ANEXO XIV

RESOLUÇÃO N. 350/2025-TJRO

NPODER JUDICIÁRIO DO ESTADO DE RONDÔNIA
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 12 - SEGURANÇA EM NUVEM

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL

Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR

Desembargador Glodner Luiz Pauletto

Desembargador Gilberto Barbosa Batista dos Santos

Juíza Valdirene Alves da Fonseca Clementele

Elaine Piacentini Bettanin

Jucélio Scheffmacher de Souza

Ângela Carmen Szymczak de Carvalho

Rosemeire Moreira Ferreira

Fabiano Sergio Paiva Dias de Sá

Gustavo Luiz Sevagnan Nicocelli

Eduardo Luiz Will Bezerra

Reginaldo de Souza Gadelha

Ignácio de Loiola Reis Junior

Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa

Reginaldo de Souza Gadelha

Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts

Ângela Carmen Szymczak de Carvalho
Fernanda Soares Lana
Ignacio de Loiola Reis Junior
Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI
4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI
Política da Segurança da Informação Cibernética (PSIC) **NSIC 12 - Segurança em Nuvem**				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**

1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

Estabelecer diretrizes, padrões e boas práticas de segurança para o uso da computação em nuvem no âmbito do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 A computação em nuvem tem se tornado cada vez mais popular e é amplamente adotada por organizações de todos os portes. No entanto, com a migração para a nuvem, surgem novos desafios relacionados à segurança da informação. Este normativo aborda as medidas de segurança necessárias para proteger os dados e recursos armazenados na nuvem.

2.2 Disciplinar por meio deste normativo, os requisitos mínimos de segurança da informação e cibernética para utilização de soluções de serviços e computação em nuvem no âmbito do PJRO;

2.3 Proteção da Confidencialidade, Integridade, Disponibilidade e Autenticidade das Informações do PJRO;

2.4 Alinhamento com as normas, regulamentações e melhores práticas relacionadas à matéria de segurança da informação e cibernética na nuvem.

3 FUNDAMENTO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da Organização.

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação.

3.3 Portaria n. 162/2021-CNJ, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário.

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

3.6 Instrução Normativa nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

3.7 NIST - SP 800-145: *The NIST Definition of Cloud Computing. National Institute of Standards and Technology.*

3.8 NIST - SP 500-291: *NIST Cloud Computing Standards Roadmap. National Institute of Standards and Technology.*

4 CONCEITOS E DEFINIÇÕES

4.1 **Computação em nuvem:** modelo que permite acesso global a recursos computacionais configuráveis e serviços por meio da rede mundial de computadores, de forma conveniente e sob demanda, que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de nuvem.

4.2 **Multicloud:** usar mais de um provedor de serviços em nuvem para atender às necessidades de uma organização. Em vez de depender de um único provedor, o *multicloud* permite que as organizações distribuam suas cargas de trabalho e recursos em várias nuvens.

4.3 **On premise:** infraestrutura de tecnologia da informação (TI) que é implantada e gerenciada localmente por uma organização em suas próprias instalações físicas, em vez de utilizar serviços em nuvem ou recursos hospedados remotamente.

4.4 **Nuvem privada:** modelo de computação em nuvem dedicado exclusivamente a uma única organização. Nesse modelo, a infraestrutura de nuvem é projetada, implementada e gerenciada internamente pela própria organização ou por um provedor de serviços de nuvem privada.

4.5 **Nuvem pública:** infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas.

4.6 **Nuvem híbrida:** infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (*on premise*, privadas ou públicas), que permanecem com suas próprias

características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.

4.7 **SaaS (Software as a Service ou Software como Serviço)**: modelo de distribuição de software em que ele é fornecido aos usuários através da Internet. O provedor do serviço de software é responsável por hospedar, gerenciar e disponibilizar o software aos usuários finais por meio de uma conexão de rede. Os usuários acessam o software por meio de um navegador web ou, em alguns casos, por meio de aplicativos específicos.

