



Ministério da Cultura
Fundação Biblioteca Nacional

ESTRATÉGIA DE USO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM DA FBN

Rio de Janeiro, outubro de 2024

Presidente

Marco Luchesi

Comitê de Governança Digital

Diretora Executiva – Suely Dias

Coordenadora-geral de Coleções e Serviços aos Leitores – Maria José da Silva Fernandes

Coordenadora-geral de Processamento e Preservação – Gabriela Ayres Ferreira

Coordenadora-geral de Pesquisa e Editoração – Naira Christofolletti Silveira

Coordenadora-geral de Cooperação e Difusão – Verônica de Oliveira Lessa

Coordenadora-geral de Administração e Planejamento – Tânia Pacheco

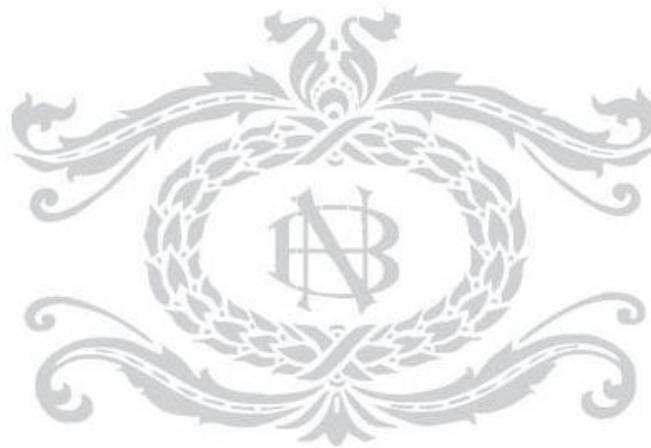
Coordenador de Tecnologia e Informação – Geraldo Gonçalves Chaves Junior

Encarregado de Dados – Wellington Silva

Equipe Técnica de Elaboração

André Chang Kapp

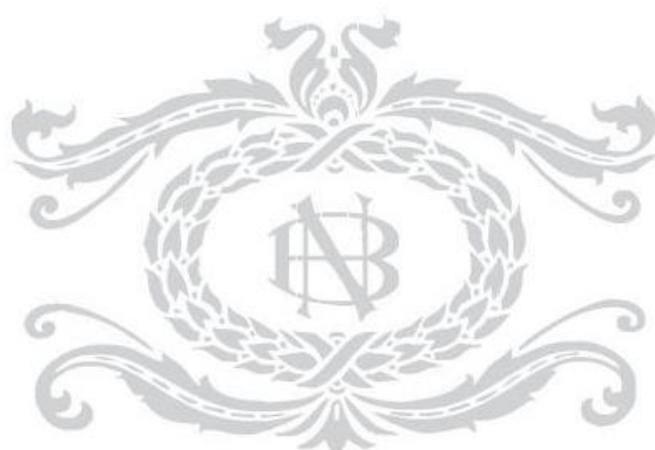
Geraldo Gonçalves Chaves Junior



Sumário

ESTRATÉGIA DE USO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM DA FBN	5
CAPÍTULO I DISPOSIÇÕES GERAIS.....	5
CAPÍTULO II DAS REFERÊNCIAS	7
CAPÍTULO III DOS OBJETIVOS.....	7
CAPÍTULO IV DIRETRIZES PARA A ESTRATÉGIA	8
Seção I.....	8
Da Identificação das Necessidades do Negócio	8
Seção II.....	8
Da Seleção dos Modelos Adequados.....	8
Seção III.....	8
Da Avaliação dos Possíveis Fornecedores	8
Seção IV	8
Da Definição de Requisitos de Segurança	8
Seção V	8
Do Estabelecimento de uma Política de Governança	8
Seção VI	9
Das Diretrizes de Uso Seguro de Software e de Serviços de Computação em Nuvem	9
Seção VII	9
Da Avaliação Quanto às Condições Mínimas de Infraestrutura de TIC da FBN para Utilizar Serviços de Computação em Nuvem	9
Seção VIII	9
Da Definição de Diretrizes de Governança para o Uso da Nuvem	9
Seção IX.....	10
Do Estabelecimento dos Princípios Norteadores da Estratégia	10
Seção X.....	10
Alinhamento com outros Planos Estratégicos.....	10
Seção XI.....	10
Estabelecimento de Linhas de Base e Metas de Benefícios/Resultados Esperados	10
Seção XII.....	10
Das Considerações Sobre Capacitação da Equipe	10
Seção XIII.....	11
Das Considerações Sobre Portabilidade e Interoperabilidade Entre Sistemas, Dados e Serviços	11

