



Autoridade Nacional de Proteção de Dados  
Conselho Diretor  
Comitê de Governança Digital

Brasília-DF, na data da assinatura.

REGISTRO DE REUNIÃO

1. DADOS DA REUNIÃO

|        |                  |
|--------|------------------|
| Número | 03/2025          |
| Data   | 15/05/2025       |
| Hora   | 14h30            |
| Local  | Videoconferência |

3. PAUTA

| ITEM | DESCRIÇÃO                                                              | SOLICITANTE |
|------|------------------------------------------------------------------------|-------------|
| 1    | ESTRATÉGIA DE USO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM – ANPD | CGTI        |

5. QUORUM

| Nome                             | Unidade              | Qualificação |
|----------------------------------|----------------------|--------------|
| Núbia Augusto de Sousa Rocha     | SG                   | Presidente   |
| Fabricio Guimarães Madruga Lopes | CGF                  | Titular      |
| Eduardo Lobato Pinheiro Neto     | Encarregado de Dados | Suplente     |
| Eduardo Gomes Salgado            | CGR II               | Titular      |
| Igor de Moura Leite Moreira      | CGTI                 | Titular      |
| Mariana Pires de Souza           | CGA                  | Suplente     |
| Mariana Almeida de Sousa Talouki | CGN                  | Suplente     |
| Gustavo Andrade Bruzzeguez       | CGTP                 | Titular      |

7. CONVIDADOS SEM DIREITO A VOTO

| Nome                      | Unidade |
|---------------------------|---------|
| Danyela de Oliveira Felix | SG      |
| Jeferson Dias Barbosa     | GABPR   |

|                                        |      |
|----------------------------------------|------|
| Jorge André Ferreira Fontelles de Lima | CGF  |
| Luciano Édipo Pereira da Silva         | CGTI |
| Rodrigo Vaz dos Santos                 | CGTI |

## 9. REGISTRO

| Item | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <p>Verificado o alcance do quórum de maioria absoluta dos membros, a Presidente do Comitê, Sra. Núbia Rocha, declarou aberta, às quatorze horas e trinta minutos, a 2ª Reunião Ordinária de 2025 do Comitê de Governança Digital da ANPD (CGD/ANPD), procedendo à introdução do item da pauta, destacando a importância da aprovação da Estratégia de Uso de Software e Serviços de Computação em Nuvem. Ressaltou que o documento foi encaminhado previamente para avaliação dos membros do colegiado e que tal estratégia constitui pré-requisito estabelecido pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) para que a ANPD possa manifestar interesse na adesão à contratação centralizada de soluções em nuvem, conduzida atualmente pela própria SGD. Acrescentou que, conforme normativo, faz-se necessário que o Comitê de Governança Digital (CGD) aprove a estratégia.</p> <p>Em seguida, a palavra foi concedida ao Coordenador-Geral de Tecnologia da Informação, Sr. Igor de Moura, que explanou sobre os fundamentos e diretrizes da referida estratégia, conforme disposto na Portaria SGD/MGI nº 5.950, de outubro de 2023, que regulamenta o modelo de contratação de software e serviços de computação em nuvem no âmbito da Administração Pública Federal. Informou, ademais, que prazo final para manifestação de interesse na adesão à solução por meio do Portal de Compras do Governo Federal é o dia 22 de maio de 2025, e que a estratégia deve estar aprovada previamente a esta data.</p> <p>Durante os debates, foi apresentado questionamento acerca da estratégia preferencial a ser adotada pelo órgão, especialmente no que se refere à priorização do modelo em nuvem.</p> <p>Encerrada as discussões e acatadas as sugestões de ajuste pontuais que foram feitas pelos participantes da reunião, a proposta foi submetida à deliberação e aprovada por unanimidade pelos membros presentes.</p> <p>A Presidente destacou que, conforme disposto na Resolução CD/ANPD nº 3, de 25 de janeiro de 2023, que instituiu o CGD/ANPD, a estratégia deverá ser apreciada pelo Comitê de Governança, Riscos e Controles (CIG), o que deve acontecer antes do dia 22 de maio.</p> <p>Não havendo outros assuntos a serem tratados, a Presidente agradeceu a participação de todos e declarou encerrada a reunião às 15h07.</p> |