4.8 **PaaS (Platform as a Service ou Plataforma como Serviço)**: modelo de computação em nuvem que fornece aos desenvolvedores uma plataforma completa para criar, implantar e gerenciar aplicativos sem se preocupar com a complexidade subjacente da infraestrutura de hardware e software. No modelo PaaS, o provedor de serviços de nuvem oferece uma plataforma na qual os desenvolvedores podem criar e executar seus aplicativos. Essa plataforma inclui recursos essenciais, como sistemas operacionais, serviços de banco de dados, servidores web, frameworks de desenvolvimento e ferramentas de implantação. Os desenvolvedores podem usar esses recursos para escrever e implantar seus aplicativos de maneira rápida e eficiente.

4.9 **IaaS (Infrastructure as a Service ou Infraestrutura como Serviço)**: modelo de computação em nuvem, onde o Provedor de Nuvem fornece infraestrutura de TIC virtualizada, incluindo recursos de hardware, como servidores, redes e sistemas de armazenamento, através da Internet. O provedor de serviços em nuvem é responsável por fornecer e gerenciar a infraestrutura física subjacente, enquanto seus clientes têm o controle e responsabilidade sobre as configurações, implantações e gerenciamento dos recursos virtuais. Os clientes podem provisionar e dimensionar recursos conforme necessário, pagando apenas pelos recursos utilizados.

4.10 **FaaS (Function as a Service ou Funções como serviço)**: também conhecido como "*serverless computing*", o FaaS permite que os desenvolvedores escrevam e implantem funções individuais de código que são executadas em resposta a eventos ou solicitações específicas. Os desenvolvedores não precisam se preocupar com a infraestrutura subjacente, pois o provedor de serviços em nuvem gerencia a execução e a escalabilidade automática dessas funções.

4.11 **CaaS (Container as a Service ou Container como Serviço)**: o CaaS é um modelo em que os provedores de serviços em nuvem oferecem plataformas para criar, implantar e gerenciar contêineres, como o Docker. Ele fornece uma infraestrutura para orquestrar e gerenciar contêineres em escala, permitindo que os desenvolvedores implantem seus aplicativos de maneira mais eficiente e com recursos isolados.

4.12 **DaaS (Desktop as a Service ou Estação de Trabalho como Serviço)**: O DaaS é um modelo em que o ambiente de desktop completo, incluindo sistema operacional, aplicativos e dados, é hospedado na nuvem e acessado remotamente pelos usuários. Isso permite que os usuários acessem seus desktops e aplicativos de qualquer dispositivo com conexão à Internet, oferecendo mobilidade e flexibilidade.

4.13 **DRaaS (Disaster Recovery as a Service ou Recuperação de Desastres como Serviço)**: O DRaaS é um modelo que fornece serviços de recuperação de desastres baseados em nuvem. Ele oferece a capacidade de replicar e armazenar dados e sistemas críticos em um ambiente de nuvem seguro, permitindo a rápida recuperação de dados e a continuidade dos negócios em caso de desastres ou interrupções.

4.14 **Nuvem do PJRO:** serviço de computação em nuvem, mediante arquitetura de serviços, como infraestrutura, plataforma ou software, fornecido por provedor de serviços em nuvem, ou localmente, por meios próprios.

4.15 **Rede de computadores do PJRO:** conjunto de recursos de TIC que, interligados em uma rede de comunicação de dados fornecida pelo PJRO possibilita compartilhamento de informações.

4.16 **Provedor de nuvem - (Cloud Service Provider)**: empresa responsável por disponibilizar e manter os serviços de computação em nuvem para organizações, e gerenciar a infraestrutura necessária para provimento dos serviços, conforme níveis mínimos de serviço e controles de segurança da informação e cibernéticos acordados.

4.17 **Cloud Broker (CB):** organização responsável por servir de ponto de contato ou interface para um ou mais provedores contratados, para gerenciamento de uso, desempenho e entregas de serviços em computação em nuvem**.**

4.18 **Modelo multi-inquilino (ou multi-locatário):** arquitetura capaz de permitir o compartilhamento de infraestruturas físicas entre diversos usuários ou locatários, proporcionando flexibilidade e eficiência, mas preservando o isolamento de instâncias lógicas dos recursos alocados entre cada usuário.

4.19 **Modelos de computação em nuvem baseados na arquitetura de serviços:** modelo baseado em serviço de computação em nuvem: infraestrutura, plataforma ou software como serviço.

4.20 **Responsável pelo ativo de TIC:** unidade, grupo, ou servidores do PJRO responsável pela administração, ainda que temporária, de ativo de TIC. Sinônimo de Administrador de ativos de TIC.

