Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN)
Comitê de Governança Digital (CGD)
Comitê de Segurança da Informação (COSEG)

NC 14 POSIN

Estratégia de uso de Software e Serviços de Computação em Nuvem

Brasília, abril de 2025

IPHAN Instituto do Patrimônio Histórico e Artístico Nacional

MINISTÉRIO DA CULTURA

INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL

Leandro Antônio Grass Peixoto

Presidente

COMITÊ DE GOVERNANÇA DIGITAL

Américo Arantes Ferreira Nogueira

Coordenador-Geral de Tecnologia da Informação (CGTI)

Adriana Fátima Bortoli Araújo

Diretora do Departamento de Planejamento e Administração (DPA)

APOIO TÉCNICO PARA ELABORAÇÃO E REVISÃO

Ana Cristina França de Queiroz Cavalcanti Lima

Analista I

Sérgio Porto Carneiro

Chefe de Divisão de Governança e Projetos de Tecnologia da Informação

Paulo Alves de Azevedo Neto

Analista I

André Megale Melo

Coordenador de Infraestrutura Tecnológica

Waldyr Lima Junior

Analista em Tecnologia da Informação

Índice

1. Propósito

Esta norma complementar à Política de Segurança da Informação (POSIN) tem como objetivo regulamentar as diretrizes, os controles e os procedimentos para a contratação, uso, monitoramento e descontinuidade de serviços de computação em nuvem no âmbito do Instituto do Patrimônio Histórico e Artístico Nacional (Iphan).

Sua elaboração fundamenta-se nas disposições legais, normativas e técnicas aplicáveis à Administração Pública Federal, incluindo a legislação de proteção de dados, as orientações do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), bem como em normas internacionais de referência em segurança da informação.

As referências legais, normativas e de boas práticas consideradas estão consolidadas no Tópico 4 – Referência Legal e de Boas Práticas desta norma complementar, que serve de base para garantir a conformidade, a integridade, a disponibilidade e a confidencialidade das informações tratadas em ambientes de computação em nuvem utilizados pelo IPHAN.

CLASSE	IDENTIFICAÇÃO	DESCRIÇÃO	APROVAÇÃO
Norma Complementar	NC/14 POSIN [V1]	Trata-se da versão base da Norma Complementar que trata do tema de utilização de serviços em nuvem.	x

2. Escopo e Público-Alvo

A Política de Gestão de Credenciais de Acesso visa estabelecer os parâmetros mínimos para as credenciais de contas de usuário comum, contas de acesso privilegiado e contas de serviço do Instituto do Patrimônio Histórico e Artístico Nacional (Iphan), além dos controles de segurança aplicadas às credenciais, seu prazo de expiração e nível de complexidade. Adotar-se-á a todos as credenciais de acesso aos ambientes virtuais, assim como aos ambientes físicos da autarquia.

Esta norma complementar NC14 deve ser observada de maneira complementar à Norma Complementar 04/POSIN – Gestão e Controle de Acesso.

Aplica-se à todas as unidades e departamentos que compõem a estrutura regimental do Iphan e, consequentemente, a todos os seus usuários de recursos de Tecnologia da Informação.

3. Termos e Definições

COMPUTAÇÃO EM NUVEM (CLOUD COMPUTING) - Modelo de fornecimento de serviços de Tecnologia da Informação (TI), baseado no uso de recursos computacionais, como servidores, armazenamento e redes, disponibilizados por meio de internet, com o objetivo de permitir a utilização de recursos sob demanda, de forma escalável e sob modelos de pagamento conforme o uso.

NUVEM DE GOVERNO - infraestrutura de nuvem privada ou comunitária gerida exclusivamente por órgãos ou empresas públicas.

NUVEM PRIVADA - infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade pode ser do próprio órgão ou de empresas públicas com finalidade específica relacionada à tecnologia da informação. O modelo de nuvem privada admite o uso de recursos computacionais de provedores de nuvem pública somente se assegurado o isolamento lógico e físico desses recursos, no ambiente do próprio órgão ou de empresas públicas, e não se configurando como uso de Nuvem Pública.