Seção XIV	11
Requisitos Regulatorios e de Conformidade	11
Seção XV	11
Indicação da Estratégia de Saída	11
Seção XVI	11
Análise de Riscos.....	11
CAPÍTULO V	11
DA DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM	11
Seção I.....	12
Do Tratamento das Informações no Ambiente de Nuvem	12
Seção II.....	12
Do Armazenamento das Informações no Ambiente de Nuvem em Outros Países.....	12
Seção III.....	12
Da utilização de ambiente de nuvem por cargas de trabalho.....	12
CAPÍTULO VI	13
DAS RESPONSABILIDADES	13
CAPÍTULO VI	13
DISPOSIÇÕES FINAIS.....	13



ESTRATÉGIA DE USO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM DA FBN

Estabelece a **estratégia de uso de software e de serviços de computação em nuvem** no âmbito da Fundação Biblioteca Nacional (FBN), em conformidade com a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, que estabelece o modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do SISP do Poder Executivo Federal.

CAPÍTULO I DISPOSIÇÕES GERAIS

Art. 1º Este documento define a estratégia de uso de software e serviços de computação em nuvem da Fundação Biblioteca Nacional (FBN), com o objetivo de promover a eficiência, segurança, conformidade, aprimoramento dos processos de trabalho e melhoria na oferta de serviços, assim como assegurar que a fundação mitigue os riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação no âmbito da FBN.

Art. 2º Para os fins desta estratégia, consideram-se as definições a seguir:

- I - **Avaliação de riscos de segurança e privacidade:** Análise sistemática dos riscos associados à segurança da informação e à privacidade de dados em serviços de computação em nuvem;
- II - **Catálogo de Serviços de Computação em Nuvem Padronizados:** Relação de serviços de computação em nuvem que um órgão ou entidade fornece aos seus usuários, elaborada de forma padronizada, de acordo com as necessidades do órgão ou entidade e conforme as orientações estabelecidas pela SGD;
- III - **Catálogo de Soluções de TIC com condições padronizadas:** Relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP, podendo incluir o nome da solução, descrição, níveis de serviço, Preço Máximo de Compra de Item de TIC - PMC-TIC, entre outros;
- IV - **Cloud brokers:** Intermediários que facilitam a integração e gestão de múltiplos provedores de serviços de computação em nuvem para uma organização;
- V - **Cloud first:** Estratégia que prioriza serviços de computação em nuvem sobre soluções locais, quando viável e seguro;
- VI - **Cloud-Native:** Aplicações desenvolvidas especificamente para funcionar em serviços de computação em nuvem, tirando proveito de sua elasticidade e escalabilidade;
- VII - **Co-location:** Locação de infraestrutura de data center pertencente a terceiros para hospedar equipamentos computacionais de uma organização.
- VIII - **Computação em nuvem:** Modelo que possibilita o provisionamento e a utilização sob demanda de recursos e serviços computacionais de qualquer lugar e a qualquer momento, de maneira conveniente, com acesso por meio de rede a recursos configuráveis;
- IX - **Estratégia de saída:** Plano para migração de dados e serviços de computação em nuvem, garantindo continuidade dos negócios e proteção dos dados;
- X - **Governança de TI:** Estruturas e processos que asseguram que as tecnologias de informação suportem e alinhem-se aos objetivos e estratégias da organização;
- XI - **Governança de nuvem:** Conjunto de processos e políticas destinados a assegurar o uso efetivo e seguro de serviços de computação em nuvem dentro da organização;
- XII - **Licença de software:** Documento que fornece diretrizes legalmente vinculantes para o uso e a distribuição de determinado software;

