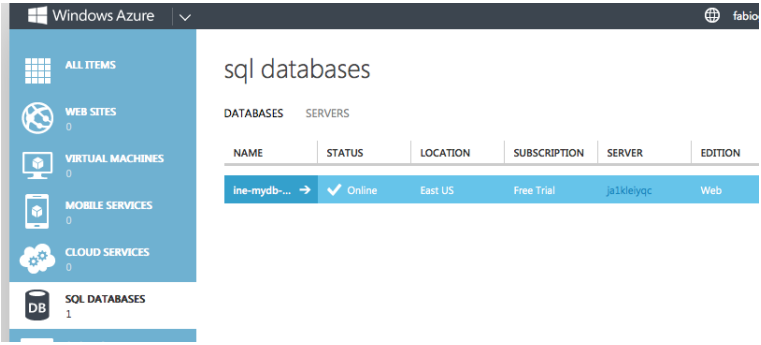


Figura 5 – Interface de Gerenciamento dos Serviços do Windows Azure

Foi criada uma conta que dá acesso aos serviços Windows Azure incluindo SQL Database para testes sem custos pelo período de um mês. Informações, documentações e interfaces puderam ser acessados através do sítio da Microsoft *http://www.windowsazure.com/*. A figura 5 mostra a interface inicial do Windows Azure com destaque para SQL Database, onde se pode consultar a base de dados e o servidor virtual associado a ela.

O SQL Azure Database oferece interoperabilidade de alto nível, possibilitando aos consumidores construir aplicações que utilizem recursos de bases relacionais. Além disso, permite a criação de aplicações híbridas em que dados podem ser compartilhados entre bases SQL Azure e SQL Server.

Tabelas oferecem capacidades NoSQL para aplicações que requeiram o tratamento de uma grande quantidade de dados não estruturados. Tabelas são virtualmente acessadas de qualquer lugar via REST ou APIs gerenciadas.

O armazenamento para Bynary Large Object (Blob) pode chegar a 200 terabytes.

A verificação dos controles descritos na seção A estão na sequência para o serviço de DBaaS da Microsoft.

Tabela 2: Verificação de Controles para Windows Azure SQL Database

Verificação de Controles para Windows Azure SQL Database		
Ctrl	**OK**	**Observações**
	Planejamento e Avaliação de Risco	
A1	–	Não foram encontradas informações sobre versões de banco para o serviço. Apenas informa as edições que podem ser usadas em tempo de criação da base: Web e Business. Além disso, é documentada de que maneira versões do Microsoft SQL Server –a saber 2008 R2, 2008 e 2005– são compatíveis com o DBaaS.
A2	Não	Versões de banco e pacotes de correção não estão disponíveis nas interfaces.
A3	Sim	Para incrementar a segurança, o Azure retirou algumas das funcionalidades nativas dos bancos SQL Server.
A4	Sim	O Windows Azure Trust Center traz informações sobre segurança, privacidade e conformidade que podem ser usados para validar procedimentos e políticas de segurança do cliente.
A5	Sim	A localização da base de testes está na região do leste do EUA sendo garantidas, conforme a necessidade e investimento do cliente replicação numa mesma região ou diferentes. Ainda estão disponíveis as regiões oeste, central norte e central sul dos EUA, norte e oeste da Europa, leste e sudeste da Ásia. As transações de banco são feitas em uma única região respeitando assim as propriedades ACID, ver subseção 2.3.1.1.
A6	Sim	O acesso pode ser feito através dos diversos serviços Windows Azure ou através de aplicação localizada no cliente. Um firewall é dedicado para o controle de acessos restrito a IPs do cliente. As interfaces de gerenciamentos são do tipo API REST.

Continua na página seguinte

Tabela 2 – *Continuação da página anterior*

Ctrl	OK	Observações
A7	Parcial	Certificados de gerenciamento são requisitos para autenticar acesso de clientes para uso de recursos do Windows Azure. No entanto, chaves criptográficas não podem ser utilizadas para o gerenciamento de criptografia de banco de dados.
A8	Parcial	São oferecidas interfaces em que é possível observar deadlocks, falhas e sucessos de conexões, performance de consultas. Há informações sobre a documentação de um processo de continuidade de negócio baseado em sincronia, cópia e backup de bases. No entanto, inexiste uma ferramenta específica para gerenciamento de incidentes.
Segurança de Sistema Operacional e Ambiente de Virtualização		
B1	Sim	As conexões são feitas através de interfaces web utilizando HTTPS. Conexões de servidores de aplicação com o banco podem usar criptografia.
B2	Sim	É possível que haja conexões seguras entre servidores e clientes. Estes podem usar uma gama de produtos dentre os quais o "Microsoft SQL Server Data Tools" que provê um ambiente integrado para desenvolvedores de bases de dados.
B3	Sim	Observe-se que a configuração ODBC no controle B1 contém a senha de conexão. Assim, deve-se armazenar com proteção e restrição esses dados. A documentação deve ser feita para proporcionar auditoria e verificações de segurança.
B4	Não	Informações sobre IDS ou IPS não foram encontradas.
B5	Parcial	As conexões para o banco podem ser limitadas através de um firewall, no entanto, para os usuários de banco não se puderam encontrar restrições.

Continua na página seguinte

Tabela 2 – *Continuação da página anterior*

Ctrl	OK	Observações
B6	Sim	Os arquivos de exportação de dados devem ficar em espaços reservados no "Windows Azure Storage". Esses espaços podem ser privados ao ambiente API REST ou públicos. Neste último caso, é permitido fazer o seu download sem criptografia em HTTP, o que pode resultar em descoberta de dados sensíveis. Os arquivos de alteração de banco não ficam disponíveis aos administradores ou desenvolvedores, no entanto, é possível definir o tempo em que se queira armazenar.
B7	Não	A troca de senhas não foi encontrada na interface de gerenciamento web.
B8	–	Não é possível utilizar tabelas externas.
B9	Sim	O acesso pode ser restrito aos administradores ou a desenvolvedores. Para estes últimos, a configuração não é possível através da interface de gerenciamento do Windows Azure.
B10	–	Não foram encontradas informações sobre antivírus. Já um controle de acessos por IP é fornecido ao cliente.
B11	Sim	Redes privadas podem ser construídas através de isolamento de redes por VLANs, conforme (KAUFMAN; VENKATAPATHY, 2010).
Autenticação e Autorização		
C1	Sim	Durante a fase de testes foi liberada apenas a criação de um usuário administrativo. A configuração de usuários para aplicação não é trivial e sugere-se a criação de ambientes separados para desenvolvimento através de "Data-tier Application".
C2	Não	Não é possível fazer auditoria de senhas da base, pois elas são armazenadas de criptograficamente.
C3	Sim	Não existem contas padrão.
C4	Não	Não foi possível incluir gerenciamento de senha para a conta de banco gerada.
C5	Não	Inexiste uma maneira trivial de gerenciar os usuários do banco através da interface web.
C6	–	Está apenas liberada a interface de conexão ao banco e não seus componentes.
Controle de Acessos		

Continua na página seguinte

Tabela 2 – *Continuação da página anterior*

Ctrl	OK	Observações
D1	Não	O acesso de toda a base é liberada a administradores ou a desenvolvedores, não sendo possível configuração administrativa de acesso granular.
D2	Sim	Não é permitido através de interface de administração, somente através de ferramentas auxiliares.
D3	Sim	Utilizando ferramentas auxiliares pode-se fazer revisões de permissões de usuários.
D4	Sim	Existem ligações entre bases sincronizadas que podem ser analisadas. As bases podem ser sincronizadas com outras regiões e, para sua realização, deve ser criado um usuário específico. Além disso, base podem ser sincronizadas, através de agentes, com bases localizadas no cliente.
D5	Sim	Através de ferramentas auxiliares.
D6	Sim	A classificação de dados pode ser executada pelo cliente.
Auditoria		
E1	Parcial	Auditoria de conexões pode ser realizada através da interface de administração. No entanto, outros tipos de auditoria devem ser estudados para verificar a implementação de ferramentas externas.
E2	Não	Uma das funcionalidades retiradas do SQL Server para que pudesse ser utilizado na nuvem foi a auditoria de dados.
E3	Sim	Interface de monitoramento permite auditoria de acessos com sucesso ou com falha à base.
Camada de Rede		
F1	Não	A porta padrão 1433 para conexão ao banco é informada ao cliente. Não se pode efetuar alterações.
F2	Sim	Não é facultado ao cliente configurar o servidor de conexões, no entanto, pode ser utilizado criptografia para conexões. Além disso, a configuração para sincronização de bases pode ser feita com criptografia.
F3	Sim	Isso pode ser feito pelo cliente.
F4	Não	Usuários para sincronização de bases são privilegiados.
F5	Sim	Especificado em diversas documentações do serviço Microsoft Azure.
Disponibilidade, Cópia de Segurança e Recuperação		