NUVEM PÚBLICA OU EXTERNA - infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de órgãos públicos, empresas privadas ou de ambos.

NUVEM HÍBRIDA - infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.

PROVEDOR DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM (PROVEDOR EM NUVEM) - Entidade responsável pela oferta de serviços de computação em nuvem, incluindo, mas não se limitando a, fornecimento de infraestrutura (IaaS), plataforma (PaaS) e software (SaaS), conforme os requisitos de segurança e regulamentação estabelecidos.

SERVIÇOS DE INFRAESTRUTURA COMO SERVIÇO (IAAS) - Modelo de computação em nuvem em que os recursos de infraestrutura, como servidores, armazenamento e redes, são fornecidos aos clientes de maneira virtualizada, permitindo a instalação e o gerenciamento de sistemas operacionais e aplicativos.

SERVIÇOS DE PLATAFORMA COMO SERVIÇO (PAAS) - Modelo de computação em nuvem em que são oferecidas plataformas para o desenvolvimento, gerenciamento e execução de aplicativos, sem que o usuário precise gerenciar a infraestrutura subjacente.

SERVIÇOS DE SOFTWARE COMO SERVIÇO (SAAS) - Modelo de computação em nuvem em que o software e as aplicações são fornecidos como um serviço, acessado via internet, permitindo que o usuário utilize os aplicativos sem se preocupar com a gestão da infraestrutura ou da plataforma.

GOVERNANÇA DE TI - Conjunto de processos, políticas e práticas que visam assegurar que os recursos de TI, incluindo os serviços de computação em nuvem, sejam utilizados de maneira eficiente, segura, conforme as normas legais e regulatórias e em alinhamento com os objetivos institucionais do IPHAN.

SEGURANÇA DA INFORMAÇÃO - Conjunto de práticas e medidas adotadas para proteger a confidencialidade, integridade e disponibilidade das informações processadas e armazenadas no ambiente de computação em nuvem, além de garantir a conformidade com a legislação vigente e os requisitos regulatórios.

CONFIDENCIALIDADE - Propriedade que assegura que a informação seja acessada apenas por pessoas ou sistemas autorizados, protegendo-a contra acessos não autorizados.

INTEGRIDADE - Propriedade que assegura que a informação não seja alterada ou corrompida durante o processamento ou transmissão, garantindo a precisão e consistência dos dados.

DISPONIBILIDADE - Propriedade que assegura que a informação e os recursos de TI estejam acessíveis e utilizáveis sempre que necessários, minimizando os tempos de inatividade ou interrupções.

BACKUP - Processo de criação de cópias de segurança de dados e informações armazenadas no ambiente de computação em nuvem, com o objetivo de protegê-las contra perda acidental ou corrupção, e assegurar a continuidade das operações.

CRIPTOGRAFIA - Técnica de proteção de dados através da conversão de informações em um formato codificado, de modo que apenas indivíduos ou sistemas autorizados possam acessá-las e compreendê-las.

4. Referência legal e de boas práticas

NORMA	DESCRIÇÃO
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50
Decreto n° 9.637/2018	Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação
Decreto n° 11.856/2023	Institui a Política Nacional de Cibersegurança (PNCiber) e o

	Comitê Nacional de Cibersegurança (CNCiber).
Portaria SGD/MGI nº 5.950/2023	A Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, estabelece um modelo de contratação de software e serviços de computação em nuvem para os órgãos e entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal. Além disso, permite, de forma excepcional, a não aplicação das diretrizes do modelo, desde que solicitada via ofício e com autorização prévia da Secretaria de Governo Digital
Instrução Normativa GSI/PR nº 5/2021	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.
Estratégia de Governo Digital (EGD) - Decreto nº 10.332/2020	Direciona a adoção de soluções digitais, incluindo computação em nuvem, como forma de modernizar a gestão pública. Estimula o uso de infraestruturas mais seguras, escaláveis e sustentáveis.
Instrução Normativa SGD/ME nº 1/2019 (Atualizada pela IN nº 3/2022)	Estabelece regras para a contratação e uso de serviços de computação em nuvem no governo federal. Define critérios como localização de dados, segurança da informação, responsabilidade sobre dados sensíveis e conformidade com a LGPD.
Decreto nº 10.046/2019 – Compartilhamento de Dados no Poder Executivo Federal	Trata da governança e do compartilhamento de dados, o que impacta diretamente a adoção de nuvem e proteção de informações.
Manual de Computação em Nuvem da Secretaria de Governo Digital (SGD/ME)	Orienta sobre: Modelos de serviço (IaaS, PaaS, SaaS); Modelos de implantação (pública, privada, híbrida);