- XIII - **Licença de uso:** Instrumento que estabelece o direito de usar o software sem haver a transferência da sua propriedade entre o licenciante e o licenciado;
- XIV - **Licença por subscrição/assinatura:** Permite aos usuários acessar o software por meio de serviços online, em vez de adquirir uma licença de uso único;
- XV - **Licença perpétua:** É uma licença que concede ao usuário o direito de usar o software por tempo indeterminado;
- XVI - **Modelo de Serviços em nuvem IaaS (*Infrastructure as a Service – Infraestrutura como Serviço*):** Capacidade fornecida ao cliente para provisionar processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais;
- XVII - **Modelo de Serviços em nuvem PaaS (*Platform as a Service – Plataforma como Serviço*):** Capacidade fornecida ao cliente para provisionar na infraestrutura de nuvem aplicações adquiridas ou criadas para o cliente;
- XVIII - **Modelo de Serviços em nuvem SaaS (*Software as a Service – Software como Serviço*):** Capacidade de fornecer uma solução de software completa que pode ser contratada de um provedor de serviços de nuvem;
- XIX - **Modelos de implantação de nuvem:** Representam como a computação em nuvem pode ser organizada, com base no controle e no compartilhamento de recursos físicos ou virtuais;
- XX - **Multicloud:** Uso combinado de serviços de múltiplos provedores de serviços de computação em nuvem para distribuir recursos e minimizar dependência de um único fornecedor.

Parágrafo único. Na aplicação desta norma deverão ser observados, no que couber, os conceitos constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Art. 3º Esta estratégia aplica-se para novas contratações de software e serviços de computação em nuvem, abrangendo as seguintes categorias:

- I - Software sob o modelo de licenciamento permanente de direitos de uso;
- II - Software sob o modelo de cessão temporária de direitos de uso;
- III - Software sob o modelo de subscrição ou como Serviço (SaaS);
- IV - Infraestrutura como Serviço (IaaS);
- V - Plataforma como Serviço (PaaS);
- VI - Suporte técnico para software e serviços de computação em nuvem;
- VII - Serviço de operação e gerenciamento de recursos em nuvem;
- VIII - Serviço de migração de recursos para ambiente de nuvem;
- IX - Integração de serviços de computação em nuvem; e
- X - Consultoria especializada em software e/ou serviços de computação em nuvem.

CAPÍTULO II DAS REFERÊNCIAS

Art. 4º Para o desenvolvimento da estratégia de uso de software e de serviços de computação em nuvem, cabe a FBN observar, sem prejuízo das demais normas em vigor:

- I - Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 que estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal. Anexo II da referida portaria define o modelo de documento de estratégia de uso de software e de serviços de computação em nuvem;
- II - Instrução Normativa GSI/PR Nº 5, de 30 de agosto de 2021: 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;
- III - Decreto nº 10.641, de 2 de março de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.
- IV - Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe o Programa de Privacidade e Segurança da Informação.

CAPÍTULO III DOS OBJETIVOS

Art. 5º Os objetivos desta estratégia incluem:

- I - Alinhar a utilização de serviços de computação em nuvem aos objetivos estratégicos da FBN;
- II - Direcionar decisões relativas à contratação e utilização de serviços de computação em nuvem na FBN;
- III - Priorizar soluções que otimizem os recursos operacionais de serviços de computação em nuvem, mantendo a segurança e a conformidade;
- IV - Aumentar a agilidade e a capacidade de resposta da FBN, acelerando o lançamento de novos projetos e protótipos;
- V - Ampliar as capacidades de entrega de soluções de TI da FBN, reduzindo a necessidade de investimentos de capital para novos ativos de TI;
- VI - Garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) e política de segurança da informação da FBN;
- VII - Promover a capacitação contínua em tecnologias de serviços de computação em nuvem para os servidores da FBN; e
- VIII - Monitorar o desempenho das soluções que utilizam serviços de computação em nuvem, ajustando estratégias para alinhar com os objetivos estratégicos da FBN.

Art. 6º A Coordenação de Tecnologia da Informação (COTI) será a unidade responsável por coordenar a implementação desta estratégia, assegurando o alinhamento com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) vigente e outras políticas relacionadas.

CAPÍTULO IV DIRETRIZES PARA A ESTRATÉGIA

Art. 7º Diretrizes deverão ser observadas pela FBN ao adotar soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Seção I

Da Identificação das Necessidades do Negócio

Art. 8º A FBN deve identificar e avaliar as necessidades de negócio antes da contratação de software e de serviços de computação em nuvem, determinando quais sistemas, aplicações, dados e serviços utilizarão esses serviços.

