ANEXO XVII
NORMA DE GESTÃO DE SERVIÇOS EM NUVEM

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	24/07/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de gestão de serviços em nuvem dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelo Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

2. OBJETIVO

Especificar e gerenciar a segurança da informação para o uso de serviços em nuvem.

3. DIRETRIZES

Orientações da norma de gestão de serviços em nuvem.

3.1 REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

A computação em nuvem é composta pelos seguintes modelos de implantação:

I - nuvem privada (ou interna);

II - nuvem comunitária;

III - nuvem pública (ou externa); e

IV - nuvem híbrida.

Para que o PJMA adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia, deverão ser observados alguns requisitos mínimos que serão vistos a seguir.

3.1.1 Transferência de Serviços para um Provedor de Serviço de Nuvem

Antes de transferir serviços ou informações para um provedor de serviço de nuvem, o PJMA deverá, no mínimo:

I - garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros;

II - realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação;

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - avaliar quais informações serão hospedadas na nuvem;

V - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução;

VI - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

3.1.2 Capacidade do Provedor de Serviço de Nuvem para Implementar Atualizações

Em função da capacidade do provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, o PJMA deverá, no mínimo:

I - definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;

II - revisar e atualizar periodicamente seus processos internos de gestão de riscos de segurança da informação.

3.1.3 Gerenciamento de Identidades e de Registros de Eventos (Logs)

Em relação ao gerenciamento de identidades e de registros, o PJMA deverá, no mínimo:

I - adotar padrão único de identidade para permitir o uso de tecnologia Single Sign-On (SSO) no processo de autenticação de seus(suas) usuários(as) no provedor de serviço de nuvem;

II - gerir junto ao provedor de serviço de nuvem o acesso ao ambiente de autenticação do PJMA;

III - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia SSO, o qual deverá ser acompanhado de Múltiplo Fator de Autenticação (MFA) ou de outra alternativa que aumente o grau de segurança no processo de autenticação de seus(suas) usuários(as) no provedor de serviço de nuvem;

IV - exigir do provedor de serviço de nuvem o registro e armazenamento de todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações e armazene tudo pelo período de 01 (um) ano, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do PJMA;

V - manter em ambiente próprio controlado, por no mínimo 02 (dois) anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem;

VI - capacitar os administradores do ambiente em nuvem, para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem.

3.1.4 Uso de Recursos Criptográficos

Em relação à necessidade do uso de recursos criptográficos, o PJMA deverá, no mínimo:

I - verificar se os dados da organização estão sendo tratados e armazenados

de acordo com a legislação vigente;

II - analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios;

III - utilizar, sempre que possível, chaves de criptografia, com tamanho mínimo de 1024 bits, baseadas em suporte criptográfico (token).

3.1.5 Segregação de Dados e da Separação Lógica

Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o PJMA, em conjunto com o provedor de serviço de nuvem, deverão estabelecer, no mínimo, as seguintes ações:

I - garantir que o ambiente contratado seja protegido de usuários(as) externos(as) do serviço em nuvem e de pessoas não autorizadas;

II - implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelo PJMA e por outros(as) usuários(as) do serviço em nuvem;

III - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

IV - garantir a separação de todos os recursos utilizados pelo provedor de serviço de nuvem daqueles recursos utilizados pela administração interna do PJMA;

V - avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

3.1.6 Tratamento da Informação

Em relação ao tratamento da informação em ambiente de computação em nuvem, o PJMA, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deverá observar as seguintes diretrizes:

I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - informação classificada como confidencial não poderá ser tratada em ambiente de computação em nuvem;

III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) a informação com restrição de acesso prevista na legislação;

b) a informação classificada como restrita regulada pelo próprio PJMA.

Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo PJMA, transferidos para o provedor de serviço de nuvem, deverão estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia de segurança deverá ser mantida em território brasileiro;

II - a informação sem restrição de acesso poderá possuir cópias de segurança fora do território brasileiro, conforme legislação aplicável;

III - a informação com restrição de acesso prevista na legislação e a classificada como restrita regulada pelo próprio PJMA, bem como suas cópias de segurança, não poderão ser tratadas fora do território brasileiro;

IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

3.1.7 Cláusulas Contratuais

O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deverá conter, minimamente, além das diretrizes que tratam esta norma, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do PJMA para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte do PJMA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III - proibição do uso de informações do PJMA pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV - conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem ao PJMA no término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do PJMA sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados;

VII - garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei no 13.709, de 14 de agosto de 2018 - LGPD.

3.2 DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Para que esteja habilitado a prestar serviços de computação em nuvem para o PJMA, o provedor de serviço de nuvem deverá cumprir, no mínimo, os seguintes requisitos:

I - possuir metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas e com a legislação, bem como realizar o gerenciamento de riscos descrito na norma de gestão de riscos da segurança da informação;

II - implementar práticas de fortalecimento dos mecanismos de virtualização;

III - possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes e com as melhores práticas nestas áreas;

IV - possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;

V - estabelecer um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS);

VI - utilizar um padrão de criptografia segura, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves criptográficas, com tamanho mínimo de 1024 bits, geradas e armazenadas pelo PJMA;

VII - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do PJMA;

VIII - notificar, imediatamente, ao PJMA incidente cibernético contra os serviços ou dados sob sua custódia;

IX - possuir procedimentos necessários para preservação de evidências, conforme legislação;

X - demonstrar estar em conformidade com os padrões de segurança do serviço em nuvem.

