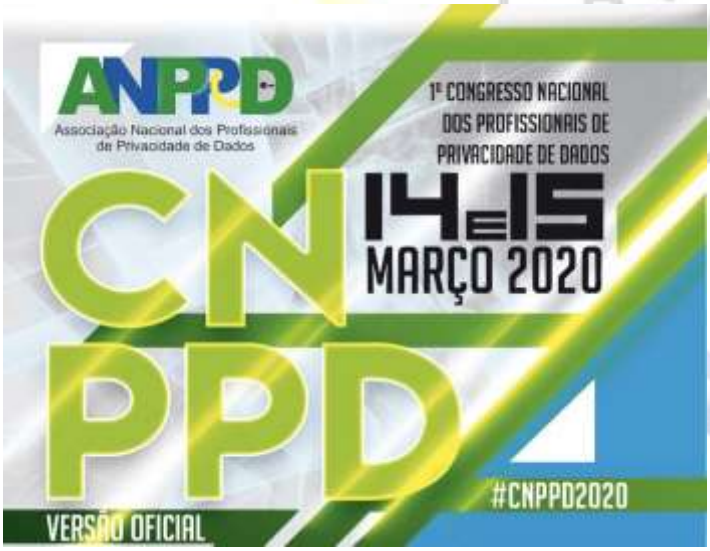
ARTIGO TÉCNICO

As “NUVENS PÚBLICAS” atendem à legislação brasileira (LGPD) sobre armazenamento de dados?

Resumo

O propósito deste artigo é avaliar de forma objetiva os principais requisitos da legislação brasileira sobre o uso de serviços em nuvem, a luz das principais leis e normativas que regem aspectos tanto do armazenamento de dados quanto as instruções que orientam quanto aos modelos de aquisição e requisitos de segurança. Apesar da Instrução Normativa Nº01 e a Norma Complementar Nº14 serem pertinentes a administração pública, as orientações da LGPD se aplicam a todas as empresas.

Palavras-chave: Nuvem, Armazenamento, LGPD, Legislação



Índice

Introdução

Vários órgãos governamentais se movimentaram fortemente na direção da contratação de serviços em nuvem em 2019. Nos últimos 2 anos vimos os primeiros ensaios governamentais através de consultas públicas e finalmente os editais do TCU e do extinto MPOG, hoje Ministério da Economia, que adotaram modelos de catálogo de serviços pagos por USN (Unidades de Serviço de Nuvem) e UST (Unidades de Serviço Técnico).

Esses movimentos são louváveis e as recentes atualizações da legislação brasileira foram muito bem estabelecidas. Decidimos avaliar as contratações públicas à luz da Instrução Normativa Nº 1 (IN01), da Norma Complementar NC 14 e da LGPD. E não só as contratações de nuvens públicas, mas também as aquisições de Storage em curso.

Dessas legislações vigentes criamos uma matriz para avaliar 4 principais aspectos nas 3 principais nuvens públicas, avaliando também a aquisição de Storage (de forma geral) e o uso de uma solução de Storage como serviço (STaaS Zadara), solução disponível nos Marketplaces das próprias nuvens públicas acima.

Aspectos avaliados:

- A recomendação da IN01 por contratação de serviços de computação em nuvem (pública ou privada);
- A exigência da IN01 para que estas soluções possuam certificações de normas de segurança da informação;
- A análise comparativa de custos (TCO), considerando ciclo de vida dos bens e serviços, garantia, manutenção, etc.
- A recomendação de uso da nuvem pública conforme a classificação das informações.