Parágrafo único. Deve-se determinar quais sistemas, aplicações, dados e serviços precisam ser movidos para a nuvem, como eles serão acessados e quais recursos computacionais e de armazenamento serão necessários.

Seção II

Da Seleção dos Modelos Adequados

Art. 9º A FBN deve avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, privada, híbrida) são mais adequados aos requisitos de negócio.

Parágrafo único. Quando viável, deve-se priorizar a adoção de serviços de computação em nuvem, como PaaS e SaaS, em nuvem pública para melhor escalabilidade, flexibilidade e eficiência de custos.

Seção III

Da Avaliação dos Possíveis Fornecedores

Art. 10º Os estudos técnicos preliminares devem abranger o levantamento dos possíveis fornecedores aptos ao atendimento dos requisitos de negócio, de forma a garantir que exista uma quantidade mínima de fornecedores com experiência e que atendam aos requisitos necessários ao atendimento da demanda.

Parágrafo único. A avaliação incluirá critérios de segurança, conformidade, disponibilidade, suporte técnico, custo de migração e custo de capacitação.

Art. 11º A FBN deve obter acesso a serviços de suporte técnico especializado oferecidos pelos provedores de serviços de computação em nuvem, a fim de assegurar que o uso das plataformas de nuvem contratadas esteja alinhado às melhores práticas de arquitetura e segurança recomendadas pelos próprios fornecedores.

Seção IV

Da Definição de Requisitos de Segurança

Art. 12º A FBN deve cumprir os requisitos de segurança para serviços de computação em nuvem conforme estabelecidos na Instrução Normativa nº 5 do GSI/PR, de 30 de agosto de 2021, e nas diretrizes da Política de Segurança da Informação FBN, de 30 novembro de 2022.

Seção V

Do Estabelecimento de uma Política de Governança

Art. 13º A política de governança deve abranger a identificação e classificação de dados, controle de acesso, gerenciamento de configuração e, quando for o caso, monitoramento das atividades em nuvem, de modo a

garantir que os serviços a serem contratados sejam executados em conformidade com os padrões adotados pela FBN.

Seção VI

Das Diretrizes de Uso Seguro de Software e de Serviços de Computação em Nuvem

Art. 14º Os fornecedores de Serviços Técnicos de Intermediação para Nuvens Públicas deverão observar as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), no tratamento dos dados pessoais ou sensíveis, em especial quanto à finalidade, boa-fé e demais princípios inscritos no art. 6º da LGPD.

Art. 15º Não poderão ser tratadas em ambiente de nuvem pública informações e cargas de trabalho classificadas em grau de sigilo (reservadas, secretas e ultrassecretas), conforme o Decreto nº 7.724, de 16 de maio de 2012, nem documentos preparatórios que possam originar informações classificadas em grau de sigilo.

Art. 16º As cargas de trabalho tratando informações com restrição de acesso, conforme previsto na legislação, poderão ser mantidas em ambiente de nuvem pública da FBN, conforme avaliação realizada pela área técnica.

Art. 17º Os dados da FBN tratados em serviços de computação em nuvem devem ser armazenados em data centers localizados no território brasileiro, sendo permitido o tratamento de dados em data centers fora do território nacional apenas quando existir uma cópia de segurança atualizada armazenada em data centers no Brasil, conforme estabelecido pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Seção VII

Da Avaliação Quanto às Condições Mínimas de Infraestrutura de TIC da FBN para Utilizar Serviços de Computação em Nuvem

Art. 18º A FBN deve garantir conectividade estável e com largura de banda suficiente para utilização dos serviços de computação em nuvem, de acordo com requisitos técnicos e de negócio.

Seção VIII

Da Definição de Diretrizes de Governança para o Uso da Nuvem

Art. 19º A FBN deve definir papéis e responsabilidades para as áreas de TI e de negócios, responsável por:

- I - Padronizar a utilização dos serviços de computação em nuvem;
- II - Definir e implementar controles para o uso dos serviços de computação em nuvem alinhados a avaliações de risco;
- III - Definir e implementar estratégias de gestão financeira (FINOPS) para otimizar os custos e investimentos em serviços de computação em nuvem;
- IV - Desenvolver planos de capacitação em tecnologias de serviços de computação em nuvem para as equipes técnicas da COTI; e
- V - Identificar oportunidades de melhoria (aumento de eficiência, diminuição de custo) na utilização de serviços de computação em nuvem.