Documento assinado eletronicamente por **Núbia Augusto de Sousa Rocha, Secretário(a)-Geral**, em 19/05/2025, às 10:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Eduardo Lobato Pinheiro Neto, Encarregado(a) pelo Tratamento de Dados Pessoais - Substituto(a)**, em 19/05/2025, às 11:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Fabício Guimarães Madruga Lopes, Coordenador(a)-Geral de Fiscalização**, em 19/05/2025, às 11:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Mariana Pires de Souza, Coordenador(a)-Geral de Administração - Substituto(a)**, em 19/05/2025, às 11:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Eduardo Gomes Salgado, Coordenador(a)-Geral de Relações Institucionais e Internacionais**, em 19/05/2025, às 14:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Igor de Moura Leite Moreira, Coordenador(a)-Geral**, em 19/05/2025, às 16:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Gustavo Andrade Bruzzeguez, Coordenador(a)-Geral - Substituto(a)**, em 19/05/2025, às 16:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Mariana Almeida de Sousa Talouki, Coordenador(a)-Geral - Substituto(a)**, em 19/05/2025, às 18:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0184672** e o código CRC **5FEEE6B3**.

# Estratégia de Uso de Software e Serviços de Computação em Nuvem – ANPD (Aprovado CGD/ANPD)

## 1. Disposições Gerais

A Estratégia de Uso de Software e de Serviços de Computação em Nuvem da Autoridade Nacional de Proteção de Dados (ANPD) tem por objetivo assegurar que a ANPD obtenha os resultados esperados com a computação em nuvem, ao mesmo tempo em que mitiga os riscos associados à adoção de novas tecnologias e modelos de contratação. Esta estratégia considera a natureza e as finalidades institucionais da ANPD – órgão que tem a missão de zelar pela proteção de dados pessoais – e está alinhada ao planejamento estratégico da Autoridade.

**Aplicabilidade:** Esta estratégia aplica-se a **novas contratações** de software e serviços de computação em nuvem no âmbito da ANPD, incluindo, mas não se limitando a:

- **Software** sob o modelo de licenciamento permanente de direitos de uso, cessão temporária de direitos de uso ou subscrição (Software como Serviço – *SaaS*);
- **Infraestrutura como Serviço (IaaS)**, englobando recursos de processamento, armazenamento e redes em nuvem;
- **Plataforma como Serviço (PaaS)** para desenvolvimento e implantação de aplicações na nuvem;
- **Serviços correlatos**, como suporte técnico a software em nuvem, operação e gerenciamento de recursos em nuvem, migração de dados/sistemas para nuvem, integração de serviços em nuvem e consultorias especializadas em software e/ou serviços de nuvem.

Conforme as diretrizes federais a adoção de computação em nuvem deve observar os princípios de segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade, bem como os preceitos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), garantindo privacidade e proteção aos dados pessoais sob custódia da ANPD. A segurança da informação aqui abrange a defesa cibernética, a segurança física e a proteção de dados organizacionais, assegurando a disponibilidade, integridade, confidencialidade e conformidade legal das informações tratadas.