Continua na página seguinte

Tabela 2 – *Continuação da página anterior*

Ctrl	OK	Observações
G1	Sim	Existe documentação do Microsoft Azure que podem auxiliar o cliente. Recomenda-se agendar a cópia periódica de uma base e, a partir desta, exportar os dados. Assim, será mantida a consistência transacional da base. Ainda, recomenda-se agendar procedimentos de recuperação.
G2	Sim	Não é informado se no procedimento de backup do Azure são utilizadas fitas, no entanto, isso pode ser feito com cliente através dos backups de bases sincronizadas.
G3	Sim	Esse procedimento pode ser feito pelo cliente.
G4	Sim	Esse procedimento também pode ser feito pelo cliente.
G5	Sim	Existe documentação do Azure referente à continuidade do negócio utilizando *data centers* diferentes para sincronização e cópias de bases de dados.
Desenvolvimento e Servidores de Aplicação		
H1	Sim	Pode ser configurado pelo cliente através da sincronização de bases. Ainda utilizando o "Data-tier Application", que é uma unidade para autorizar, construir e gerenciar objetos de dados. Ele simplifica atualizações de uma versão de banco de dados para outra.
H2	Sim	Com facilidades de sincronia e cópia de ambientes, a segmentação entre produção, desenvolvimento, homologação ou teste pode ser obtida.
H3	Sim	Como a base pode ser acessada externamente, serviços de portal podem ser configurados em outros provedores. Isso aumenta o desafio e os cuidados para garantir a segurança de usuários de portal. Internamente, existe o serviço de configuração de Web Sites no Windows Azure em que se podem fornecer dados para conexão em tempo de criação do serviço.
H4	Sim	De fácil execução pelo cliente.
H5	Sim	Um documento extenso com objetivo de apoiar a segurança em aplicativos do Windows Azure está disponível, veja (MEIER; ENFIELD, 2010). No entanto, não foram encontradas informações sobre o uso de IDS ou IPS.
Contratos e Comprometimento		

Continua na página seguinte

Tabela 2 – *Continuação da página anterior*

Ctrl	OK	Observações
I1	Sim	Há possibilidade de uso de ferramenta própria para verificar a disponibilidade de serviços já que o SQL Azure pode ser acessado externamente.
I2	Sim	Os serviços de suporte não puderam ser avaliados em tempo de testes do ambiente.
I3	Sim	Existem ferramentas de monitoramento e ainda um serviço à parte chamado "SQL Reporting". As ferramentas de monitoramento não permitem fazer análises avançadas.
I4	Sim	Existe farta documentação disponível publicamente na Internet que pode ser consultada e utilizada para elaboração de manuais e treinamentos internos.
I5	Parcial	Existem equipes atendendo a incidentes de segurança, no entanto, não está especificado o tratamento com polícias regionais.
I6	Parcial	Delega ao cliente a verificação de conformidade com regulamentações e legislações regionais. Há certificação para ISO/IEC 27001:2005, SSAE 16/ISAE 3402 e HIPAA.
I7	Sim	Término, suspensão e eliminação de dados estão expressos em contrato. Os dados do cliente são armazenados por, pelo menos, 90 dias após o término do contrato, caso solicitado pelo cliente. Após essa retenção, em até 30 dias todos os dados do cliente serão eliminados.

4.1.3 Oracle Database Cloud Service

Foi criada uma conta para efetuar testes que dá o direito de uso dos serviços pelo período de um mês sem custo. As ferramentas, interfaces e informações foram feitas através do sítios *https://cloud.oracle.com/*.

O serviço de banco de dados traz uma solução integrada entre aplicação e banco, permitindo o desenvolvimento rápido de aplicações, serviços web RESTful, suporte a SQL e PL/SQL, aplicações de produtividade disponíveis.

Baseado na versão 11gR2 do banco de dados da Oracle, o ambiente foi construído em equipamentos da própria Oracle, o Exadata, em conglome-

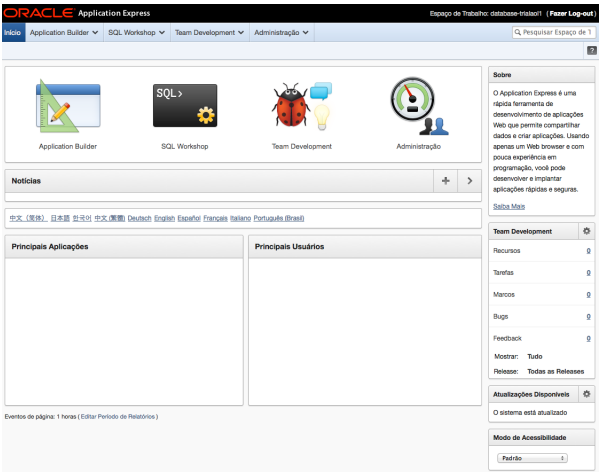


Figura 6 – Interface do Oracle Appplication Express

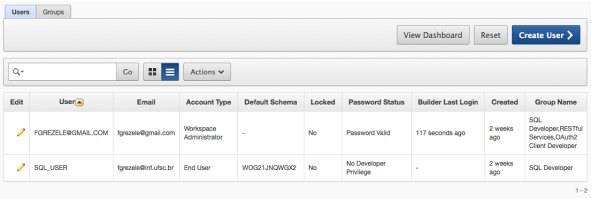


Figura 7 – Interface de Administração de Usuários e Grupos

rados redundantes com alta-disponibilidade. Os dados dos clientes são isolados, o armazenamento é criptografado e existe gerenciamento de recursos. O acesso é feito através da interface Oracle Application Express e serviços web. Ainda podem ser criados internamente na rede do serviço conexões JDBC.

Observe na figura 6 a interface de administração dos serviços de nuvem da Oracle. Informações importantes como atualizações disponíveis para a infraestrutura do banco podem ser vistas nessa tela de entrada. Além disso, acessos às interfaces de desenvolvimento de aplicações, gerenciamento de desenvolvimento, administração do serviço e ferramentas SQL também podem ser feitos. Mais detalhadamente, a interface de administração permite gerenciar o serviço, usuários e grupos, monitorar atividades, gerar relatórios e acessar um painel de controle.

Segue a validação da Proposta para o serviço de DBaaS do Oracle Database Cloud Service.

Tabela 3: Verificação de Controles para Oracle Cloud

Verificação de Controles para Oracle Database Cloud Service		
Ctrl	**OK**	**Observações**
Planejamento e Avaliação de Risco		
A1	Sim	Segundo o documento (ORACLE, 2012), a versão de banco utilizada é a mais recente já com o último pacote de atualizações aplicado. Além disso, a interface de gerenciamento "Oracle Application Express", figura 6, informa que o sistema está atualizado e não atualizações disponíveis.
A2	Sim	Conforme o mesmo documento (ORACLE, 2012), a versão do Oracle Database Cloud Service é baseada no Oracle Database 11g Release 2, edição Enterprise, com o último pacote de atualizações aplicado. O serviço de DBaaS está na versão 13.1.
A3	Sim	Para incrementar a segurança do DBaaS muitas funcionalidades opcionais foram retiradas tais como geolocalização ou OLAP. O único opcional mantido foi o particionamento de objetos do banco. Além disso, o acesso a objetos, dados de dicionário, recursos e serviços são restritos se comparado ao banco convencional.
A4	Sim	Estão bem documentados os procedimentos para conformidade com políticas, regulamentações, normas e procedimentos existentes no cliente.
A5	Sim	Os serviços de nuvem estão localizados nos EUA, no *data center* de Austin. A escolha de data center é feita em tempo de criação dos serviços e, depois, na conexão. Existem ainda as opções de Chicago e a regional da Europa, do *Middle East* e África (EMEA). As transações de banco são feitas numa única região respeitando as propriedades ACID, ver subseção 2.3.1.1.
A6	Sim	O uso de aplicações é restrito. Oracle Application Express (APEX) é plataforma de desenvolvimento e serviços web RESTful faz a interface com os dados.