	Gestão de riscos e análise de impacto; Controle de acesso e criptografia; Definições de responsabilidades entre o órgão e o provedor.
Normas Técnicas Complementares (ABNT/NBR ISO/IEC 27001 e 27002)	Referências para gestão da segurança da informação, especialmente úteis na definição de requisitos técnicos e operacionais para ambientes em nuvem.

5. Requisitos para Adoção de Serviços em Nuvem

A adoção de serviços de computação em nuvem pelo IPHAN deverá seguir rigorosos critérios de segurança, conformidade e eficiência, conforme descrito abaixo. Seguem os requisitos essenciais a serem cumpridos para a implementação e utilização de serviços em nuvem, visando garantir a integridade, confidencialidade e disponibilidade das informações, além de atender à governança institucional.

5.1. Planejamento e Análise de Necessidades

Antes de adotar qualquer serviço de computação em nuvem, o IPHAN deverá realizar um planejamento detalhado, incluindo a análise das necessidades institucionais, os objetivos a serem alcançados, e a definição de quais serviços são mais adequados para as operações da instituição. Este planejamento deve abranger:

- Avaliação das funcionalidades e benefícios do serviço de nuvem a ser contratado.
- Determinação de qual modelo de nuvem (privada, pública ou híbrida) será adotado.
- Análise de custos envolvidos, incluindo o custo-benefício da migração para a nuvem.
- Definição de objetivos claros de segurança da informação e governança.
- Análise/Definição de diretrizes para evitar lock in na migração de uma plataforma de nuvem para outra.

5.2. Avaliação de Provedores de Serviços de Nuvem

O IPHAN deverá avaliar criteriosamente os provedores de serviços de computação em nuvem com base nos seguintes critérios:

- Segurança e Conformidade: O provedor deve demonstrar conformidade com as normas brasileiras e internacionais de segurança da informação, incluindo, mas não se limitando a, a Lei Geral de Proteção de Dados (LGPD), e outras regulamentações aplicáveis.
- Histórico de Confiabilidade: O provedor deve ter um histórico comprovado de entrega de serviços de alta qualidade, com baixa taxa de incidentes e interrupções.
- Certificações de Segurança: O provedor deve possuir certificações relevantes, como ISO 27001, SOC 2, ISO/IEC 27017 – Segurança na Nuvem, ou outras certificações reconhecidas na área de segurança e proteção de dados.
- Acordos de Nível de Serviço (SLAs): Os SLAs devem ser claramente definidos e garantir a disponibilidade, performance e segurança dos serviços contratados, com penalidades previstas em caso de não cumprimento, além de serem definidos de acordo com o dado ou serviço mantido.

5.3. Avaliação de Segurança e Riscos

Antes de adotar um serviço de computação em nuvem, o IPHAN deverá realizar uma avaliação de riscos detalhada, que deve abranger:

- Análise de Vulnerabilidades: Identificação de possíveis vulnerabilidades de segurança no ambiente de nuvem, incluindo riscos relacionados ao armazenamento de dados sensíveis, uso indevido de credenciais e falhas na infraestrutura.
- Controle de Acesso: Definição de políticas claras de controle de acesso e autenticação de usuários, incluindo a implementação de autenticação multifatorial (MFA) para proteger o acesso aos sistemas.
- Criptografia: Exigência de criptografia de dados em trânsito e em repouso, assegurando que todas as informações armazenadas na nuvem estejam protegidas contra acessos não autorizados.
- Autenticidade ou irretratabilidade: soluções com dados sensíveis ou que exigem uma segunda senha para efetivação de funcionalidades.