Art. 20º O modelo de governança e operação da plataforma de nuvem deverá seguir as seguintes orientações:

- I - As decisões sobre a arquitetura dos sistemas em nuvem serão de responsabilidade dos servidores da FBN, que contarão com o suporte técnico especializado dos provedores de serviços de computação em nuvem ou através de contratos específicos voltados para a assistência em arquitetura; e
- II - As atividades operacionais de rotina devem ser realizadas prioritariamente por equipes terceirizadas contratadas especificamente para suporte operacional.

Seção IX

Do Estabelecimento dos Princípios Norteadores da Estratégia

Art. 21º A FBN deve adotar os seguintes princípios norteadores da estratégia:

- I - *Cloud first*;
- II - Transferir as aplicações de sistemas locais para a nuvem, quando tecnicamente viável;
- III - Modernização de aplicações utilizando melhores práticas de utilização de serviços de computação em nuvem;
- IV - Desenvolvimento de novas aplicações usando preferencialmente a abordagem *Cloud-Native*;
- V - Emprego de até dois provedores principais de serviços de computação em nuvem, escolhidos por sua importância estratégica, com a opção de utilizar um terceiro provedor adicional conforme necessário para atender a demandas específicas ou complementares; e
- VI - Escolha do provedor de serviços de computação em nuvem por tipo de tecnologia e não por aplicação específica

Parágrafo único. Na aquisição de serviços ou produtos de infraestrutura de computação deve ser priorizada a solução de ambiente em nuvem, a fim de garantir benefícios ao órgão, salvo quando demonstrada sua inviabilidade, técnica ou econômica, em estudo técnico preliminar da contratação, segundo as diretrizes da Instrução Normativa SGD/MGI nº 94.

Seção X

Alinhamento com outros Planos Estratégicos

Art. 22º Esta estratégia deve estar alinhada com os seguintes planos:

- I - Planejamento Estratégico Institucional;
- II - Plano Diretor de Tecnologia da Informação e Comunicação;
- III - Plano de Contratações Anual; e
- IV - Plano de Preservação Digital;

Seção XI

Estabelecimento de Linhas de Base e Metas de Benefícios/Resultados Esperados

Art. 23º A FBN deve definir linhas de base e metas de benefícios/resultados esperados objetivando maior agilidade, redução de custos, resiliência e maior segurança.

Seção XII

Das Considerações Sobre Capacitação da Equipe

Art. 24º A FBN deve investir na capacitação contínua dos servidores em novas tecnologias e metodologias de trabalho, reconhecendo a importância de uma equipe bem-preparada para gerenciar, operar ou utilizar os recursos de software e de serviços em nuvem.

Seção XIII

Das Considerações Sobre Portabilidade e Interoperabilidade Entre Sistemas, Dados e Serviços

Art. 25º A FBN deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor (*lock-in*) e, sempre que possível, devem ser realizadas ações preventivas antes ou durante a adoção de software ou da execução dos serviços em nuvem, a exemplo de:

- I - Adotar padrões tecnológicos interoperáveis;
- II - Avaliar se o uso de tecnologias e ferramentas proprietárias poderá dificultar a portabilidade de aplicações e de dados entre nuvens de diferentes provedores; e
- III - Considerar a contratação de mais de um provedor de nuvem como contingência.

Seção XIV

Requisitos Regulatórios e de Conformidade

Art. 26º A FBN deve considerar os requisitos regulatórios e de conformidade para o uso seguro de software e serviços de computação em nuvem no âmbito da fundação e da administração pública.

Seção XV

Indicação da Estratégia de Saída

Art. 27º A FBN deve considerar a análise de dependências e aspectos de portabilidade (backup, redundância, contratos de apoio, retorno para a infraestrutura local, etc.). No caso de saída do serviço de computação em nuvem, deve ser realizado o planejamento dos custos de saída.