## 2. Referências Normativas

No desenvolvimento e implementação desta estratégia, a ANPD observará as seguintes normas e diretrizes públicas (sem prejuízo de outros normativos aplicáveis):

- **Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023:** Estabelece o modelo de contratação de software e de serviços de computação em nuvem no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal;
- **Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021:** Dispõe sobre requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem por órgãos e entidades da Administração Pública Federal;
- **Decreto nº 9.637, de 26 de dezembro de 2018:** Institui a Política Nacional de Segurança da Informação, definindo princípios e diretrizes gerais a serem observados;
- **Decreto nº 10.641, de 2 de março de 2021:** Altera o Decreto nº 9.637/2018, dispondo sobre a governança da segurança da informação e incluindo disposições atualizadas relevantes;
- **Resolução do GSI/PR nº 1, de 11 de setembro de 2019:** Aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;
- **Portaria GSI/PR nº 93, de 26 de setembro de 2019:** Aprova o Glossário de Segurança da Informação, com definições importantes para o setor;
- **Decreto nº 10.222, de 5 de fevereiro de 2020:** Aprova a Estratégia Nacional de Segurança Cibernética (*E-Ciber*), a ser considerada nas iniciativas de computação em nuvem;
- **Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:** Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e entidades da APF, relevante para governança de segurança em nuvem;
- **Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021:** Dispõe sobre processos relacionados à gestão de segurança da informação nos órgãos e entidades da APF, incluindo aspectos de computação em nuvem;
- **Portaria SGD/MGI nº 852, de 28 de março de 2023:** Dispõe sobre o Programa de Privacidade e Segurança da Informação, com diretrizes que a ANPD, por sua missão, deve observar rigorosamente;

- **Demais legislações e normativos** de TIC, segurança da informação e proteção de dados pessoais aplicáveis, publicados por órgãos centrais (Secretaria de Governo Digital, GSI/PR, ANPD etc.), que venham a complementar esta estratégia.

### 3. Conceitos e Definições

Para os fins desta estratégia, adotam-se os seguintes conceitos, em conformidade com o glossário oficial de segurança da informação e computação em nuvem do SISP:

- **Computação em nuvem:** Modelo que possibilita o provisionamento e a utilização sob demanda de um conjunto compartilhável de recursos de TIC (por exemplo: servidores, armazenamento, redes, softwares e serviços) de forma conveniente e escalável, com mínimo esforço de gerenciamento pelo cliente e alta elasticidade de oferta pelo provedor.
- **Modelo de Serviço em nuvem – IaaS:** *Infrastructure as a Service* – Infraestrutura como Serviço. Capacidade fornecida ao cliente de provisionar processamento, armazenamento, redes e outros recursos fundamentais de computação, em que o cliente pode implantar e executar software arbitrário (incluindo sistemas operacionais e aplicações), sem gerenciar a infraestrutura física subjacente.
- **Modelo de Serviço em nuvem – PaaS:** *Platform as a Service* – Plataforma como Serviço. Capacidade fornecida ao cliente de implantar, em infraestrutura de nuvem, aplicações criadas ou adquiridas pelo cliente usando linguagens de programação, bibliotecas e ferramentas suportadas pelo provedor. O cliente não gerencia a infraestrutura subjacente, mas tem controle sobre as aplicações implantadas e, possivelmente, sobre configurações do ambiente de hospedagem.
- **Modelo de Serviço em nuvem – SaaS:** *Software as a Service* – Software como Serviço. Capacidade fornecida ao cliente de utilizar aplicações do provedor executando em infraestrutura de nuvem. As aplicações são acessíveis de diversos dispositivos via web, sem necessidade de instalação local, e o cliente não gerencia a infraestrutura ou mesmo as configurações da aplicação (salvo ajustes limitados de parâmetros).
- **Nuvem Privada:** Infraestrutura de nuvem provisionada para uso exclusivo de uma única organização, podendo ser de propriedade, gerenciamento e operação internos ou de terceiros, e podendo existir dentro ou fora das instalações da organização.