5.4. Conformidade Legal e Regulatória

O IPHAN deve garantir que todos os serviços de computação em nuvem adotados estejam em conformidade com a legislação brasileira e com as políticas internas

Desta forma, o provedor deve cumprir todas as exigências da LGPD no que diz respeito ao tratamento e proteção de dados pessoais, garantindo a privacidade e segurança dos dados sensíveis.

O serviço prestado pelo provedor não poderá contrariar as políticas internas de segurança da informação e comunicações, assegurando que os processos de adoção e uso da nuvem não contrariem as diretrizes estabelecidas na POSIN e em outras normas internas.

O IPHAN deve garantir que o provedor de nuvem tenha clareza quanto à localização física dos dados e à jurisdição em que eles estarão armazenados, evitando a transferência de dados para países ou regiões que possam não oferecer um nível adequado de proteção.

5.5. Governança e Monitoramento

A governança de TI deve ser uma prioridade na adoção de serviços de computação em nuvem. O IPHAN deverá adotar as seguintes práticas:

- Gestão de Contratos e SLAs: A gestão contínua dos contratos e SLAs com provedores de nuvem deve ser realizada pela área de governança de TI, garantindo que os termos acordados sejam cumpridos.
- Monitoramento Contínuo: O IPHAN deverá implementar mecanismos de monitoramento para avaliar o desempenho e a segurança dos serviços em nuvem, incluindo a verificação da disponibilidade, integridade e confidencialidade dos dados armazenados.
- Auditoria Regular: Auditorias regulares devem ser realizadas para garantir que as práticas de segurança e conformidade estão sendo seguidas, além de identificar e corrigir falhas antes que se tornem problemas críticos.
- O Subcomitê de Segurança da Informação (COSEG) poderá instituir núcleos e grupos de trabalho com o intuito de obter a segurança da informação sobre as nuvens utilizadas no IPHAN.

5.6. Continuidade de Negócios e Recuperação de Desastres

É essencial garantir a continuidade das operações e a recuperação de desastres nos serviços de nuvem adotados. Para isso, o IPHAN deve ter:

- Plano de Recuperação de Desastres (DRP): O provedor de nuvem deve apresentar um plano de recuperação de desastres que cubra a restauração dos serviços e dados em caso de incidentes graves.
- Backup de Dados: O provedor deve garantir que dados críticos sejam periodicamente copiados e armazenados em locais seguros, com a possibilidade de recuperação rápida e eficiente em caso de falhas ou perdas.
- Testes Regulares: O IPHAN deve realizar testes regulares de recuperação de desastres para garantir que os planos e processos definidos sejam eficazes em situações reais.

5.7. Treinamento e Capacitação

A equipe do IPHAN envolvida na gestão de serviços em nuvem deve ser adequadamente treinada sobre as ferramentas, processos e boas práticas de segurança aplicáveis. O treinamento deve incluir:

- Aconselhamento sobre a importância da segurança em nuvem.
- Capacitação sobre o uso correto de plataformas e ferramentas de nuvem, incluindo controle de acessos.
- Conscientização sobre a proteção de dados pessoais e sensíveis.
- Procedimentos de resposta a incidentes e gestão de riscos.

6. Funções e responsabilidades dos agentes

Os agentes e unidades envolvidas no processo de adoção, gestão e monitoramento dos serviços de computação em nuvem no IPHAN, possuem funções com foco na segurança da informação, conformidade regulatória e eficiência operacional. Cada agente ou unidade tem um papel definido no âmbito da Política de Segurança da Informação (POSIN) e nas diretrizes de governança digital.

6.1. Gestores da Informação

Os gestores da informação são agentes públicos formalmente responsáveis pela gestão dos serviços e das informações disponibilizadas no ambiente de computação em nuvem, sendo de sua competência garantir que os dados e os serviços estejam em conformidade com as diretrizes estabelecidas pelo IPHAN.