Continua na página seguinte

Tabela 3 – *Continuação da página anterior*

Ctrl	OK	Observações
A7	Não	No entanto, há criptografia de dados armazenados na base ou em arquivos de backup utilizando Transparent Data Encryption (TDE). Não há necessidade de alteração de códigos para uso de dados, pois a criptografia é feita de forma transparente.
A8	Parcial	Existe interface para monitor e gerenciar serviços. Possibilidade de abrir requisições ao suporte e monitorar os SLAs. Além disso, internamente, é utilizado um gerenciador de recursos que impede o uso excessivo de processamento e memória. No entanto, o APEX, figura 6, não fornece uma interface exclusiva para o gerenciamento de incidentes ou recursos.
Segurança de Sistema Operacional e Ambiente de Virtualização		
B1	Sim	Segundo (GREENWALD, 2012) e (ORACLE, 2012), interações nativas de rede com o banco são restritas. Serviços web permitem acesso seguro a SQL e PL/SQL.
B2	Sim	As aplicações rodam apenas no ambiente de nuvem, ficando restritas. Conexões restritas podem ser feitas pelo cliente usando o aplicativo da Oracle PL/SQL Developer, permitindo visualizar o esquema do banco, mas não interagir com ele. Usuários específicos devem ser criados para esse tipo de conexão. Observe figura 7.
B3	Sim	O cliente deverá fazer essa varredura em seu ambiente.
B4	Sim	Existência de IDS e IPS, conforme contrato padrão (ORACLE, 2013).
B5	Sim	Durante a criação de usuários são permitidos os papéis de administrador e desenvolvedor e grupos para conexão através da aplicação, da interface de gerenciamento ou desenvolvimento.
B6	Sim	É permitida a auditoria ao cliente. Os dados exportados ficam em um diretório para transferência por SFTP. Alterações na aplicação são armazenadas em tabelas do banco.
B7	Sim	A importação de dados pode ser feita através de usuários com perfil de SQL Developer, utilizando o aplicativo de mesmo nome. As senhas podem ser alteradas ou até mesmo retirar o perfil de SQL Developer do usuário que fez a importação.

Continua na página seguinte

Tabela 3 – *Continuação da página anterior*

Ctrl	OK	Observações
B8	–	Não é permitido o uso de tabelas externas.
B9	–	Aplicações e códigos executados no banco só são permitidos através de interface própria, desenvolvida para o uso em DBaaS.
B10	Sim	Políticas contratuais especificam o uso de antivírus para upload de arquivos e firewall para controle de tráfego. Ademais, as aplicações e bancos rodam em ambientes isolados em modelo multi-tenant.
B11	Sim	As conexões com as aplicações e banco são feitas através de serviços web em HTTPS ou utilizando a ferramenta SQL Developer.
Autenticação e Autorização		
C1	Sim	É possível extrair dados para auditoria através de relatórios disponíveis na interface de administração.
C2	Não	Não é possível fazer auditoria das senhas da base, pois elas são armazenadas de maneira criptografada. Além disso, não é possível criar funções para reforçar a segurança de senhas da aplicação. Deve-se usar políticas nativas do ambiente, descritas abaixo no controle C4.
C3	Sim	Não possuem contas padrão.
C4	Parcial	Não é oferecida essa funcionalidade para contas, no entanto, são aplicadas restrições para criação de contas administrativas que devem ter ao menos 6 caracteres, sendo ao menos um número e uma letra maiúscula. Contas da aplicação devem ter ao menos 8 caracteres, sendo ao menos um número e uma letra.
C5	Sim	As senhas de usuários privilegiados são criadas em tempo de configuração dos serviços DBaaS, não havendo usuários ou senhas padrão.
C6	Sim	Não se tem conhecimento sobre configuração do gerenciador de conexão, no entanto, aplicação e banco só podem ser utilizados através de senhas.
Controle de Acessos		
D1	Não	O acesso de toda a base é liberada para usuários administrativos ou desenvolvedores.
D2	Sim	Permitido através da interface de gerenciamento de usuários da figura 7 e também de um Console de Identidade.

Continua na página seguinte

Tabela 3 – *Continuação da página anterior*

Ctrl	OK	Observações
D3	Sim	As interfaces citadas em D2 permitem fazer a revisão de usuários e permissões.
D4	–	Não é permitida a ligação entre bases de dados.
D5	Sim	As interfaces citadas em D2 permitem fazer a revisão de usuários e permissões.
D6	Sim	A classificação de dados é permitida através das ferramentas Web disponibilizadas pelo DBaaS e também pelo SQL Developer.
Auditoria		
E1	Sim	A auditoria é feita através de relatórios e interfaces administrativas. Auditoria vem configurada por padrão, no entanto, novos requisitos ou padronizações não são possíveis de serem implementados.
E2	Parcial	Erros de aplicação são auditados o que pode ser usado para encontrar falhas de inserção. No entanto, não há como auditar especificamente falhas de inserção.
E3	Sim	São disponibilizados relatórios para falhas e sucesso de conexões para os diversos componentes do DBaaS.
Camada de Rede		
F1	–	Não é possível obter detalhes de como as conexões ao banco são feitas.
F2	Sim	Conforme (GREENWALD, 2012), múltiplos hóspedes são isolados e não há conexões entre bancos.
F3	–	Não é possível a conexão entre bancos.
F4	–	Não existem conexões entre bancos.
F5	Sim	Segundo (ORACLE, 2012), isolamento seguro está configurado para o DBaaS.
Disponibilidade, Cópia de Segurança e Recuperação		
G1	Sim	Conforme (ORACLE, 2013), cláusulas contratuais informam os procedimentos de backup e recuperação. No entanto, o cliente deve se responsabilizar por um plano de continuidade de negócio.
G2	Sim	Os ambientes são redundantes e o armazenamento é feito em discos ou fitas.
G3	Não	Não facultado ao cliente a validação de mídias de recuperação.
G4	Não	Não facultado ao cliente o teste de seu plano de continuidade.

Continua na página seguinte

Tabela 3 – *Continuação da página anterior*

Ctrl	OK	Observações
G5	Sim	O cliente deve elaborar documentação apropriada para procedimentos de recuperação de desastre, conforme descritos em contrato.
Desenvolvimento e Servidores de Aplicação		
H1	Sim	Existe uma configuração em que cada página da aplicação pode ser bloqueada para desenvolvedores.
H2	Parcial	É permitida a cópia de aplicações para utilizar outros esquemas de bancos de dados, no entanto, não existe uma ferramenta para facilitar o fluxo de trabalhos para o ambiente de produção. Além disso, é viável exportar e importar aplicações.
H3	Sim	As aplicações rodam com usuários criados exclusivamente para elas, com acesso exclusivo para este fim no banco. A segurança desses usuários fica restrita ao provedor de DBaaS, não sendo possível alterações através das interfaces de administração.
H4	Sim	As interfaces administrativas permitem a exclusão de aplicações e dados de exemplo.
H5	Parcial	O controle de vulnerabilidade pode ser feito por IDS e IPS, além disso, existe uma equipe que responde por incidentes de segurança. No entanto, não estão especificados como são feitos os controles de injeção de código e dados. Cláusulas contratuais reforçam que períodos de ataques por DoS ou desastres naturais, por exemplo, não podem ser contabilizados como de indisponibilidade.
Contratos e Comprometimento		
I1	Sim	É de responsabilidade do cliente documentar, verificar e fiscalizar os níveis de serviço e cláusulas contratuais. Essa atividade é de grande valia para o sucesso de implementações em DBaaS.
I2	Sim	Existe suporte para todos os serviços contratados, no entanto, ele não pôde ser avaliado. Esta prática foi feita em modo de testes do DBaaS e o suporte não está aberto para esse tipo de contrato.
I3	Sim	Ferramentas de monitoramento e relatórios são disponibilizadas. No entanto, está especificado em contrato que não é facultado ao cliente introduzir suas próprias ferramentas de monitoramento.