3.2.1 Gerenciamento de Identidades e de Registros de Eventos (Logs)

Em relação ao gerenciamento de identidades e registros o provedor de serviço de nuvem deverá:

I - possuir procedimentos de controle de acesso que abordam a transição entre as funções, os limites e controles dos privilégios dos(as) usuários(as) e os controles de utilização das contas de usuários(as);

II - impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

III - suportar tecnologia SSO para autenticação;

IV - suportar mecanismos de Múltiplo Fator de Autenticação (MFA) ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários(as) do PJMA no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

V - permitir ao PJMA gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem;

VI - atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo PJMA em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso).

3.2.2 Segurança de Aplicações Web

Em relação à segurança de aplicações web disponibilizadas no ambiente remoto o provedor de serviço de nuvem deverá:

I - utilizar firewalls especializados na proteção de sistemas e aplicações;

II - desenvolver código web em conformidade com as diretrizes da norma de desenvolvimento seguro do PJMA, além de seguir as melhores práticas aplicadas no mercado;

III - utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;

IV - realizar ou permitir a realização de testes de invasão (pentest) de redes e de aplicações;

V - possuir um programa de análise/correção de vulnerabilidades.

3.2.3 Segregação de dados

Em relação à segregação de dados o provedor de serviço de nuvem deverá:

I - isolar, utilizando separação lógica, todos os dados e serviços do PJMA de outros clientes de serviço em nuvem;

II - segregar o tráfego de gerenciamento do tráfego de dados do PJMA;

III - implementar mecanismos de segurança entre zonas.

3.2.4 Descarte de Ativos de Informação e de Dados

O provedor de serviço de nuvem deverá possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

I - sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;

II - destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição;

III - armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico ou lógico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.

3.3 CLOUD BROKER

O cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre o PJMA e dois ou mais provedores de serviço de nuvem.

Caso o PJMA realize contratação por meio do cloud broker, plataforma de gestão de múltiplos serviços de nuvem (multinuvem), para realizar procedimentos de provisionamento e orquestração de ambiente, é necessário que a ferramenta observe as disposições seguintes.

3.3.1 Provisionamento e Orquestração

Em relação às funcionalidades de provisionamento e orquestração de multinuvem, o cloud brokers deverá:

I - provisionar para o(a) usuário(a) final um único portal integrado;

II - utilizar modelos de provisionamento;

III - implementar automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;

IV - realizar fluxos de trabalho de orquestração baseada em eventos;

V - apresentar soluções seguras integradas de criação de Infraestrutura por Código - IaaC.

3.3.2 Monitoramento e Análise

Com relação às funcionalidades de monitoramento e análise em multinuvem, a plataforma deverá:

I - entregar relatórios de monitoramento de desempenho de recursos na nuvem;

II - realizar coleta e monitoramento dos registros;

III - apresentar procedimentos de monitoramento de alertas.

3.3.3 Inventário e Classificação

Em relação às funcionalidades de inventário e classificação em multinuvem, o cloud brokers deverá:

I - inventariar os recursos na nuvem;

II - apresentar procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem;

III - detectar recursos sem etiqueta.

3.3.4 Gerenciamento de Segurança, Conformidade e Identidade

Em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade, a plataforma deverá:

I - possuir mecanismos de SSO e de Múltiplo Fator de Autenticação (MFA) das plataformas em nuvem;

II - dispor de gerenciamento seguro de usuários(as) e de grupos de usuários(as);

III - realizar gerenciamento de segurança dos recursos;

IV - apresentar notificações de eventos de alerta multicanal;

V - possuir gerenciamento de identidade e acesso - IAM;

VI - realizar registros de atividades da plataforma em nuvem;

VII - armazenar os dados em datacenter abrigado em território brasileiro;

VIII - cumprir a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD;

IX - atender aos requisitos de disponibilidade, de escalabilidade, de redundância e de criptografia.

O cloud broker poderá utilizar ferramentas de Software as a Service (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar esta plataforma.

O cloud broker será o responsável por garantir que os provedores de serviço de nuvem que ele representa:

I - cumpram todos os requisitos previstos nesta norma e na legislação

brasileira;

II - operem de acordo com as melhores práticas de segurança.

O PJMA deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - supervisionar o serviço em nuvem disponibilizado pelo provedor de serviço, observando as disposições desta norma;

II - estabelecer os países nos quais dados e informações custodiados pelo PJMA poderão ser armazenados em soluções de computação em nuvem;

III - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pelo PJMA, em soluções de computação em nuvem;

IV - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao PJMA, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

V - supervisionar a aplicação de medidas de correção pelo provedor de serviço de nuvem;

VI - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;

VII - capacitar a equipe responsável por esse gerenciamento nas tecnologias

utilizadas pelo provedor de serviço de nuvem;

VIII - exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços;

IX - elaborar uma matriz que inclua obrigações e responsabilidades do PJMA e do provedor de serviço de nuvem;

X - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem.

5. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

6. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

7. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.