São atribuições dos gestores da informação:

a) Solicitar, formalmente, a inclusão de informações e serviços no ambiente de computação em nuvem;

b) Solicitar, formalmente, a remoção de informações e serviços no ambiente de computação em nuvem;

c) Autorizar a solicitação de inclusão ou remoção de serviços e informações feitas pela Coordenação-Geral de Tecnologia da Informação (CGTI);

d) Validar, negocialmente, a inclusão ou remoção de serviços e informações eventualmente solicitadas pela CGTI.

6.2. Gestor de Segurança da Informação

O gestor de segurança da informação é o agente responsável por coordenar e supervisionar as práticas de segurança da informação no uso de serviços de computação em nuvem, garantindo a proteção e conformidade dos dados processados, armazenados ou compartilhados.

São atribuições do gestor de segurança da informação:

a) Instituir e coordenar a equipe responsável pela elaboração e revisão do ato normativo sobre o uso seguro de computação em nuvem;

b) Supervisionar a aplicação do ato normativo sobre o uso seguro de computação em nuvem, garantindo que as práticas de segurança sejam seguidas corretamente;

c) Assegurar a comunicação contínua com o provedor de serviços de nuvem para garantir que os controles e níveis de serviço acordados sejam cumpridos de maneira eficaz;

d) Supervisionar a aplicação das medidas corretivas pelo provedor de nuvem, em caso de eventuais desvios ou falhas no serviço;

e) Comunicar incidentes cibernéticos informados pelo provedor de serviços de nuvem aos órgãos competentes, conforme a relevância e a gravidade dos incidentes;

f) Divulgar e promover o ato normativo sobre o uso seguro de computação em nuvem às partes interessadas dentro e fora da organização.

6.3. Comitê de Governança Digital

O Comitê de Governança Digital -CGD é o órgão responsável pela supervisão estratégica e pela definição das diretrizes gerais para a governança digital no IPHAN, incluindo a gestão de serviços de computação em nuvem.

São atribuições do Comitê de Governança Digital:

A) Propor e acompanhar a execução do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) no que couber computação em nuvem.

a) Estabelecer diretrizes estratégicas sobre o uso de serviços de computação em nuvem no IPHAN, alinhadas com as políticas digitais e de segurança da informação da instituição;

b) Aprovar as iniciativas e projetos relacionados ao uso de computação em nuvem, incluindo a validação dos aspectos de segurança, privacidade, financeiro e conformidade legal;

c) Coordenar e revisar as políticas internas de governança digital para garantir que o uso de serviços de nuvem atenda aos objetivos estratégicos da instituição.

d) Acompanhar indicadores de desempenho e resultados das iniciativas em nuvem, promovendo ajustes sempre que necessário.

6.4. Subcomitê de Segurança da Informação

O Subcomitê de Segurança da Informação atua como uma instância consultiva e executiva na implementação de políticas de segurança da informação no uso de serviços de computação em nuvem, sendo fundamental para assegurar a proteção dos dados da instituição.

São atribuições do Subcomitê de Segurança da Informação:

a) Estabelecer os países e regiões nos quais os dados e informações custodiados pelo IPHAN podem ser armazenados em soluções de computação em nuvem, considerando requisitos de segurança e jurisdição;

b) Definir os requisitos criptográficos mínimos para o armazenamento de dados e informações do IPHAN em soluções de computação em nuvem, com o objetivo de garantir a confidencialidade e integridade das informações;

c) Analisar, em caráter conclusivo, as minutas de elaboração e revisão do ato normativo sobre o uso seguro de computação em nuvem, garantindo que todas as medidas de segurança sejam implementadas corretamente;

d) Avaliar a adequação dos provedores de nuvem à legislação vigente e às exigências de segurança e conformidade estabelecidas pelo IPHAN.

e) Garantir que os projetos em nuvem estejam em conformidade com a POSIN institucional, com foco em princípios de confidencialidade, integridade, disponibilidade e autenticidade e requisitos mínimos de controle de acesso, criptografia e monitoramento.

f) orientar às unidades do IPHAN através de normativos quanto ao uso de técnicas de anonimizações e pseudominizações.