Continua na página seguinte

Tabela 3 – *Continuação da página anterior*

Ctrl	OK	Observações
I4	Sim	Existe farta documentação e tutoriais de apoio que podem ser usados para elaboração de treinamentos das equipes do cliente.
I5	Parcial	Existe uma equipe de resposta a incidentes, no entanto, não está especificado como seriam os tratamentos com polícias localizadas na região do cliente.
I6	Parcial	Solicita ao cliente que informe a Oracle quaisquer requisitos de obrigações regulatórias antes de assinar contratos. Especifica que está alinhado com boas práticas da ISO/IEC 27002:2005.
I7	Sim	Existe uma política específica para suspensão e término de contrato. Garante que dados de ambientes ou aplicações serão apagados de modo que não permita serem lidos ou acessados, a menos que haja impedimento legal para isso. A migração de dados deve ser feita com antecedência pelo próprio cliente, através das interfaces de administração.

4.2 DBAAS EM NUVEM PRIVADA

Em ambientes em que haja o domínio da infraestrutura, existe a possibilidade de que alguns dos controles, propostos no capítulo 3, possam ser averiguados com ferramentas e gerar métricas. Assim, criou-se em laboratório um ambiente baseado em nuvem privada e utilizou-se o PCMONS (*Private Cloud MONitoring System* ou Sistema de Monitoramento para Nuvem Privada) como ferramenta de gerenciamento e monitoramento. A ferramenta possibilita aos provedores fornecer um serviço de métricas para as suas entregas. Sob o ponto de vista do cliente, esse poderá ampliar sua visão sobre aquilo que recebe do provedor, podendo fiscalizar e monitorar os serviços. Além disso, as métricas configuradas podem dar suporte aos clientes na análise de níveis de contrato. A ferramenta possibilita, ainda, que alertas sejam enviados em casos de alteração daquilo que foi preestabelecido.

Através do trabalho de (CHAVES, 2010), o ambiente de laboratório foi construído. As especificações para o ambiente foram:

1. Equipamento servidor com suporte à virtualização através da CPU;

2. Sistema operacional hospedeiro: GNU/Linux Ubuntu;

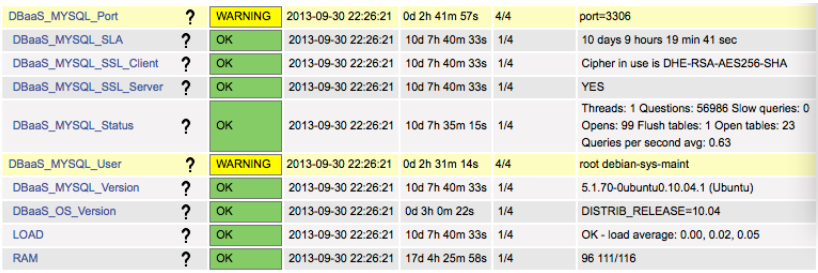
3. Camada de infraestrutura: OpenNebula utilizado para gerenciar e monitorar o ambiente de *data center* de nuvem privada;

4. Camada de virtualização: KVM (*Kernel-based Virtual Machine*) utilizado para criar instâncias de máquina virtual. O KVM é gerenciado pelo OpenNebula;

5. Camada de visualização: Nagios que é uma aplicação com visualização através da web utilizada para monitoramento de servidores, serviços e aplicações. Configurado em modo passivo, permite o recebimento de informações de agentes externos;

6. Camada de monitoramento: PCMONS que possui uma interface de comunicação com o Nagios;

7. Sistemas de Gerenciamento de Banco de Dados: MySQL 5.1 e Oracle Database Express Edition 11g.



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

Figura 8 – Controles verificados pelo PCMONS

O PCMONS é um sistema modular e extensível. Seus módulos são executados nos seguintes componentes da estrutura da nuvem privada: 1. *Boot* da máquina virtual: permite que configurações iniciais sejam atribuídas no momento em que máquinas virtuais são instanciadas, dando a essas um novo contexto. Um conjunto de políticas pode ser definida para monitoramento de SLA, por exemplo, em tempo de *boot*; 2. Máquinas virtuais em execução: nesta fase, tendo um contexto já definido na fase anterior, com a máquina virtual já em execução, são ativadas as operações de monitoramento através de agentes; 3. Interface: um servidor de notificação que roda no ambiente da camada de infraestrutura recebe informações dos agentes sendo executados

nas máquinas virtuais. Esses agentes tratam essas informações e as enviam para o Nagios.

Nem todos os controles internos descritos no capítulo 3 podem ser quantificados, assim somente um subconjunto deles será avaliado nesta seção. Abaixo estão listadas métricas geradas para o PCMONS, utilizando o MySQL, (figura 8):

- **Métrica: DBaaS_MYSQL_Audit**
  Detalhes: A auditoria para MySQL pode ser adicionada, a partir das versões 5.6.10 Enterprise Edition, diferente da versão usada em laboratório. A especificação pode ser adicionada nos arquivos de configuração do SGBD, geralmente, o arquivo my.cnf.
  Controle medido: E1, E2, E3
  Exemplo de saída: plugin-load=audit_log.so

- **Métrica: DBaaS_MYSQL_Port**
  Detalhes: Informa a porta para conexão com o servidor de banco de dados MySQL. Observe que, neste caso, está sendo utilizada a porta padrão. Ela pode ser obtida no arquivo my.cnf.
  Controle medido: F1
  Exemplo de saída: port=3306

- **Métrica: DBaaS_MySQL_SLA**
  Detalhes: Essa métrica foi obtida através do *status* do banco MySQL, onde se informa o *uptime*. Observa-se que o SLA, em termos de disponibilidade, pode variar conforme contrato com o provedor. Por exemplo, para Amazon RDS (AMAZON, 2012c), os clientes recebem estorno de valores para indisponibilidade maior do que 0,05% (3h36min por mês).
  Controle medido: I1
  Exemplo de saída: 10 days 9 hours 34 min 44 sec

- **Métrica: DBaaS_MySQL_SSL_Client**
  Detalhes: Verifica se na conexão com o servidor está sendo usada criptografia por SSL. Em caso positivo, qual algoritmo de cifragem está sendo usado. Para que uma conexão seja criptografada é necessário a criação e uso de uma Infraestrutura de Chaves Públicas (ICP).
  Controle medido: A6, A7, B1, B2, F5
  Exemplo de saída: Cipher in use is DHE-RSA-AES256-SHA

- **Métrica: DBaaS_MySQL_SSL_Server**
  Detalhes: Verifica se está habilita a criptografia SSL no servidor. Uma ICP é utilizada para habilitar a criptografia por SSL no banco. Ela

deve ser armazenada e configurada nos parâmetros de inicialização do MySQL.
Controle medido: A6, A7, B1, B2, F5
Exemplo de saída: YES

- **Métrica: DBaaS_MySQL_Status**
  Detalhes: Informa os estado do banco com detalhes de performance. Essa métrica pode ser utilizada para verificar se alguma indisponibilidade ocorre por problemas de sobrecarga, em que a quantidade de consultas com lentidão seria alta ou tempo de resposta alto.
  Controle medido: I1
  Exemplo de saída: Threads: 1 Questions: 57030 Slow queries: 0 Opens: 99 Flush tables: 1 Open tables: 23 Queries per second avg: 0.63