4.21 **Responsável por recurso de TIC:** usuário ou grupo de usuários responsável por definir critérios de utilização e autorizar, conceder ou modificar privilégios de uso sobre o recurso de TIC. Sinônimo de Administrador de recursos de TIC.

4.22 **Unidade gestora de TIC:** responsável pela definição de processos de trabalho, requisitos, regras de negócio e níveis de serviço aplicáveis à solução de TIC.

4.23 **Unidades provedoras de TIC:** Unidade responsável pelos serviços, soluções e infraestrutura de TIC.

4.24 **Divisão de Responsabilidade:** a figura 1 ilustra as áreas de responsabilidade entre PJRO e o Provedor de Serviço em Nuvem, de acordo com o tipo de implantação da pilha, se dividindo em responsabilidades do PJRO, do Provedor de Nuvem e Compartilhadas entre o PJRO e o Provedor de Nuvem.

4.25 **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

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

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

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

Figura 1. Modelo de responsabilidade compartilhada.

5 CONTROLES

Seção I
Das Diretrizes Principais

5.1 A nuvem do PJRO é um serviço de computação em nuvem, mediante arquitetura de serviços como infraestrutura de TIC, plataforma ou software, fornecido por provedor de serviços de nuvem pública ou privada, ou localmente, por meios próprios.

5.2 A nuvem do PJRO estende a infraestrutura de serviços fornecidos pela rede PJRO.

5.3 O provimento da nuvem do PJRO pode ser intermediado por Cloud Broker.

5.4 A nuvem do PJRO disporá de ambiente seguro e atenderá, no que couber, às diretrizes estabelecidas no normativo sobre Controle de Acesso e Gerenciamento de Identidade.

5.5 A nuvem PJRO atenderá aos seguintes requisitos:

5.5.1. Auto provisionamento de recursos na nuvem e ajuste de acordo com as necessidades no decorrer do tempo, de maneira automática, sem a necessidade de interação com provedor de serviços;

5.5.2. Elasticidade na alocação e liberação de recursos contratados dinamicamente, conforme demanda;

5.5.3 Mensuração automática de serviços para estabelecimento de níveis mínimos de serviço, otimização de recursos e, se aplicável, precificação por uso;

5.5.4. Isolamento de recursos computacionais oriundos do provedor, caso haja a prestação de serviços para múltiplos clientes, em arquitetura multi-inquilino;

5.5.5. Amplo acesso aos recursos da nuvem por diferentes recursos de TIC, como estações de trabalho, tablets e smartphones;

5.5.6. Monitoramento para assegurar transparência no uso de recursos, controle de uso, observâncias às normas definidas pelo PJRO e fornecer evidências, no caso de incidentes de segurança da informação e cibernética, respeitados os direitos e as garantias individuais previstos em lei;

5.5.7. Segurança em múltiplas camadas para proporcionar a sobreposição de controles de segurança, a fim de mitigar riscos, particularmente se houver ataque bem-sucedido em uma das camadas;

5.5.8. Autenticação robusta e controle de acesso para proteger os recursos na nuvem, podendo usar medidas de autenticação multifator, como senhas fortes, tokens ou autenticação biométrica. Além disso, deve-se ter uma gestão adequada de privilégios de acesso, garantindo que apenas os usuários autorizados tenham permissão para acessar os dados e serviços;

5.5.9. Os dados devem ser criptografados tanto em trânsito quanto em repouso, utilizando algoritmos robustos e chaves de criptografia seguras, onde o PJRO mantenha o controle total sobre as chaves de criptografia, evitando a dependência exclusiva do provedor de serviços em nuvem;

5.5.10. Implementação de sistemas de monitoramento e detecção de ameaças para identificar atividades suspeitas ou maliciosas na nuvem. Devem ser utilizadas ferramentas que possibilitem o monitoramento em tempo real, a análise de logs de eventos e a detecção de comportamentos anormais, a fim de garantir uma resposta rápida a incidentes de segurança;

5.5.11. Realização de backups regulares dos dados armazenados na nuvem para a continuidade do negócio. Deve-se garantir que existam procedimentos de backup adequados e que os dados possam ser recuperados de forma rápida e confiável em caso de falhas ou incidentes de segurança;