6.5. Coordenação-Geral de Tecnologia da Informação (CGTI)

A Coordenação-Geral de Tecnologia da Informação (CGTI) é a unidade operacional responsável pela gestão técnica e estratégica dos serviços de computação em nuvem no IPHAN.

São atribuições da CGTI:

a) Gerir a implementação e a manutenção dos serviços de computação em nuvem adotados pelo IPHAN, incluindo a negociação com os provedores e a definição de requisitos técnicos;

b) Coordenar a integração dos serviços em nuvem com as infraestruturas de TI existentes no IPHAN, garantindo a continuidade dos processos de negócio;

c) Monitorar o desempenho e a segurança dos serviços em nuvem, realizando auditorias periódicas e garantindo que os contratos e SLAs sejam cumpridos;

d) Apoiar os gestores da informação na solicitação e validação de serviços e informações a serem incluídos ou removidos do ambiente de nuvem;

e) Fornecer suporte contínuo para a implementação de medidas corretivas ou de melhoria, caso sejam identificados problemas ou riscos no ambiente de nuvem.

7. Plano de migração e uso do ambiente de computação em nuvem

Esta seção descreve as diretrizes e os procedimentos para a migração e o uso contínuo de serviços no ambiente de computação em nuvem no IPHAN, com foco na segurança, eficiência operacional e conformidade com as políticas de segurança da informação.

7.1. Objetivo do Plano de Migração

O plano de migração e uso do ambiente de computação em nuvem tem como objetivo garantir que serviços, dados e sistemas do IPHAN que sejam transferidos para o ambiente de nuvem, o façam de forma controlada, segura e eficiente. O plano deve assegurar que a migração não comprometa a continuidade dos serviços e que todos os requisitos de segurança e conformidade sejam atendidos, bem como a migração entre plataformas de nuvens diferentes.

7.2. Etapas do Plano de Migração

A migração para o ambiente de computação em nuvem deve ser realizada de forma planejada e estruturada, com as seguintes etapas:

8. Planejamento Inicial

Antes de iniciar a migração para a nuvem, o IPHAN deve realizar um planejamento detalhado que envolva as seguintes ações:

1. Avaliação de Necessidades: Identificar quais serviços e dados serão migrados para a nuvem, levando em consideração requisitos de desempenho, segurança, custo, tempo, capacidade técnica contratual para suporte e conformidade.
2. Seleção dos modelos adequados: é necessário avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, nuvem privada, nuvem híbrida etc.) melhor se adequam aos requisitos de negócio. Caso o órgão ou entidade não possua maturidade suficiente na contratação de serviços em nuvem ou possua impedimentos técnicos ou normativos para migração de alguns workloads, é recomendável sempre dar preferência à adoção de uma abordagem estratégica de nuvem híbrida. Caso o órgão possua maturidade e já tenha concluído que a demanda prevista pode ser atendida integralmente por meio de serviços em nuvem, uma abordagem completa, incluindo as demandas de migração do ambiente on-premises para a nuvem pode ser adotada;
3. Avaliação dos possíveis fornecedores: 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. Fatores como segurança, conformidade, disponibilidade e suporte técnico devem ser considerados nessa avaliação;
4. Avaliação de Riscos: Identificar e avaliar os riscos associados à migração, incluindo riscos técnicos, de segurança, legais e operacionais, e definir estratégias para mitigá-los.

8.1. Preparação para a Migração

Após o planejamento inicial, o IPHAN deve se preparar para a migração, incluindo as seguintes ações:

1. Definição de Recursos e Ferramentas: Selecionar as ferramentas e recursos necessários para realizar a migração (como softwares de backup e transferência de dados), além de definir as configurações de segurança no ambiente de nuvem.
2. Treinamento e Capacitação: Capacitar as equipes técnicas e de segurança envolvidas na migração para garantir que todos entendam as boas práticas de segurança, conformidade e gestão de dados na nuvem.
3. Elaboração de Plano de Contingência: Desenvolver um plano de contingência para garantir que, caso ocorra algum problema durante a migração, o processo possa ser revertido ou ajustado sem impactos significativos nos serviços.