- **Métrica: DBaaS_MYSQL_User**
  Detalhes: Lista os usuários do banco. Observe que existem somente dois usuários: o padrão administrativo (root) e o padrão para manutenção em sistemas GNU/Linux Ubuntu (debian-sys-maint). Para esse último usuário, a permissão de acesso só está permitida para o IP local que hospeda o SGBD.
  Controle medido: C1, C3, D2, D5, H3
  Exemplo de saída: root debian-sys-maint

- **Métrica: DBaaS_MySQL_Version**
  Detalhes: Informa a versão de SGBD MySQL sendo utilizada.
  Controle medido: A1, A2
  Exemplo de saída: 5.1.70-0ubuntu0.10.04.1 (Ubuntu)

- **Métrica: DBaaS_OS_Version**
  Detalhes: Informa a versão de sistema operacional sendo utilizada pela máquina virtual.
  Controle medido: A1, A2
  Exemplo de saída: DISTRIB_RELEASE=10.04

Além do MySQL, foi instalado em laboratório, o Oracle Database Express Edition 11g. Não foram feitas alterações nos parâmetros de inicialização do SGBD. Eles podem ser alterados através de comandos dados diretamente ao banco e, para consultar os seus valores, existem visões de tabelas de sistema (dicionário). Para o Oracle, foram geradas as métricas descritas abaixo:

- **Métrica: DBaaS_Ora_Audit**
  Detalhes: Através da visão v$parameter foi possível observar se as

trilhas de auditoria haviam sido ativadas.
Controle medido: E1, E2, E3
Exemplo de saída: audit_trail NONE

- **Métrica: DBaaS_Ora_Bkp**
  Detalhes: Oracle utiliza a ferramenta RMAN (*Recovery Manager*) para efetuar cópias de segurança. Ainda, existe uma visão de banco v$rman_status que permite observar históricos de procedimentos de backup.
  Controle medido: G1
  Exemplo de saída: 15-SEP-13 BACKUP FAILED

- **Métrica: DBaaS_Ora_Link**
  Detalhes: Verificar as ligações entre as bases. Para tanto existe a visão all_db_links além dos arquivos de configuração para rede listener.ora, sqlnet.ora e tnsnames.ora.
  Controle medido: D4, F2, F3,
  Exemplo de saída: Não foram configuradas ligações para outras bases em laboratório.

- **Métrica: DBaaS_Ora_Port**
  Detalhes: Através do arquivo de configuração listener.ora é possível obter informação da porta utilizada para conexão ao banco. Observa-se que a porta utilizada neste ambiente é a padrão.
  Controle medido: F1
  Exemplo de saída: PORT = 1521

- **Métrica: DBaaS_Ora_Privs**
  Detalhes: Consultando a visão dba_tab_privs pode-se obter o número de objetos com permissão de execução ou privilégios de manipulação de dados. Além desta, é possível observar o número de usuários que possuem permissões de sistema através da visão dba_sys_privs. Já a visão dba_role_privs informa quem possui privilégios de administrador da base.
  Controle medido: B9, D1 , D2, D3, F4
  Exemplo de saída: Exec: 73 DML: 7 Sys: 24 DBA: 18

- **Métrica: DBaaS_Ora_Options**
  Detalhes: Consulta à visão v$option informa para quais funcionalidades o SGDB foi compilado.
  Controle medido: A3
  Exemplo de saída: Objects, Connection multiplexing, Connection pooling, Database queuing, Incremental backup and recovery, Instead-of

triggers, Parallel load, Proxy authentication/authorization, Plan Stability, Transparent Application Failover, Sample Scan, OLAP Window Functions

- **Métrica: DBaaS_Ora_SLA**
  Detalhes: Essa métrica foi obtida através da visão v$instance.
  Controle medido: I1
  Exemplo de saída: version: 11.2.0.2.0 startup_time: 15-sep-13 instance_name: xe status: open

- **Métrica: DBaaS_Ora_SSL_Client**
  Detalhes: Configurações de uso de criptografia para conexões com o banco é feita através do arquivo sqlnet.ora. Nele é possível verificar que o valor padrão para o parâmetro ssl_client_authentication é TRUE
  Controle medido: B1, B2, F5
  Exemplo de saída: ssl_client_authentication=TRUE

- **Métrica: DBaaS_Ora_TabExt**
  Detalhes: É possível obter informações de uso de tabelas externas através da visão all_external_tables.
  Controle medido: B8
  Exemplo de saída: Não foram criadas tabelas externas no ambiente de laboratório.

- **Métrica: DBaaS_Ora_User**
  Detalhes: Lista os usuários do banco. Observe que os usuários sys e system são usuários administrativos padrão do banco. Ainda, hr é um usuário para aplicações de exemplo.
  Controle medido: C1, C3, D2, D5, H3, H4
  Exemplo de saída: anonymous apex_040000 apex_public_user ctxsys flows_files hr mdsys outln sys system xdb xs$null

- **Métrica: DBaaS_Ora_Version**
  Detalhes: A visão v$instance pode trazer informação da versão de banco e a dba_registry_history histórico de atualizações.
  Controle medido: A1, A2
  Exemplo de saída: 11.2.0.2.0

4.3 ANÁLISE DE VULNERABILIDADES

Além de possibilitar a averiguação dos contratos de serviço de provedores, os controles internos gerados para este trabalho puderam examinar se em um DBaaS existe um nível de segurança aceitável.

Entretanto, sob ponto de vista de auditoria, pode-se valer de uma ferramenta para análise de vulnerabilidades.

O ambiente de nuvem pública escolhido para os testes de invasão e vulnerabilidades foi o Amazon Relation Database Service (RDS) com o MySQL.

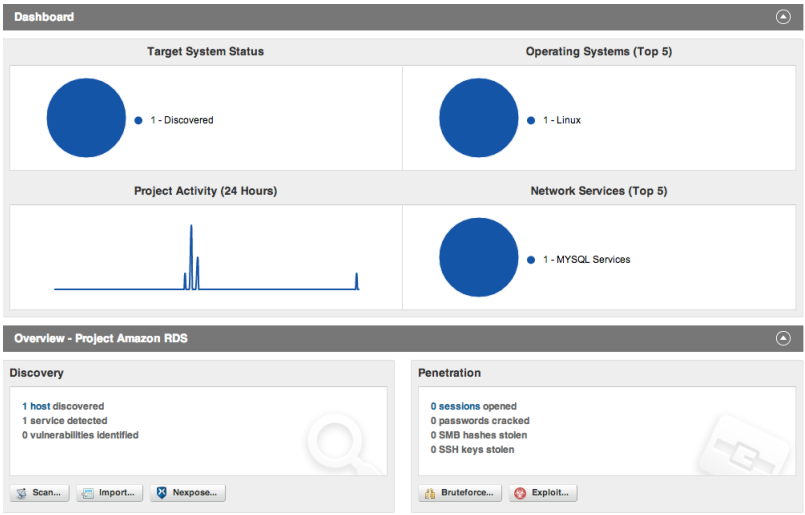


Figura 9 – Visão sobre análise do DBaaS pelo Metasploit

Mestasploit (KENNEDY et al., 2011) foi a ferramenta escolhida para explorar vulnerabilidades. Desenvolvida pela empresa Rapid7, possui versões para desenvolvedores, estudantes, pequenas e médias empresas. A versão utilizada foi a Metasploit Pro com direito de uso para testes por 7 dias. Após uma varredura no ambiente, forneceu informações sobre os equipamentos descobertos, serviços, vulnerabilidades, dados capturados e topologia da rede.