5.5.12. Ter um plano de resposta a incidentes de segurança específico para a nuvem. O PJRO deve estabelecer procedimentos claros para lidar com violações de segurança, como vazamento de dados ou acesso não autorizado. O plano deve abranger a notificação de incidentes, a investigação, a mitigação e a recuperação de incidentes, além de envolver os responsáveis internos e o provedor de serviços em nuvem, quando necessário;

5.5.13. Conscientização e treinamento dos magistrados(as) e servidores(as) para garantir a segurança da nuvem. Todos os usuários devem ser educados sobre as melhores práticas de segurança na nuvem, incluindo o uso adequado de senhas, o reconhecimento de ameaças e a proteção de informações sensíveis. O PJRO deve realizar treinamentos regulares e

manter os magistrados(as) e servidores(as) atualizados sobre as políticas e procedimentos de segurança;

5.5.14. Realizar testes regulares e auditorias de segurança para avaliar a eficácia das medidas de segurança na nuvem. Isso pode incluir testes de penetração, análise de vulnerabilidades e revisões de conformidade. Os resultados desses testes devem ser utilizados para aprimorar as políticas e controles de segurança existentes;

5.5.15. Revisar e atualizar regularmente as políticas e controles de segurança da nuvem para garantir que estejam alinhados com as melhores práticas e padrões de segurança mais recentes. O PJRO deve acompanhar as atualizações do provedor de serviços em nuvem e as mudanças nas regulamentações de segurança para garantir uma postura de segurança atualizada;

5.5.16. O PJRO deve deter o maior nível de privilégio na administração dos recursos e serviços das nuvens públicas contratadas;

5.5.17. A comunicação lógica com o(s) provedor(es) de serviços de nuvem, deve ter rotas de contingências, devendo o PJRO implementar links diretos junto aos provedores e com redundância via rede de Internet;

5.5.18. As contas criadas, junto aos provedores de nuvem, devem seguir as melhores práticas relativas à governança, conexão de rede e segurança da informação na nuvem; e

5.5.19. Implementar e validar as propriedades de segurança das aplicações durante o ciclo de vida de design, desenvolvimento e implantação.

5.6 A nuvem do PJRO será promovida e mantida pela Secretaria de Tecnologia da Informação e Comunicação do PJRO com apoio da alta gestão.

5.7 São princípios para o uso da nuvem do PJRO:

5.7.1. Security by design: Incorporar boas práticas de segurança da informação para diminuir as vulnerabilidades desde a fase de planejamento e projeto dos serviços digitais;

5.7.2. Governança: Implementar mecanismos para garantir a identificação de cargas de trabalho, usuários e permissionamento no ambiente da nuvem, bem como a adequada gestão de recursos e de processos de trabalho por meio da automação;

5.7.3. Modelo de segurança compartilhada: Habilitar os mecanismos de segurança pertinentes à carga de trabalho implementada (security by default) seguindo a divisão de responsabilidade entre provedor de nuvem e o PJRO de acordo com o modelo de serviço implementado (IaaS, PaaS, SaaS entre outros); e

5.7.4. Gerenciamento de risco: Incorporar mecanismos de análise de riscos e estabelecer medidas de tratamento de riscos desde a fase de planejamento e projeto.

5.8 São funções relativas ao uso de nuvem:

5.8.1. Gestor de segurança da informação e cibernética;

5.8.2. Comitê de Gestão de Segurança da Informação e Cibernética;

5.8.3. Comitê Consultivo de Mudanças (CCM);

5.8.4. Responsável pelo recurso de TIC;

5.8.5. Responsável pela infraestrutura de TIC;

5.8.6. Provedores de nuvem; e

5.8.7. Cloud Broker.

Seção II - Das Responsabilidades
Gestor de Segurança da Informação e Cibernética

5.9 São responsabilidades do Gestor de Segurança da Informação e Cibernética:

5.9.1. Instituir e coordenar a equipe responsável pelas revisões deste normativo referente ao uso seguro de computação em nuvem;

5.9.2. Validar as propriedades de segurança das aplicações que serão implantadas em nuvem; e

5.9.3. Supervisionar a aplicação deste normativo sobre o uso seguro de computação em nuvem.

5.10 São responsabilidades do Comitê de Gestão de Segurança da Informação:

5.10.1. Classificar os dados e informações do PJRO com base em sua sensibilidade e nível de criticidade. A classificação permitirá a implementação de controles de segurança apropriados, de acordo com as necessidades específicas de cada tipo de dado;

5.10.2. Estabelecer restrições geográficas aplicáveis a dados e informações custodiados pelo PJRO de acordo com sua classificação;

5.10.3. Analisar, em caráter conclusivo, as minutas de revisão deste normativo sobre o uso seguro da computação em nuvem; e

5.10.4. Definir a necessidade de criptografia para o trânsito e armazenamento de dados e informações, custodiados pelo PJRO, em soluções de computação em nuvem de acordo com sua classificação.

