Número da Norma Complementar	Revisão	Emissão	Folha
14/IN01/DSIC/GSIPR	00	30/JAN/12	1/7

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

DIRETRIZES RELACIONADAS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA O USO DE COMPUTAÇÃO EM NUVEM NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL, NORMATIVA E BIBLIOGRÁFICA

Decreto nº 3.505, de 13 de junho de 2000.
ABNT NBR ISO/IEC 27002:2005 - Código de Práticas para a Gestão da Segurança da Informação.
Instrução Normativa GSI Nº 1, de 13 de junho de 2008, e respectivas Normas Complementares.
The NIST Definition of Cloud Computing (Special Publication 800-145).
CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.
Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, versão 01 – Nov./2010.

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

1. **Objetivo**
2. **Considerações Iniciais**
3. **Fundamento Legal da Norma Complementar**
4. **Conceitos e Definições**
5. **Princípios e Diretrizes**
6. **Responsabilidades**
7. **Vigência**
8. **Anexo**

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

2 CONSIDERAÇÕES INICIAIS

A Computação em Nuvem despontou com a grande promessa de reduzir os custos das organizações em tecnologia da informação – seja pela simplificação dos ambientes, pela diminuição dos encargos de administração das infraestruturas ou pela facilidade de alocação de recursos ou serviços. Porém, o uso dessa tecnologia exige esforços e atenção por parte dos órgãos e entidades da APF para que possam viabilizar e assegurar a SIC. Esse novo cenário está gerando lacunas e, inevitavelmente, dúvidas a respeito de que medidas devem ser tomadas para que a nova tecnologia seja melhor aproveitada para atender, com segurança, aos objetivos estratégicos institucionais.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1. **Agente Responsável:** servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de implementar procedimentos relativos ao uso seguro de tecnologias de computação em nuvem;

4.2. **Ativos de Informação**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

4.3. **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

4.4. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

4.5. **Computação em Nuvem**: modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

4.6. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

4.7. **Gestão de Segurança da Informação e Comunicações**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

4.8. **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

4.9. **Modelo de Serviço**: são modelos de serviço da computação em nuvem, em geral: Software em Nuvem como um Serviço (*Software as a Service* - SaaS); em Nuvem como um Serviço (*Plataform as a Service* - PaaS); e Infraestrutura em Nuvem como um Serviço (*Infrastructure as a Service* - IaaS);

4.10. **Modelo de Implementação:** são os modelos de implementação da computação em nuvem em geral: Nuvem Própria, Nuvem Comunitária, Nuvem Pública e Nuvem Híbrida;

4.11. **Política de Segurança da Informação e Comunicações (POSIC)**: documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

4.12. **Segurança da Informação e Comunicações (SIC):** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação;

4.13. **Valor do Ativo de Informação**: valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão ou entidade da APF, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.

5 PRINCÍPIOS E DIRETRIZES

5.1. O órgão ou entidade da APF deve observar, no mínimo, antes de adotar a tecnologia de computação em nuvem:

5.1.1. As diretrizes estabelecidas em sua POSIC;

5.1.2. As diretrizes do processo de Gestão de Riscos de SIC a respeito da adoção dos modelos de serviço e implementação de computação em nuvem;

5.1.3. As diretrizes do processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC;

5.2. Ao contratar ou implementar um serviço de computação em nuvem, o órgão ou entidade da APF deve garantir que:

5.2.1. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes e normas de SIC, estabelecidas pelo GSIPR, e às legislações vigentes;

5.2.2. A legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem;

5.2.3. O contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

5.3. Os órgãos ou entidades da APF devem avaliar quais informações serão hospedadas na nuvem, considerando:

5.3.1. O processo de Classificação da Informação de acordo com a legislação vigente;

5.3.2. O valor do ativo de informação;

5.3.3. Os Controles de Acesso, físicos e lógicos, relativos à SIC;

5.3.4. O modelo de serviço e de implementação de computação em nuvem a serem adotados;

5.3.5. A localização geográfica onde as informações estarão fisicamente armazenadas.

6 RESPONSABILIDADES

6.1. Cabe à Alta Administração dos órgãos ou entidades da APF, no âmbito de suas competências, assegurar a utilização de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta norma;

6.2. Ao Gestor de SIC, no âmbito de suas atribuições, cabe propor ações de SIC para a implementação ou a contração, nos órgãos ou entidades da APF, de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta Norma Complementar;

6.3. De acordo com as necessidades de cada órgão ou entidade da APF, podem ser indicados agentes responsáveis pela implementação dos procedimentos relativos ao uso seguro de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta Norma Complementar.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

8 ANEXO

O modelo de computação em nuvem possui cinco características essenciais, três modelos de serviço e quatro modelos de implementação:

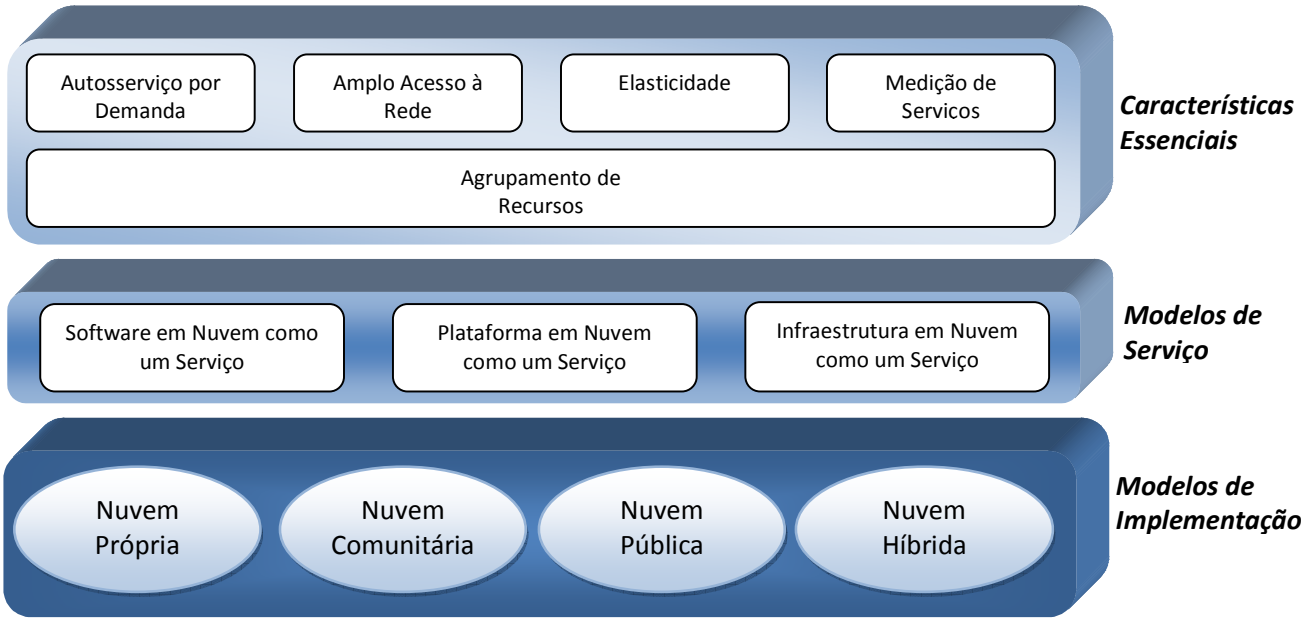

Figura: Adaptado de *CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, p. 13.

1 CARACTERÍSTICAS ESSENCIAIS

1.1. Autosserviço por demanda: os clientes podem provisionar, conforme suas necessidades, capacidades computacionais – como servidores e espaço de armazenamento de dados – de maneira automática, sem solicitar diretamente ao provedor de serviços;

1.2. Amplo acesso à rede: os recursos computacionais estão disponíveis através da rede e podem ser acessados através de mecanismos padrão, que possibilitam uso de plataformas heterogêneas;

1.3. Agrupamento de recursos: os recursos de computação dos provedores de serviço estão organizados em um modelo de negócio com multi-arrendatários, com diversos recursos físicos e virtuais, que podem ser dinamicamente configurados pelos clientes conforme suas demandas;

1.4. Elasticidade: os recursos podem ser provisionados de maneira rápida, ou até mesmo automaticamente, para se ajustar à demanda necessária. Para os clientes de computação em nuvem, as capacidades dos recursos parecem ser ilimitadas;

1.5. Medição de Serviços: os sistemas de nuvem gerenciam os recursos por meio de medições num certo nível de abstração apropriado para o tipo de serviço, como por exemplo: espaço de armazenamento, processamento, largura de banda utilizada e contas de usuários ativos. Relatórios sobre o uso de recursos podem ser utilizados pelas partes de modo a trazer transparência na prestação do serviço.

2 MODELOS DE SERVIÇOS

2.1. Software em Nuvem como um Serviço (*Software as a Service* - SaaS): nesta modalidade, o cliente tem a possibilidade de utilizar aplicações do provedor de serviços na infraestrutura da nuvem, que são acessíveis de vários equipamentos por meio de uma interface leve, como um navegador. Essencialmente, trata-se de uma forma de trabalho cuja aplicação é oferecida como serviço, eliminando-se a necessidade de se adquirir licenças de uso ou infraestutura para utilizá-la. O cliente de computação em nuvem gerencia apenas as configurações dos aplicativos, específicas do usuário;

2.2. Plataforma em Nuvem como um Serviço (*Plataform as a Service* - PaaS): nesta modalidade, o cliente tem a possibilidade de ter sua capacidade computacional atendida por uma infraestrutura customizada na nuvem, possibilitando o uso de aplicações adquiridas ou desenvolvidas utilizando-se de ferramentas, bibliotecas, serviços ou linguagens de programação suportadas pelo provedor de serviço. O cliente tem ingerência sobre os aplicativos implementados e hospedados na nuvem, e sobre as configurações do ambiente;

2.3. Infraestrutura em Nuvem como um Serviço (*Infrastructure as a Service* - IaaS): esta modalidade assemelha-se ao conceito de **Plataforma em Nuvem como um Serviço**, mas a diferença está na oferta da infraestrutura do hardware – processamento, armazenamento, comunicação –, seja físico ou virtual, do provedor de serviço. O cliente tem liberdade para implementar e executar arbitrariamente suas aplicações, o que inclui o sistema operacional e seus recursos.

3 MODELOS DE IMPLEMENTAÇÃO

3.1. Nuvem Própria: a infraestrutura da nuvem pertence apenas a uma organização e suas subsidiárias;

3.2. Nuvem Comunitária: a infraestrutura da nuvem é compartilhada entre diversas organizações que possuem necessidades comuns (missão, valores, requisitos de segurança, políticas, requisitos legais);

3.3. Nuvem Pública: a infraestrutura da nuvem está disponível para a sociedade ou para um grupo de organizações e é administrada por um provedor os serviços;

3.4. Nuvem Híbrida: é a composição de dois ou mais modelos de nuvem interligados por padrões ou tecnologias proprietárias que proporcionam a interoperabilidade entre elas, possibilitando a portabilidade de aplicações e dados.