Após a varredura inicial, o Metasploit identificou que o sistema operacional executado no ambiente de nuvem é o Linux e apenas um serviço disponível, o MySQL, como se pode ver na figura 9. Os seguintes testes foram aplicados:

- Força bruta: Conforme especificado nos controles C1, C3, D2 e D5 do apêndice A, foi possível listar os seguintes usuários de banco de dados: inemaster (criado para uso do serviço de nuvem) e rdsadmin (para uso restrito do Amazon RDS com permissão de acesso somente para o IP

local que hospeda o SGBD). Nenhum desses usuários é padrão para o SGBD, como se observou na especificação da métrica DBaaS_MYSQL_User, na seção 4.2. Assim, um teste de força bruta não se torna efetivo, pois o usuário de conexão não é conhecido pela ferramenta. Além disso, a versão de banco testada possui um parâmetro que só pode ser alterado por superusuários, o max_connect_errors com valor igual a 10. Após 10 tentativas de acesso com falha, o servidor bloqueia o acesso para o IP de origem. O usuário inemaster não é superusuário, logo não tem permissão para alterar o parâmetro.

- Explorar vulnerabilidades: A métrica DBaaS_MYSQL_Version, na seção 4.2 e também os controles A1 e A2 do apêndice A, trazem informações sobre a versão de banco. Essa foi mostrada na seção 4.1.1 como sendo 5.5.31. O Metasploit obteve essa informação e identificou seis prováveis vulnerabilidades, sendo todas elas relativas a acesso de usuários remotos autenticados. Confira, conforme *Common Vulnerabilities and Exposures (CVE)*, as seguintes: CVE-2013-3783, CVE-2013-3793, CVE-2013-3802, CVE-2013-3804, CVE-2013-3809 e CVE-2013-3812. Apesar disso, a ferramenta, sem conhecimento de usuários do banco, não conseguiu explorar nenhuma das vulnerabilidades. Conforme proposto no controle A1, em que se diz para identificar e aplicar correções conhecidas e reportadas para vulnerabilidades, dando a ele prioridade alta e incluído em todas as fases de ciclo de vida de um projeto, cabe ao cliente fazer essa verificação. Neste caso do Amazon RDS, existe a possibilidade de o cliente fazer um upgrade para a versão 5.5.33 do MySQL que não possui vulnerabilidades conhecidas até o momento. Assim, reforça-se que a aplicação periódica de controles internos em cada fase do projeto é vital para a garantia da segurança em DBaaS.

4.4 DISCUSSÃO SOBRE RESULTADOS

Neste trabalho foi proposto a criação de um *framework* de controles internos capaz de auxiliar a clientes na escolha de um serviço de banco de dados em nuvem com segurança necessária para os seus negócios organizacionais. Esse *framework* provê maior direção na análise de contratos de serviço (SLA) e ainda dá suporte para fiscalização do contrato celebrado entre clientes e provedores. Ele foi divido em 9 famílias ou domínios de controle: 1. Planejamento e Avaliação de Risco; 2. Segurança de Sistema Operacional e Ambiente de Virtualização; 3. Autenticação e Autorização; 4. Controle de Acessos; 5. Auditoria; 6. Camada de Rede; 7. Disponibilidade, Cópia de

Segurança e Recuperação 8. Desenvolvimento e Servidores de Aplicação e 9. Contratos e Comprometimento. Para que a segurança seja mantida ao longo do tempo, são propostos períodos em que esses controles devem ser avaliados.

Ambientes de nuvem pública foram avaliados tendo como base nas famílias de controles, mostradas no apêndice A. Amazon Relation Database Service teve a maior quantidade de controles positivamente verificados. Em seguida vem Oracle Database Cloud e Microsoft Azure SQL. Apesar dessa averiguação, as diferenças são pequenas e todos possuem boa segurança. A qualidade do serviço está relacionada com as práticas de segurança adotadas pelos SGBDs, mesmo estando em ambientes fora da nuvem. A escolha de um cliente deve levar em conta os requisitos de seu negócio, sobre quais controles dará prioridade e quais deles são cobertos pelos provedores. Uma análise de vulnerabilidades mostrou que um dos serviços de banco de dados em nuvem está bem dimensionado em termos de segurança obtida através dos controles.

Além disso, um ambiente de nuvem privada foi elaborado e algumas métricas foram descritas como formas de validação de entrega de serviços. Através de ferramentas, é possível fazer a fiscalização contínua dos serviços de banco de dados em nuvem como, por exemplo, disponibilidade para os termos de SLA ou se os canais usados nas comunicações são criptografados.

5 CONCLUSÕES E TRABALHOS FUTUROS

5.1 CONCLUSÕES

Este trabalho sobre segurança de banco de dados em nuvem apresentou a construção de um *framework* conceitual (semelhantemente ao COBIT) baseado em famílias de controles internos que dá suporte para análise de contratos de serviços seguindo a definição de SLA. A pesquisa focou-se no modelo DBaaS, que é uma especialização de serviço em nuvem.

Os controles internos definidos foram implantados em ambientes de testes de nuvens públicas e privadas. No ambiente de nuvem pública foram considerados os provedores Amazon (MySQL), Microsoft (SQL Server) e Oracle (Oracle Database). Na nuvem privada foram abordados os SGBDs MySQL e Oracle Database.

Como principais conclusões e contribuições, pode-se citar que um *framework* de controles internos:

- É adequado para averiguar a segurança da informação em banco de dados em nuvem: estudos de caso e análise de vulnerabilidades foram empregados para verificação da segurança;
- É apropriado para fiscalizar níveis e contratos de serviços: existem controles específicos para análise de contratos e níveis de serviços;
- Dá suporte para a criação de métricas para monitoramento de serviços: através de controles, é possível que alguns possam ser quantificados e usados como métricas para ferramentas;
- Pode ser integrado aos contratos de serviços para dar mais transparência às entregas de serviços: os controles podem ser usados para verificar se algumas cláusulas ou itens de contrato não foram especificados apropriadamente;
- Ajuda a direcionar a escolha de provedores de serviços, pois permite melhor avaliação dos níveis de serviço após a aplicação dos controles.

Foram efetuados estudos de caso para averiguar esses controles e uma análise de vulnerabilidades para verificar a segurança requisitada pelos controles.

Este trabalho limitou-se ao uso de DBaaS em ambiente de laboratório para apenas bancos de dados relacionais.

5.2 TRABALHOS FUTUROS

Como trabalhos futuros, propõe-se:

- Uso do *framework* em ambientes corporativos;
- Melhor ajuste da prioridade e das fases em que os controles devem ser aplicados, baseando-se em experiências reais;
- Uso do *framework* para bancos de dados objeto-relacionais como, por exemplo, PostgreSQL.

REFERÊNCIAS

ABADI, D. Data management in the cloud: Limitations and opportunities. **IEEE Data Eng. Bull**, v. 32, n. 1, p. 3–12, 2009.

AGRAWAL, D. et al. Database management as a service: Challenges and opportunities. In: IEEE. **Data Engineering, 2009. ICDE'09. IEEE 25th International Conference on**. [S.l.], 2009. p. 1709–1716.

ALLIANCE, C. S. **Cloud Controls Matrix (CCM)**. April 2010. Disponível em: <https://cloudsecurityalliance.org/research/ccm/>. Acesso em: 27-09-2013.

AMAZON. **Amazon Elastic Block Store (EBS)**. November 2012. Disponível em: <http://aws.amazon.com/ebs/>. Acesso em: 12-11-2012.

AMAZON. **Amazon Elastic Compute Cloud (Amazon EC2)**. November 2012. Disponível em: <http://aws.amazon.com/ec2/>. Acesso em: 12-11-2012.

AMAZON. **Amazon Relational Database Service (Amazon RDS)**. November 2012. Disponível em: <http://aws.amazon.com/rds/>. Acesso em: 12-11-2012.

AMAZON. **Amazon Simple Storage Service (Amazon S3)**. November 2012. Disponível em: <http://aws.amazon.com/s3/>. Acesso em: 12-11-2012.

AMAZON. **Amazon DynamoDB**. February 2013. Disponível em: <http://aws.amazon.com/dynamodb/>. Acesso em: 11-02-2013.

AMAZON. **Amazon Web Services (Overview of Security Processes)**. [S.l.], June 2013. 48 p. Disponível em: <http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf>. Acesso em: 12-06-2013.

ANSTETT, T. et al. Towards bpel in the cloud: Exploiting different delivery models for the execution of business processes. In: IEEE. **Services-I, 2009 World Conference on**. [S.l.], 2009. p. 670–677.