Seção III - Das Responsabilidades
Comitê Consultivo de Mudança

5.11 São responsabilidades do Comitê Consultivo de Mudança:

5.11.1. Receber e aprovar ou reprovar as propostas de mudanças para nuvem pública;

5.11.2. As propostas de mudanças para nuvem pública devem ter os seguintes itens:

5.11.2.1. Justificativa da mudança;

5.11.2.2. Objetivo da mudança;

5.11.2.3. Descrição das ações, prazos e responsáveis;

5.11.2.4. Riscos ao PJRO se a mudança não ocorrer;

5.11.2.5. Requisitos de Segurança da Informação e Cibernéticos para garantir a proteção adequada dos dados e recursos da aplicação contra ameaças internas e externas, com criptografia de dados em repouso e em trânsito, controle de acesso granular, autenticação robusta, monitoramento de segurança e resposta a incidentes;

5.11.2.6. Requisitos de disponibilidade para garantir que a aplicação esteja sempre disponível para os usuários. Envolvendo a implementação de redundância, balanceamento de carga, *failover* automático, tolerância a falhas e alta disponibilidade de serviços e infraestrutura;

5.11.2.7. Requisitos de desempenho para garantir que a arquitetura promova um desempenho adequado e que envolva otimização de consultas de banco de dados, escalabilidade horizontal e vertical, uso eficiente dos recursos de computação, armazenamento e rede, além de monitoramento e ajuste contínuos;

5.11.2.8. Requisitos de escalabilidade para garantir que a aplicação possa lidar com aumentos na demanda de forma eficiente e com a capacidade de adicionar ou remover recursos facilmente, como instâncias de servidor, armazenamento e balanceadores de carga, para lidar com picos de tráfego ou crescimento no número de usuários;

5.11.2.9. Requisitos de conformidade para garantir que a aplicação esteja em conformidade com regulamentos e padrões relevantes, como proteção de dados, privacidade, governança de TI, segurança da informação e requisitos específicos da indústria;

5.11.2.10. Requisitos de latência e tempo de resposta para garantir que a aplicação responda de forma rápida e eficiente às solicitações dos usuários. Isso envolve otimização de rede, redução de latência, uso de CDN (*Content Delivery Network*) e caches;

5.11.2.11. Requisitos de backup e recuperação para garantir a resiliência e a integridade dos dados em caso de falhas ou incidentes. Isso inclui a realização regular de backups, a replicação de dados e a validação de procedimentos de recuperação;

5.11.2.12. Requisitos de custos para estimar a previsão orçamentária, gerência e otimização dos custos associados à execução da aplicação na nuvem pública, com o dimensionamento adequado dos recursos, o uso eficiente dos serviços da nuvem, a escolha dos modelos de preços corretos e a implementação de monitoramento de custos;

5.11.2.13. Requisitos de integração para garantir a capacidade de integração da aplicação com outros sistemas e serviços, como APIs, serviços de autenticação, bancos de dados externos e sistemas de terceiros;

5.11.2.14. Desenho da arquitetura;

5.11.2.15. Componentes computacional, serviços ou solução de nuvem a serem utilizados; e

5.11.2.16. Apresentação do custo e impacto orçamentário.

5.11.3. Se autorizada, após implementação das configurações e recursos necessários em ambiente de nuvem, a requisição de mudança deve ser encaminhada ao CCM para liberação, a fim de receber autorização de disponibilidade em ambiente de produção;

5.11.3.1. O pedido de liberação deve conter no mínimo a data da execução, as ações com prazos, responsáveis e riscos, também deve constar o plano de *rollback*, caso a implementação apresente falha, e a validação dos requisitos de segurança da informação e cibernético;

Seção IV - Das Responsabilidades
Unidade responsável pela Infraestrutura de TIC

5.12 São responsabilidade da unidade responsável pela infraestrutura de TIC:

5.12.1. Assegurar a contínua efetividade da comunicação lógica com o(s) provedor(es) de serviços de nuvem, sejam eles através de links direto ou via rede de Internet, e a assegurar que os controles e níveis de serviços acordados sejam cumpridos;

5.12.2. Supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios; e

5.12.3. Aplicar, no que couber, as responsabilidades definidas na Política de Segurança da Informação Cibernética do PJRO.