- **Nuvem Pública:** Infraestrutura de nuvem provisionada para uso aberto ao público em geral, geralmente de propriedade e operação de um provedor comercial de serviços de nuvem, localizada nas instalações do provedor.
- **Nuvem Híbrida:** Combinação de duas ou mais infraestruturas de nuvem (privadas, públicas e/ou comunitárias) que permanecem entidades únicas, mas são unidas por tecnologia padronizada ou proprietária que permite portabilidade de dados e aplicações (por exemplo, *cloud bursting* para balanceamento entre nuvens).
- **Cloud Broker (Integrador de Serviços de Nuvem):** Entidade que gerencia o uso, o desempenho e a entrega de serviços de computação em nuvem, e intermedia relações entre o provedor de nuvem e o contratante. No contexto público, um *cloud broker* pode auxiliar o órgão na descoberta, integração, monitoramento e gestão de múltiplos provedores de nuvem, agregando valor e garantindo aderência a padrões e segurança.
- **Workload (Carga de trabalho):** Conjunto de aplicações, serviços, dados e processos de TI que consomem recursos computacionais. No contexto de nuvem, refere-se a um conjunto identificável de recursos e tarefas que podem ser migrados ou executados em ambiente de computação em nuvem.
- **Estratégia de saída (Exit Strategy):** Plano prévio para a eventual migração reversa ou transferência de serviços, aplicações e dados de um ambiente de nuvem para outra nuvem ou para infraestrutura local. Visa evitar dependência excessiva de um único provedor (*lock-in*), prevendo medidas para portabilidade e continuidade do negócio caso o contrato com o provedor precise ser encerrado.

*(Demais termos técnicos adotados neste documento correspondem às definições do Glossário de Segurança da Informação [Portaria GSI/PR nº 93/2019] e do Anexo I da Portaria SGD/MGI nº 5.950/2023.)*

## 4. Princípios

A implementação desta estratégia pela ANPD será norteadada por princípios fundamentais da Administração Pública e da gestão de tecnologia, assegurando aderência aos valores institucionais e às melhores práticas de TIC:

- **Legalidade e Transparência:** Respeito integral às normas legais e regulatórias aplicáveis, especialmente no que diz respeito à proteção de dados pessoais, licitações e contratos de TI, com ampla divulgação das diretrizes desta estratégia dentro da ANPD.

- **Segurança da Informação e Privacidade:** Compromisso com a proteção das informações sob responsabilidade da ANPD, adotando-se medidas de segurança robustas em todo o ciclo de vida das soluções em nuvem, bem como práticas de *privacy by design/default* para salvaguardar dados pessoais sensíveis, em conformidade com a LGPD.
- **Eficiência e Inovação:** Busca contínua por eficiência operacional e qualidade na prestação dos serviços, utilizando a computação em nuvem como catalisador para inovação, agilidade e melhoria dos processos internos, sempre que agregar valor ao interesse público.
- **Otimização de Recursos:** Utilização racional e otimizada dos recursos de TI disponíveis, priorizando soluções em nuvem quando estas se mostrarem mais vantajosas em termos de custo-benefício, desempenho e escalabilidade, e garantindo o melhor aproveitamento possível da infraestrutura local existente em complementação à nuvem.
- **Alinhamento Estratégico:** Coerência com os objetivos estratégicos da ANPD e com as políticas e planos de governo digital federais, garantindo que a adoção de nuvem sirva de apoio às metas institucionais e não seja tratada isoladamente como fim em si mesma.
- **Responsabilidade Socioambiental:** Consideração de práticas sustentáveis na adoção de serviços de nuvem, valorizando fornecedores que adotem energia limpa e otimização de consumo energético em seus datacenters, bem como garantindo acessibilidade e inclusão digital nos serviços disponibilizados aos cidadãos, em linha com diretrizes de governança sustentável de TI.