ARMBRUST, M. et al. A view of cloud computing. **Commun. ACM**, ACM, New York, NY, USA, v. 53, n. 4, p. 50–58, abr. 2010. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/1721654.1721672>.

AVIZIENIS, A. et al. Fundamental concepts of dependability. **Technical Report Series-University Of Newcastle Upon Tyne Computing Science**, UNIVERSITY OF NEWCASTLE UPON TYNE, 2001.

BERTINO, E.; SANDHU, R. Database security-concepts, approaches, and challenges. **Dependable and Secure Computing, IEEE Transactions on**, IEEE, v. 2, n. 1, p. 2–19, 2005.

BRANTNER, M. et al. Building a database on s3. In: **Proceedings of the 2008 ACM SIGMOD international conference on Management of data**. New York, NY, USA: ACM, 2008. (SIGMOD '08), p. 251–264. ISBN 978-1-60558-102-6. Disponível em: <http://doi.acm.org/10.1145/1376616.1376645>.

BRODKIN, J. **Gartner: Seven cloud-computing security risks**. [S.l.], 2008. 1–3 p. Disponível em: <http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853>. Acesso em: 20-11-2012.

BRUNETTE, G.; MOGULL, R. Security guidance for critical areas of focus in cloud computing v2. 1. **Cloud Security Alliance**, p. 1–76, 2009.

BUTLER, B. Gartner's state of cloud security: Outages are bigger risk than breaches. **Network World**, p. 1–2, 2012. Disponível em: <https://www.networkworld.com/news/2012/111412-gartner-cloud-security-264268.html>.

CALDER, B. et al. Windows azure storage: a highly available cloud storage service with strong consistency. In: **Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles**. New York, NY, USA: ACM, 2011. (SOSP '11), p. 143–157. ISBN 978-1-4503-0977-6. Disponível em: <http://doi.acm.org/10.1145/2043556.2043571>.

CAMPBELL, D. G.; KAKIVAYA, G.; ELLIS, N. Extreme scale with full sql language support in microsoft sql azure. In: **Proceedings of the 2010 ACM SIGMOD International Conference on Management of data**. New York, NY, USA: ACM, 2010. (SIGMOD '10), p. 1021–1024. ISBN 978-1-4503-0032-2. Disponível em: <http://doi.acm.org/10.1145/1807167.1807280>.

CARROLL, M.; MERWE, A. van der; KOTZE, P. Secure cloud computing: Benefits, risks and controls. In: **Information Security South Africa (ISSA), 2011**. [S.l.: s.n.], 2011. p. 1 –9.

CHAVES, S. **Arquitetura e sistema de monitoramento para computação em nuvem privada**. Dissertação (Mestrado) — Programa de Pós-Graduação em Ciência da Computação, Centro Tecnológico, UFSC, 2010.

CHOW, R. et al. Controlling data in the cloud: outsourcing computation without outsourcing control. In: **Proceedings of the 2009 ACM workshop on Cloud computing security**. New York, NY, USA: ACM, 2009. (CCSW '09), p. 85–90. ISBN 978-1-60558-784-4. Disponível em: <http://doi.acm.org/10.1145/1655008.1655020>.

COOPER, B. F. et al. Pnuts: Yahoo!'s hosted data serving platform. **Proceedings of the VLDB Endowment**, VLDB Endowment, v. 1, n. 2, p. 1277–1288, 2008.

CURINO, C. et al. Relational cloud: A database-as-a-service for the cloud. **5th Biennial Conference on Innovative Data Systems Research, CIDR 2011**, January 2011.

FERRARI, E. Database as a service: Challenges and solutions for privacy and security. In: **Services Computing Conference, 2009. APSCC 2009. IEEE Asia-Pacific**. [S.l.: s.n.], 2009. p. 46 –51.

FINNIGAN, P. **Oracle Database checklist**. [S.l.], 2004.

FOSTER, I. et al. Cloud computing and grid computing 360-degree compared. In: **Grid Computing Environments Workshop, 2008. GCE '08**. [S.l.: s.n.], 2008. p. 1 –10.

FOX, A. et al. Cluster-based scalable network services. **SIGOPS Oper. Syst. Rev.**, ACM, New York, NY, USA, v. 31, n. 5, p. 78–91, out. 1997. ISSN 0163-5980. Disponível em: <http://doi.acm.org/10.1145/269005.266662>.

FRANK, L. Countermeasures against consistency anomalies in distributed integrated databases with relaxed acid properties. In: **Innovations in Information Technology (IIT), 2011 International Conference on**. [S.l.: s.n.], 2011. p. 266 –270.

GILBERT, S.; LYNCH, N. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. **SIGACT News**, ACM, New York, NY, USA, v. 33, n. 2, p. 51–59, jun. 2002. ISSN 0163-5700. Disponível em: <http://doi.acm.org/10.1145/564585.564601>.

GOOGLE. **Google Cloud Platform**. February 2013. Disponível em: <https://cloud.google.com/>. Acesso em: 10-02-2013.

GREENWALD, R. **Oracle Database and the Oracle Database Cloud**. [S.l.], September 2012. 8 p.

HACIGUMUS, H.; IYER, B.; MEHROTRA, S. Providing database as a service. In: **Data Engineering, 2002. Proceedings. 18th International Conference on**. [S.l.: s.n.], 2002. p. 29 –38. ISSN 1063-6382.

ITGI. **COBIT 4.1 Excerpt**. [S.l.], 2007. 31 p. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf>. Acesso em: 07-06-2013.

KANDUKURI, B.; PATURI, V.; RAKSHIT, A. Cloud security issues. In: **Services Computing, 2009. SCC '09. IEEE International Conference on**. [S.l.: s.n.], 2009. p. 517–520.

KAUFMAN, C.; VENKATAPATHY, R. **Windows Azure Security Overview**. [S.l.], August 2010. 24 p. Disponível em: <http://go.microsoft.com/?linkid=9740388&clcid=0x409>. Acesso em: 27-05-2013.

KENNEDY, D. et al. **Metasploit: The Penetration Tester's Guide**. [S.l.]: No Starch Press, 2011.

KRASKA, T. **Building Database Applications in the Cloud**. ETH, 2010. Disponível em: <http://books.google.com.br/books?id=PXa9XwAACAAJ>.

LEITNER, P. et al. Monitoring, prediction and prevention of sla violations in composite services. In: IEEE. **Web Services (ICWS), 2010 IEEE International Conference on**. [S.l.], 2010. p. 369–376.

MEIER, J. D.; ENFIELD, P. **Windows Azure Security Notes**. [S.l.], 2010. 121 p. Disponível em: <http://go.microsoft.com/?linkid=9741707&clcid=0x409>. Acesso em: 27-05-2013.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing**. [S.l.], September 2011. 7 p. Disponível em: <http://csrc.nist.gov/publications/PubsSPs.html>. Acesso em: 05-06-2013.

NATAN, R. B. **Implementing Database Security and Auditing**. [S.l.]: Digital Press, 2005.

NIST. **Recommended Security Controls for Federal Information Systems and Organizations**. [S.l.], August 2009. 7 p. Disponível em: <http://csrc.nist.gov/publications/PubsSPs.html>. Acesso em: 06-06-2013.

NWAFOR, C. I. et al. A cobit and nist-based conceptual framework for enterprise user account lifecycle management. In: IEEE. **Internet Security (WorldCIS), 2012 World Congress on**. [S.l.], 2012. p. 150–157.

ORACLE. **Oracle Database Security Checklist**. [S.l.], June 2008. 16 p.

ORACLE. **Oracle Database Cloud Service security lockdown**. [S.l.], August 2012. 9 p.

ORACLE. **Oracle Cloud Enterprise Hosting and Delivery Policies**. [S.l.], June 2013. 17 p. Disponível em: <http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>. Acesso em: 07-06-2013.

PAL, D. G. et al. A novel open security framework for cloud computing. **International Journal of Cloud Computing and Services Science (IJ-CLOSER)**, v. 1, n. 2, p. 45–52, 2012.