Seção V - Das Responsabilidades
Provedor de Nuvem e Cloud Broker

5.13 São de responsabilidades do provedor de nuvem:

5.13.1 Assinar o termo de confidencialidade que impeça o mesmo de usar, transferir e liberar dados, sistemas, processos e informações do PJRO para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

5.13.2 Garantir a exclusividade de direitos, por parte do PJRO, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

5.13.3 Conformidade das suas normas com as legislações brasileira e melhores práticas recomendados por instituições e organizações que orientam sobre segurança da informação e cibernética;

5.13.4 Devolução integral dos dados, informações e sistemas sob sua gerência ao PJRO, ao término do contrato;

5.13.5. Eliminação, ao término do contrato, de qualquer dado, informação ou sistema sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados;

5.13.6 Garantir o direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 - LGPD;

5.13.7 Seguir o modelo de responsabilidade compartilhada de acordo com a fig. 1 deste normativo;

5.13.8 Prover, manter, atualizar e ajustar as configurações necessárias para melhorar o nível de segurança da informação e cibernética; e

5.13.9 Ofertar soluções alinhadas e atualizadas com as demandas de mercado, para prover a segurança da informação cibernética em sua estrutura e nos recursos e serviços contratados pelo PJRO.

5.14 São de responsabilidades do Cloud Broker:

5.14.1 Garantir que os provedores de serviço de nuvem, que ele representa, cumpram todos os requisitos previstos neste normativo e na legislação brasileira operando de acordo com as melhores práticas de segurança física e da informação.

Seção V - Das Responsabilidades Finais

5.15 Além dos aspectos da segurança da informação e cibernética, o PJRO deve implementar os seguintes requisitos de governança para promover a confiabilidade, integridade e disponibilidade dos serviços, dados e informações operados em nuvem:

5.15.1. Alocar e garantir a dotação orçamentária para manter e expandir os serviços existentes, em nuvem;

5.15.2. Estabelecer as competências e estrutura organizacional das atividades para computação em nuvem, com responsabilidades e autoridades, garantindo que as linhas de comunicação, estratégia e objetivos estejam estabelecidos, promovendo a transparência e a prestação de contas;

5.15.3. Implementar processos para identificar, avaliar e gerenciar os riscos associados às operações em computação em nuvem do PJRO, realizar análises de risco periódicas, definir medidas de mitigação e criação de planos de contingência para lidar com eventos adversos;

5.15.4. Monitorar e controlar regularmente o desempenho e a conformidade das unidades em relação às políticas estabelecidas, através de auditorias internas, revisões de conformidade, avaliações de desempenho e relatórios periódicos;

5.15.5. Promover a transparência na tomada de decisões e nas operações, comunicando claramente os objetivos, as metas e os resultados alcançados; e

5.15.6. Avaliar os provedores de serviços em nuvem antes de assinar contrato. Considerando histórico de segurança, certificações de conformidade, práticas de gerenciamento de vulnerabilidades e políticas de segurança, devendo contratar provedores confiáveis e que incluam cláusulas de segurança e privacidade adequadas.

5.16 A unidade responsável pela infraestrutura de TIC do PJRO adotará as medidas necessárias para operacionalizar o disposto neste normativo.

5.17 À alta administração compete aprovar as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem e divulgá-las às partes interessadas.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, os logs dos serviços em nuvem serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por no mínimo 6 (seis) meses e até 12 (doze) meses.

6.2 Em caso de indícios de descumprimento das diretrizes previstas neste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética poderá de ofício ou por determinação do Comitê Gestor de Segurança da Informação e Cibernética realizar auditoria sobre os fatos.

6.3 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética serão encaminhados ao Comitê Gestor de Segurança da Informação, para análise e deliberação.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.