## 5. Objetivos e Necessidades de Negócio

São objetivos a serem alcançados com a adoção controlada e estratégica de soluções de software e computação em nuvem na ANPD:

- **Modernização e Agilidade:** Modernizar a infraestrutura e os serviços de TIC da ANPD por meio da adoção de tecnologias de nuvem flexíveis e escaláveis, aumentando a agilidade para atender às demandas institucionais e às mudanças regulatórias dinâmicas na área de proteção de dados.
- **Otimização de Custos:** Melhorar o controle e a gestão dos custos de TIC, evitando gastos desnecessários com infraestrutura própria. A computação em nuvem possibilita um modelo de pagamento conforme o uso, permitindo à ANPD pagar somente pelos recursos consumidos e reduzir despesas com manutenção de data centers tradicionais.



- **Escalabilidade e Desempenho:** Aumentar a capacidade de processamento e armazenamento de forma elástica, garantindo que a ANPD possa lidar eficientemente com volumes crescentes de dados (incluindo dados de incidentes de vazamento, denúncias e comunicações com controladores/operadores) sem prejuízo ao desempenho. Ambientes de nuvem oferecem escalabilidade praticamente ilimitada para atender picos de demanda, assegurando desempenho adequado dos sistemas analíticos e de fiscalização da ANPD.
- **Inovação Tecnológica:** Reduzir o intervalo entre a disponibilização de novas tecnologias no mercado (por exemplo, soluções de inteligência artificial para análise de grandes volumes de dados ou ferramentas avançadas de compliance) e sua adoção efetiva pela ANPD. A nuvem facilita a experimentação e a implementação ágil de novas soluções tecnológicas, impulsionando a inovação nos processos de trabalho e na oferta de serviços aos cidadãos e empresas.
- **Eficiência Operacional:** Automatizar e simplificar processos de TI por meio de soluções em nuvem, aumentando a produtividade da equipe e permitindo que o foco seja direcionado a atividades finalísticas de maior valor (como a fiscalização e orientação sobre proteção de dados), ao invés de operações manuais de infraestrutura.
- **Segurança e Conformidade Aprimoradas:** Fortalecer a segurança da informação na ANPD, aproveitando recursos de segurança avançados oferecidos por provedores de nuvem (monitoramento 24/7, detecção de intrusão, criptografia robusta, etc.) e garantindo conformidade com requisitos legais e regulatórios. A adoção de nuvem deve resultar em proteção reforçada dos dados e sistemas da ANPD em ambiente de nuvem, servindo de referência em boas práticas de segurança e privacidade no setor público.
- **Continuidade e Resiliência:** Aumentar a disponibilidade dos serviços da ANPD e a capacidade de recuperação diante de incidentes. Espera-se que, com a nuvem, a ANPD tenha planos de contingência mais sólidos (como backups geograficamente distribuídos, redundância de sistemas) para assegurar a continuidade do negócio, mesmo frente a desastres ou indisponibilidades localizadas.

Adicionalmente, estão associadas a esta estratégia necessidades de negócio específicas da ANPD: melhoria da gestão de dados sensíveis sob sua custódia, atendimento ágil às solicitações dos titulares de dados e adaptação rápida a novas demandas (como grandes operações de fiscalização ou sanções) que possam exigir recursos computacionais além da capacidade atual.

## 6. Diretrizes para Adoção de Software e Serviços de Nuvem

As seguintes diretrizes estratégicas deverão ser observadas pela ANPD ao planejar, contratar e utilizar soluções de software e serviços de computação em nuvem de forma segura e eficaz. Cada diretriz é adaptada à realidade da ANPD, mas inspirada em boas práticas já adotadas por outros órgãos públicos:

### 6.1. Identificação das Necessidades do Negócio

Antes de qualquer iniciativa de migração ou contratação de nuvem, a ANPD deve identificar e avaliar cuidadosamente as suas necessidades de negócio. Deve-se determinar quais sistemas, aplicações, dados e serviços da ANPD **fazem sentido** serem movidos para a nuvem, levando em conta os benefícios esperados e os riscos envolvidos. Durante as fases de concepção de novos serviços ou sistemas, deve-se analisar a viabilidade e pertinência de desenvolver tais soluções já em ambiente de nuvem, ou mantê-las *on-premises*, conforme o que melhor atender aos requisitos da ANPD. Em resumo, a decisão de “ir para a nuvem” deve ser guiada por demandas reais de negócio e alinhada ao planejamento estratégico, não por tendência tecnológica apenas.