RAMAKRISHNAN, R.; GEHRKE, J. **Database management systems**. [S.l.]: McGraw-Hill, 2003.

RIDLEY, G.; YOUNG, J.; CARROLL, P. Cobit and its utilization: a framework from the literature. In: **System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on**. [S.l.: s.n.], 2004. p. 8 pp.–.

SAKR, S. et al. Clouddb autoadmin: Towards a truly elastic cloud-based data store. In: IEEE. **Web Services (ICWS), 2011 IEEE International Conference on**. [S.l.], 2011. p. 732–733.

SANDHU, R.; SAMARATI, P. Access control: principle and practice. **Communications Magazine, IEEE**, v. 32, n. 9, p. 40–48, 1994. ISSN 0163-6804.

SHIM, S. S. Guest editor's introduction: The cap theorem's growing impact. **Computer**, IEEE Computer Society, Los Alamitos, CA, USA, v. 45, n. 2, p. 21–22, 2012. ISSN 0018-9162.

SILBERSTEIN, A. et al. Pnuts in flight: Web-scale data serving at yahoo. **Internet Computing, IEEE**, v. 16, n. 1, p. 13–23, 2012. ISSN 1089-7801.

SOUSA, F. R.; MACHADO, J. C. Towards elastic multi-tenant database replication with quality of service. In: IEEE COMPUTER SOCIETY. **Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing**. [S.l.], 2012. p. 168–175.

VENGURLEKAR, N. **Security in Private Database Clouds**. [S.l.], July 2012. 14 p.

VOGELS, W. Eventually consistent. **Commun. ACM**, ACM, New York, NY, USA, v. 52, n. 1, p. 40–44, jan. 2009. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/1435417.1435432>.

WANG, C. et al. Toward publicly auditable secure cloud data storage services. **Network, IEEE**, v. 24, n. 4, p. 19 –24, july-august 2010. ISSN 0890-8044.

WANG, C. et al. Toward secure and dependable storage services in cloud computing. **Services Computing, IEEE Transactions on**, v. 5, n. 2, p. 220 –232, april-june 2012. ISSN 1939-1374.

WANG, Q. et al. Enabling public auditability and data dynamics for storage security in cloud computing. **Parallel and Distributed Systems, IEEE Transactions on**, v. 22, n. 5, p. 847 –859, may 2011. ISSN 1045-9219.

WEBER, T. Um roteiro para exploração dos conceitos básicos de tolerância a falhas. **Relatório técnico, Instituto de Informática UFRGS**, 2002.

WEIS, J.; ALVES-FOSS, J. Securing database as a service: Issues and compromises. **Security & Privacy, IEEE**, IEEE, v. 9, n. 6, p. 49–55, 2011.

WIESMANN, M. et al. Understanding replication in databases and distributed systems. In: **Distributed Computing Systems, 2000. Proceedings. 20th International Conference on**. [S.l.: s.n.], 2000. p. 464 –474. ISSN 1063-6927.

YAHOO! **PNUTS - Platform for Nimble Universal Table Storage**. Maio 2013. Disponível em: <http://research.yahoo.com/project/212>. Acesso em: 15-05-2013.

ZHAO, L.; SAKR, S.; LIU, A. Application-managed replication controller for cloud-hosted databases. In: IEEE. **Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on**. [S.l.], 2012. p. 922–929.

ZHAO, L.; SAKR, S.; LIU, A. A framework for consumer-centric sla management of cloud-hosted databases. IEEE, 2013.

APÊNDICE A – Famílias de Controles

A.1 TABELAS DE FAMÍLIAS DE CONTROLES

Os controles foram esquematicamente subdivididos em famílias ou domínios. Para facilitar a visualização foram colocados em tabelas, conforme segue abaixo.

Tabela 4: Planejamento e Avaliação de Risco

Planejamento e Avaliação de Risco	
Controle	**Especificação**
A1	Identificar e aplicar correções conhecidas e reportadas para vulnerabilidades
A2	Identificar e gravar versões de software (banco de dados, sistema operacional e aplicações) e de pacotes de correções no sistema
A3	Utilizar somente as funcionalidades necessárias
A4	Rever procedimentos e políticas de segurança
A5	Verificar localização física dos servidores e conformidade com o Teorema CDP
A6	Definir arquitetura de acesso da aplicação
A7	Infraestrutura de Chave Pública (ICP)
A8	Gerenciamento de Incidentes

Tabela 5: Segurança de Sistema Operacional e Ambiente de Virtualização

Segurança de Sistema Operacional e Ambiente de Virtualização	
Controle	**Especificação**
B1	Segurança e criptografia nas conexões de rede
B2	Troca segura de senhas entre servidores e clientes
B3	Auditoria nas máquinas clientes para evitar arquivos de configuração com usuários e senhas
B4	Detecção e prevenção de intrusos
B5	Assegurar privilégios mínimos de conexão
B6	Auditoria sobre arquivos de exportação e de registros de alteração da base

Continua na página seguinte

Tabela 5 – *Continuação da página anterior*

Controle	Especificação
B7	Troca de senhas após importação de dados
B8	Auditoria sobre tabelas externas
B9	Restringir acesso para compilação de código no banco
B10	Firewall e antivírus
B11	Virtual Private Network (VPN)

Tabela 6: Autenticação e Autorização

Autenticação e Autorização	
Controle	**Especificação**
C1	Auditoria de usuários ativos da base e de usuários de aplicação
C2	Auditoria de senhas da base
C3	Auditoria de contas padrão
C4	Incluir gerenciamento de senhas para contas por padrão
C5	Alterar senhas de usuários privilegiados de sistema
C6	Inclusão de senhas para todos os componentes da base

Tabela 7: Controle de Acessos

Controle de Acessos	
Controle	**Especificação**
D1	Segurança granular: verificação de acessos a partes de tabelas, visões, parte de procedimentos e funções
D2	Checar usuários com permissão de operação e administração da base
D3	Revisar permissões de sistema garantida a usuários
D4	Verificar acessos através de ligações permitidas entre bases
D5	Controle de usuários, papéis e gerenciamento de identidade
D6	Classificação de dados

Tabela 8: Auditoria

Auditoria	
Controle	**Especificação**
E1	Configurar auditoria
E2	Auditoria em falhas de inserção em objetos
E3	Auditoria de acesso à base

Tabela 9: Camada de Rede

Camada de Rede	
Controle	**Especificação**
F1	Não utilizar portas padrão para conexão
F2	Segurança do servidor de conexão e ligações entre bases
F3	Auditoria e criação de políticas para definir ligações entre bases
F4	Usuários de conexões entre bases não pode ser usuário privilegiado
F5	Transferência de dados com criptografia entre servidores e clientes

Tabela 10: Disponibilidade, Cópia de Segurança e Recuperação

Disponibilidade, Cópia de Segurança e Recuperação	
Controle	**Especificação**
G1	Revisar e documentar procedimentos de backup e recuperação
G2	Armazenamento de mídias em localização distinta
G3	Validar mídias de backup regularmente
G4	Validar procedimentos de recuperação regularmente
G5	Documentar e rever procedimentos de recuperação de desastre

Tabela 11: Desenvolvimento e Servidores de Aplicação

Desenvolvimento e Servidores de Aplicação	
Controle	**Especificação**
H1	Ambiente de produção isolado e sem acesso para desenvolvedores
H2	Procedimentos de replicação de ambientes
H3	Segurança de usuários de portal na base
H4	Remover programas e dados de exemplo de portal e base
H5	Controle de vulnerabilidades: injeção de código e SQL, DoS e DDoS, cross-site script

Tabela 12: Contratos e Comprometimento

Contratos e Comprometimento	
Controle	**Especificação**
I1	Documentar, verificar e fiscalizar periodicamente os níveis de serviço contratados
I2	Fiscalizar e avaliar serviços de suporte
I3	Verificar e avaliar ferramentas de monitoramento e geração de relatórios
I4	Verificar documentação para treinamento interno de equipes
I5	Suporte à investigação
I6	Conformidade com legislações e regulamentações
I7	Término contratual, migração e eliminação de dados