COMPLIANCE DE ARMAZENAMENTO DE DADOS CONFORME LEGISLAÇÃO BRASILEIRA								
RESUMO IN01 e NC14				AWS	AZURE	GOOGLE	AQUISIÇÃO	ZADARA
Instrução Normativa Nº 1 (IN01), de 04 de ABRIL de 2019	[...]por meio da contratação de serviços de computação em nuvem,[...]	Serviços sob demanda, As a Service em **Nuvem Pública**	Object Storage (Armazenamento de **Objetos**)	OK	OK	OK	NOK	OK
			Block Storage (Armazenamento de **Volumes/Discos**)	OK	OK	OK	NOK	OK
			File Storage (Armazenamento de **Arquivos**)	OK	OK	OK	NOK	OK
		Serviços sob demanda, As a Service **On Premise (local)**	Object Storage (Armazenamento de **Objetos**)	NOK	NOK	NOK	NOK	OK
			Block Storage (Armazenamento de **Volumes/Discos**)	NOK	NOK	NOK	NOK	OK
			File Storage (Armazenamento de Arquivos)	NOK	NOK	NOK	NOK	OK
	[...] possuam **certificações de normas de segurança da informação** aplicáveis ao objeto da contratação, [...]	**ISO 27.001**		OK	OK	OK	OK	OK
		ISO 27.017		OK	OK	OK	NOK	OK
		ISO 27.018		OK	OK	OK	NOK	OK
		LGPD (GDPR)	Saber exatamente **onde** os dados estão armazenados **fisicamente** (discos)	NOK	NOK	NOK	OK	OK
			Possibilidade de esquecimento, **eliminação completa** dos dados.	NOK	NOK	NOK	OK	OK
			Possibilidade de **isolamento** e **entrega dos dados**/discos para autoridades competentes	NOK	NOK	NOK	OK	OK
			Atendimento Básico e demais itens	OK	OK	OK	OK	OK
	A análise comparativa de custos deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo: a) comparação de custos totais de propriedade (**Total Cost Ownership - TCO**) por meio da obtenção dos **custos inerentes ao ciclo de vida dos bens e serviços** de cada solução, a exemplo dos valores de **aquisição** dos ativos, insumos, **garantia**, **manutenção**; [...]			OK	OK	OK	NOK	OK
Norma Complementar NC14/ IN01/ DSIC/ GSIPR, de 19 de MARÇO de 2018	**Informação sem restrição de acesso**			OK	OK	OK	OK	OK
	Informação sigilosa			NOK	NOK	NOK	OK	OK
	Informação classificada			NOK	NOK	NOK	OK	OK
	Informação com restrição de acesso prevista em legislação vigente			OK	OK	OK	OK	OK
	Documento Preparatório			OK	OK	OK	OK	OK

LEGENDA	DESCRIÇÃO
OK	**Atende o requisito**
NOK	**Não atende o requisito**

O primeiro ponto que chama a atenção é o modelo de aquisição de storage, que apesar de poder atender aos requisitos da LGPD e da NC 14, não atende à orientação da IN01 relativa à contratação como serviço. E muitos órgãos ainda seguem este modelo de aquisição de hardware, que exige alto investimento de aquisição, mas péssima análise de TCO. O custo de aquisição é altíssimo por um volume que muitas vezes só é alocado anos depois e não consideram o End of Life dos produtos, os custos de garantia, manutenções, atualizações de firmware e depreciação de ativos.

*"**4.1.** Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados **deverão fazê-lo por meio da contratação de serviços de computação em nuvem**, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação.*

Subseção II – Art. 11.

a) *comparação de **custos totais de propriedade** (Total Cost Ownership – TCO) por meio da obtenção dos **custos inerentes ao ciclo de vida dos bens e serviços de cada solução**, a exemplo dos valores de **aquisição** dos **ativos, insumos, garantia e manutenção**.*

O segundo ponto a se destacar é que as 3 principais nuvens públicas não atendem, pelo menos ainda, a possibilidade de serviços locais, on premise. Isto não chega a ser um problema, mas é um entrave para muitos órgãos que têm esta necessidade de storage local, pois precisam atender o que pede a NC 14 sobre a restrição de uso de nuvem pública para informações sigilosas ou classificadas.

> *"5.2 Sobre o tratamento da informação:*
> *[...]*
>
> *5.2.2 **Informação sigilosa:** como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:*
> *5.2.2.1. **Informação classificada:** é vedado o tratamento em ambiente de computação em nuvem;*
>
> *[...]*
> *5.2.2.2. Conhecimento e informação contida em **material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem**;*
>
> *5.2.2.3. Informação com restrição de acesso prevista em legislação vigente: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade (DICA);*
>
> *5.2.2.4. Documento Preparatório: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA;*
>
> *5.2.2.5. Documento preparatório que possa originar informação classificada deve ser tratado conforme o item 5.2.2.1; e 5.2.2.6. Informação pessoal relativa à intimidade, vida privada e imagem: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA."*

Mas o terceiro ponto é o mais crítico: as nuvens públicas não atendem integralmente à LGPD. Nelas não é possível saber exatamente onde estão armazenados os dados. Não é possível apontar fisicamente os discos, dada a arquitetura disponibilizada. Também não é possível garantir a total eliminação dos dados através da plena formatação dos discos. Por último, não é possível isolar dados no caso de intervenção/auditoria de autoridade competente, não é possível isolar e entregar os discos a autoridade. As nuvens também não atendem à restrição da NC 14 quanto às informações sigilosas e classificadas.