### 6.2. Seleção dos Modelos Adequados

Para cada caso de uso identificado, a ANPD deve avaliar **quais modelos de serviço em nuvem** (IaaS, PaaS ou SaaS) e **quais modelos de implementação** (nuvem pública, privada ou híbrida) melhor se adequam aos requisitos de negócio levantados. Essa avaliação deve considerar o grau de maturidade da ANPD em computação em nuvem e eventuais restrições técnicas ou legais. Sempre que possível, deve-se adotar uma abordagem de **nuvem híbrida** como estratégia, combinando o uso de nuvem pública e infraestruturas privadas/governo, de forma a equilibrar benefícios de escalabilidade com requisitos de segurança e soberania dos dados.

- *Preferência Estratégica:* Caso a demanda possa ser suprida integralmente por serviços em nuvem de forma segura, a ANPD poderá optar por uma migração mais ampla para a nuvem (estratégia “cloud-first”). Entretanto, se existirem impedimentos técnicos ou normativos para migrar certos sistemas (por exemplo, dados sensíveis que não podem sair de uma rede restrita), pode-se adotar uma abordagem gradual, iniciando por nuvem híbrida ou mantendo parte do *workload on-premises*.
- *Evitar “lift-and-shift” puro:* A migração de aplicações legadas do datacenter para a nuvem sem adaptações (modelo *lift-and-shift*) deve ser tratada como último recurso. Antes de migrar, é recomendável modernizar as aplicações ou rearquitetá-las para aproveitar adequadamente as vantagens da nuvem (elasticidade, serviços gerenciados etc.). A ANPD deve evitar replicar na

nuvem ineficiências existentes *on-premises*; em vez disso, cada sistema migrado deve passar por avaliação e possíveis melhorias.

### 6.3. Avaliação dos Possíveis Fornecedores

Nos estudos técnicos preliminares para contratação, a ANPD deve realizar levantamento de possíveis fornecedores de serviços de nuvem aptos a atender seus requisitos de negócio, garantindo **competitividade** e **experiência comprovada**. Devem ser identificados no mercado pelo menos alguns provedores qualificados e compatíveis com o setor público para cada serviço desejado. Nesta avaliação, levar em conta:

- **Segurança e Conformidade:** Verificar se o provedor possui certificações de segurança (ISO/IEC 27001, ISO/IEC 27701, SOC 2 Tipo II, PCI-DSS, entre outras) e se seus serviços permitem conformidade com a LGPD e demais leis brasileiras. Fatores como localização dos datacenters (jurisdição), medidas de proteção de dados e acordo de níveis de serviço de segurança devem influenciar a seleção.
- **Capacidade e Suporte:** Avaliar a disponibilidade de suporte técnico local, idioma e acordo de suporte do provedor, bem como sua capacidade de atender às necessidades de escala da ANPD. Provedores com histórico de alta disponibilidade e amplo portfólio de serviços (incluindo ferramentas de análise de dados, segurança avançada, inteligência artificial) podem melhor apoiar as futuras iniciativas da ANPD.
- **Custos e Modelo de Negócio:** Comparar modelos de precificação dos provedores (pagamento por uso, subscrição fixa, descontos por volume, etc.), assegurando que a opção escolhida seja economicamente vantajosa e sustentável no longo prazo. Analisar também potenciais custos de saída (ex: cobrança para download de dados ao migrar de volta *on-premises* ou para outro provedor) para evitar aprisionamento tecnológico inadvertido.
- **Requisitos de Experiência:** Sempre que aplicável, exigir evidências de experiência do fornecedor em atender órgão públicos ou em implantações de escopo similar. Atas de registros de preços existentes, contratações feitas por outros órgãos e o Quadrante Mágico do Gartner podem servir de insumo na identificação de líderes de mercado confiáveis para as categorias de serviço desejadas.