8.2. Execução da Migração

A execução da migração deve ser feita de forma gradual e controlada para garantir que os serviços sejam transferidos sem interrupções significativas. Os dados, aplicativos e sistemas devem ser migrados para o ambiente de nuvem, com base no plano de migração previamente aprovado.

Após a migração testes para validar a integridade e o funcionamento dos dados e serviços devem ser realizados, visando:

- confiabilidade de funcionamento integral dos sistemas,
- confiabilidade da integração entre sistemas e
- integridade dos dados migrados.

8.3. Monitoramento Pós-Migração

Após a migração, o IPHAN deve monitorar continuamente o ambiente de nuvem para garantir que todos os serviços continuem operando corretamente. As ações incluem:

- Monitorar continuamente o desempenho dos serviços em nuvem para garantir que os níveis de serviço acordados sejam cumpridos.
- Realizar auditorias periódicas de segurança para garantir que os dados e serviços estejam protegidos contra ameaças e vulnerabilidades.
- Identificar qualquer risco emergente no novo ambiente e implementar medidas corretivas imediatamente.

8.4. Diretrizes para utilização de serviços de nuvem por tipo informação

Devem ser observadas as seguintes diretrizes:

1. informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;
2. informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e
3. 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, conforme o Anexo I desta Norma Complementar;
    b. o material de acesso restrito regulado pelo próprio órgão ou pela entidade;
    c. a informação pessoal relativa à intimidade, vida privada, honra e imagem; e
    d. o documento preparatório não previsto no inciso II do caput.

8.5. Uso Contínuo do Ambiente de Computação em Nuvem

Após a migração, o IPHAN deve garantir a gestão contínua do ambiente de nuvem para assegurar que ele continue a atender às necessidades operacionais e de segurança da instituição. O uso contínuo do ambiente de nuvem deve seguir as seguintes diretrizes:

8.6. Gerenciamento de Recursos

O gerenciamento eficiente dos recursos em nuvem é fundamental para garantir que o IPHAN aproveite ao máximo as vantagens da nuvem, como escalabilidade e flexibilidade. Isso inclui:

- Ajustar os recursos de computação e armazenamento de acordo com a demanda, para garantir que os serviços permaneçam eficientes e econômicos.
- Monitorar os custos associados ao uso de recursos na nuvem, identificando oportunidades para otimizar gastos sem comprometer a qualidade ou a segurança dos serviços.

8.7. Atualizações e Manutenção

A manutenção contínua do ambiente de nuvem é fundamental para garantir que os serviços permaneçam atualizados e seguros. Isso inclui:

- Implementação de Atualizações e Patches: Garantir que as atualizações de segurança, patches e novas versões dos serviços de nuvem sejam implementados de forma oportuna.
- Testes de Continuidade de Negócio: Realizar testes regulares de recuperação de desastres e continuidade de negócios para garantir que o IPHAN esteja preparado para eventuais falhas nos serviços de nuvem.

8.8. Descontinuação de Serviços em Nuvem

Caso o IPHAN decida descontinuar o uso de um serviço em nuvem ou mudar de provedor, um plano de descontinuação deve ser seguido, incluindo:

- Planejamento da Remoção de Dados: Garantir que todos os dados sejam removidos de forma segura e que a transferência de informações para o novo ambiente (se necessário) seja feita sem perdas ou compromissos de segurança.
- Comunicação com o Provedor: Negociar com o provedor de nuvem a remoção dos dados e a garantia de que todas as obrigações contratuais, de segurança e legais sejam cumpridas.

9. Necessidades Transitórias dos Contratos Vigentes de Serviços em Nuvem

Os contratos vigentes podem apresentar necessidades de adequação em relação aos serviços em nuvem, a fim de garantir a continuidade dos serviços durante o processo de migração para um novo ambiente de computação em nuvem, bem como a adequação e ajustes necessários nos termos contratuais. As necessidades transitórias visam assegurar que os contratos existentes sejam mantidos em conformidade, sem comprometer a qualidade ou segurança dos serviços durante a transição.