Seção XVI

Análise de Riscos

Art. 28º A FBN deve considerar as diretrizes de gerenciamento de riscos constantes no modelo de contratação de software e de serviços de computação em nuvem estabelecidos na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

CAPÍTULO V

DA DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 29º A FBN trata os requisitos para uso seguro de computação em nuvem visando promover alta disponibilidade e aumento de desempenho das soluções de TI, bem como de resiliência dos dados, com base nos princípios da segurança da informação, corroborando com a garantia de continuidade do negócio, interoperabilidade dos dados na execução de políticas públicas, tempestividade no suporte às iniciativas do Governo Digital, otimização dos custos de infraestrutura e de serviços e redução do tempo para disponibilização de recursos.

Seção I

Do Tratamento das Informações no Ambiente de Nuvem

Art. 30º Informações públicas podem ser tratadas em ambiente de nuvem, considerando a legislação em vigor e os riscos de segurança da informação.

Art. 31º É vedado o tratamento em ambiente de nuvem de informação classificada em grau de sigilo segundo as hipóteses previstas na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), bem como de documento preparatório que possa originar informação classificada.

Art. 32º Informações restritas podem ser tratadas em ambiente de nuvem, desde que sejam considerados os riscos de segurança da informação e a legislação vigente sobre:

- I - informações com restrição de acesso previstas em hipóteses legais de sigilo e de segredo de justiça;
- II - material de acesso restrito regulado pelo próprio órgão;
- III - informação pessoal relativa à intimidade, vida privada, honra e imagem, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD); e
- IV - documento preparatório não previsto no art. 31º.

Art. 33º Antes de transferir os sistemas para um provedor de serviço de nuvem, deve-se observar, no mínimo, as seguintes condições:

- I - implementação de, no mínimo, os controles já existentes no ambiente atual *on-premises*; e
- II - realização de análise de riscos da migração da solução para o ambiente de computação em nuvem pela COTI, com participação da unidade gestora da solução de tecnologia da informação.

Art. 34º A unidade custodiante da informação deve analisar a necessidade de criptografar as informações que se enquadram no art. 32º, tendo por base os requisitos legais, os riscos, o nível de criticidade, os custos e os benefícios implicados.

Seção II

Do Armazenamento das Informações no Ambiente de Nuvem em Outros Países

Art. 35º O armazenamento em nuvem de dados e informações produzidos ou custodiados pela FBN em outros países deverá seguir as diretrizes da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

Parágrafo único. No caso de tratamento de dados pessoais, também deverão ser observadas as diretrizes da Lei nº 13.709, de 2018 e da Política de Privacidade e Proteção de Dados Pessoais (PPDP) da FBN.

Seção III

Da utilização de ambiente de nuvem por cargas de trabalho

Art. 36º Para cada carga de trabalho (*workload*) que utilizar a plataforma de nuvem, deverão ser realizadas as seguintes ações:

- I - Um estudo de saída da nuvem;
- II - Definição dos indicadores *Recovery Point Objective* (RPO) e *Recovery Time Objective* (RTO) em conformidade com a política de backup da FBN;

- III - A definição e aprovação de um orçamento;
- IV - Uma avaliação de risco de segurança da informação; e
- V - A definição e documentação de arquitetura levando em consideração os padrões de arquitetura definidos pela COTI.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 37º Aplica-se ao ambiente de computação em nuvem da FBN o modelo de responsabilidade compartilhada nos diferentes níveis mínimos de serviço (SLAs), conforme detalhamento registrado no respectivo contrato de aquisição, cabendo:

- I - Ao provedor - manter a segurança do ambiente de nuvem, por meio da proteção à infraestrutura que engloba hardware, software, redes, instalações físicas, storage, datacenter e servidores virtuais;
- II - À COTI - primar pela segurança da informação, mediante o gerenciamento das aplicações, bancos de dados, sistemas operacionais, identidade e acesso, regras de firewall e atualizações para a segurança;
- III - Ao usuário - cumprir as diretrizes emanadas da Política de Segurança da Informação da FBN; e
- IV - Ao provedor e integrador dos serviços de computação em nuvem – manter o alinhamento com os normativos vigentes e operar de acordo com as melhores práticas de segurança.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 38º Esta estratégia, bem como os documentos gerados a partir dela, deverão ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas políticas e normas da FBN ou quando considerada necessária pelo Comitê de Governança Digital da FBN, assegurando que a estratégia permaneça relevante e eficaz.

Art. 39º Os casos omissos e não abordados neste documento serão analisados pelo Comitê de Governança Digital da FBN.

Art. 40º Esta norma entra em vigor a partir da data de sua publicação.