*"XIII – **bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;*

*XIV – **eliminação**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;* "

A exigência de bloqueio mediante a guarda do dado pessoal ou do banco de dados é possível mediante a possibilidade de isolamento completo do dado, ou seja, sem nenhum tipo de acesso físico ou lógico durante o período do bloqueio.

Da mesma forma a lei exige a eliminação através da exclusão definitiva dos dados pessoais.

A LGPD é reiteradamente clara em relação a estas duas exigências, conforme os demais destaques abaixo reproduzidos.

"*Capítulo VIII DA FISCALIZAÇÃO – Seção I – Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:*

[...]

*V – **bloqueio** dos dados pessoais a que se refere a infração até a sua regularização;*

*VI **– eliminação** dos dados pessoais a que se refere a infração;"*

[...]

*"Art. 6º – I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, **sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;** "*

[...]

***"Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento**, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:* "

[...]

*"CAPÍTULO III – DOS DIREITOS DO TITULAR. VI – **eliminação dos dados pessoais** tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;"*

"CAPÍTULO X – DISPOSIÇÕES FINAIS E TRANSITÓRIAS – Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

*"Art. 7º – X – **exclusão definitiva dos dados pessoais** que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas*

as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;"

Devido a este terceiro ponto, muitos órgãos acabam acreditando ser necessário a aquisição de storage local, on premise, mas que como já reportamos, não atende adequadamente aspectos de consumo sob demanda da IN01 e análise comparativa de custos (TCO).

Por último, testamos a solução de Storage como Serviço da Zadara, disponível através dos Marketplaces das nuvens públicas e através de contratação direta. Em nossos testes, o storage Zadara foi utilizado em conjunto com as nuvens, ou seja, toda a parte de processamento, de servidores, foi usada das nuvens e toda a parte de armazenamento foi utilizada a solução Zadara.

Através da Zadara foi possível usar armazenamento de blocos/volumes, de objetos e de arquivos, de forma totalmente integrada com as nuvens ou com soluções locais de servidores. Totalmente sob demanda, paga como serviço por hora. Diferentemente da AWS, AZURE ou GOOGLE, a Zadara isola os discos para o cliente na tecnologia patenteada chamada VPSA (Virtual Private Storage Array) e ainda permite que seja implementada chave de criptografia de uso exclusivo e não compartilhado com o provedor.

O Storage da Zadara está disponível para uso tanto nas principais regiões das nuvens públicas, como localmente. É possível ter o armazenamento sob demanda dentro do seu datacenter, configurando como desejar a quantidade e tipo de discos, criando tenants com criptografia específica, configurando a quantidade de processadores, de memória, de cache e até permite rodar Docker dentro do storage.

Considerações finais

Se usadas como solução única, as nuvens públicas atendem parcialmente os requisitos. Todavia, no cenário híbrido testado, em conjunto com solução de storage como serviço disponível no próprio Marketplace dos 3 principais provedores (AWS, Azure e Google), foi possível atender integralmente todos os requisitos da legislação considerada: Instrução Normativa Nº01, Norma Complementar Nº14 e Lei Nº 13.709/2018 (LGPD).

Referências

LEI Nº13.709, DE 14 DE AGOSTO DE 2018. **Diário Oficial da União.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 07 de jan. de 2020.

INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019. **Diário Oficial da União.** Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535>. Acesso em: 07 de jan. de 2020.

NORMA COMPLEMENTAR Nº 14, DE 13 DE MARÇO DE 2018. **Presidência da República.** Disponível em: <http://dsic.planalto.gov.br/arquivos/documentos-pdf/NC_14_R01.pdf>. Acesso em: 07 de jan. de 2020.

CLASSIFICAÇÃO DESSE DOCUMENTO - PÚBLICO

Anielle Martinelli, DPO
Diretora do Comitê de Conteúdo da ANPPD

Davis Alves, Ph.D
Presidente da ANPPD

Elaborado por:
Jônatas Mattes, Membro ANPPD

Data de publicação:
Fevereiro de 2020