9.1. Identificação e Análise de Contratos Vigentes

Antes de iniciar o processo de migração ou a adoção de novos serviços de computação em nuvem, o IPHAN deve realizar um levantamento completo dos contratos vigentes relacionados a serviços em nuvem. Essa análise deve incluir a revisão de termos e condições, para identificar cláusulas que possam ser impactadas pela migração, como prazos, cláusulas de rescisão, garantias de segurança e níveis de serviço (SLA).

Além disso, é necessário verificar a conformidade dos contratos com as novas diretrizes de segurança, governança e proteção de dados, incluindo exigências como a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis.

Também é importante avaliar a continuidade dos serviços contratados durante a migração, ou se será necessário buscar alternativas para garantir a continuidade dos serviços de forma ininterrupta.

9.2. Ajustes Contratuais Necessários

Durante o processo de migração, ajustes podem ser necessários nos contratos vigentes para garantir que as obrigações e os serviços estejam alinhados com o novo ambiente de nuvem. Isso pode envolver a renegociação de termos contratuais, caso o contrato vigente não atenda às novas necessidades de segurança, desempenho ou conformidade, incluindo a modificação de prazos de serviço, níveis de segurança ou cláusulas relacionadas ao armazenamento e proteção de dados.

Os Acordos de Nível de Serviço (SLAs) também podem precisar ser ajustados de acordo com as necessidades do novo ambiente, garantindo que o provedor de serviços de nuvem cumpra os requisitos de disponibilidade, desempenho e segurança.

Além disso, caso o contrato vigente não contemple adequadamente as necessidades de backup ou planos de recuperação de desastres, é fundamental realizar ajustes para garantir a integridade e continuidade dos serviços durante a transição.

10. Alterações e revisões

Essa norma complementar será analisada criticamente a intervalos planejados de no máximo dois anos de acordo com o inciso V do Art. 5º da IN nº 5/2021, ou quando mudanças significativas ocorrerem, de modo a assegurar a sua contínua pertinência, adequação e eficácia.

O gerenciamento desta norma é realizado pelo Subcomitê de Segurança da Informação e Comunicação (COSEG), sob supervisão do Comitê de Governança Digital - CGD. As alterações e revisões serão submetidas a essas instâncias deliberativas de forma periódica ou sempre que verificada a necessidade de atualização de seu conteúdo por demandas internas ou por força de normativos externos.

Esta norma complementar de controle de acesso entra em vigor da data de sua publicação no Boletim Administrativo Eletrônico e será disponibilizada na íntegra no repositório eletrônico de normas de Segurança da Informação e Comunicações.

ANEXO 1 - QUADRO EXEMPLIFICATIVO DE TIPOS DESCRITIVOS DE INFORMAÇÃO

Obtido do Anexo da Instrução Normativa nº 5, de 30 de agosto de 2021.

Tipo	Descrição	
1. OSTENSIVA	Transparência Ativa	
	Transparência Passiva	
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1 Reservada - Prazo máximo de restrição de acesso de 5 anos	
	2.2 Secreta - Prazo máximo de restrição de acesso de 15 anos	
	2.3 Ultrassecreta - Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.	
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1 Sigilos Decorrentes de Direitos de Personalidade	
		3.1.1 Sigilo Fiscal
		3.1.2 Sigilo Bancário
		3.1.3 Sigilo Comercial
		3.1.4 Sigilo Empresarial
		3.1.5 Sigilo Contábil
	3.2 Sigilos de Processos e Procedimentos	
		3.2.1 Sigilo do Procedimento Administrativo Disciplinar em Curso
		3.2.2 Sigilo do Inquérito Policial
		3.2.3 Segredo de Justiça no Processo Civil
		3.2.4 Segredo de Justiça no Processo Penal
	3.3 Informação de Natureza Patrimonial	
		3.3.1 Segredo Industrial
		3.3.2 Direito Autoral
		3.3.3 Propriedade Intelectual de Programa de Computador
		3.3.3 Propriedade Industrial
4. PESSOAL	4.1. Pessoal - Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.	