### 6.4. Definição de Requisitos de Segurança

A ANPD deve definir, antecipadamente no processo de planejamento da contratação, **quais requisitos de segurança da informação** serão mandatórios ou de alta importância para suas soluções em nuvem. Esses requisitos devem

abranger: controle de acesso, criptografia de dados em repouso e em trânsito, gestão de identidades, monitoramento de incidentes, entre outros. Para cada requisito de segurança identificado como crítico, deve-se avaliar como cada fornecedor candidato o atende ou pode atendê-lo.

Em virtude do papel sensível da ANPD, requisitos de segurança **adicionais ou mais rigorosos** podem ser justificados, tais como: exigência de que dados pessoais sensíveis sejam armazenados criptografados com chaves gerenciadas pela própria ANPD; *logging* detalhado de acesso a dados; isolamento robusto dos ambientes de nuvem utilizados pela ANPD, evitando qualquer risco de acesso indevido por terceiros. Tais condições deverão constar dos editais e contratos, garantindo obrigação formal dos fornecedores em cumpri-las.

Além disso, *testes de segurança* (como *pentests* e avaliações de vulnerabilidade) deverão ser previstos nos contratos de nuvem da ANPD, para verificação periódica independente da robustez das proteções, em conformidade com as normas de gestão de segurança da informação.

## 6.5. Política de Governança de Nuvem

Deverá ser instituída uma **Política de Governança de Nuvem** que oriente a gestão e o uso dos serviços contratados. Essa política interna deve abranger: classificação dos dados e *workloads* quanto a sensibilidade; diretrizes de controle de acesso e segregação de funções na nuvem; procedimentos de configuração segura; monitoramento e auditoria do ambiente em nuvem; e integração com os processos de governança já existentes (riscos, continuidade de negócio, gestão de mudanças etc.). O objetivo é garantir que os serviços em nuvem sejam utilizados em conformidade com padrões de segurança e qualidade adotados pela ANPD, e que haja clareza sobre *quem faz o quê* no contexto de nuvem (por exemplo, responsabilidades do provedor versus do cliente nos modelos de responsabilidade compartilhada).

Esta política de governança de nuvem deve ser elaborada em conjunto pelas áreas responsáveis pela governança de TI, segurança da informação e pela operação dos sistemas em nuvem. Somente com o envolvimento multidisciplinar será possível cobrir aspectos técnicos e de negócio, assegurando que a nuvem agregue valor de forma alinhada aos objetivos institucionais.

## 6.6. Uso Seguro de Software e Serviços de Nuvem

O uso de softwares na nuvem pela ANPD estará sujeito aos **mesmos controles e restrições** aplicados aos softwares instalados em ambiente local, acrescido de controles específicos de ambiente de nuvem. Isso significa que todo software em nuvem (por exemplo, um SaaS de gestão ou colaboração) deve passar pelo processo de avaliação e homologação de segurança da ANPD antes de ser

utilizado, verificando conformidade com a Política de Segurança da Informação e com esta Estratégia.

Algumas diretrizes específicas de uso seguro incluem:

- **Proteção de Dados Pessoais:** Garantir que dados pessoais armazenados ou processados em nuvem sejam tratados conforme as diretrizes da ANPD para proteção de dados. Isso envolve verificar se o provedor adota criptografia adequada, gestão de consentimento (quando aplicável) e atende aos direitos dos titulares (como exclusão de dados) em suas plataformas. A ANPD deve dar o exemplo de conformidade, exigindo contratualmente que o fornecedor de nuvem atue em conformidade com a LGPD ao tratar dados em nome da ANPD.
- **Segregação Lógica de Ambientes:** Exigir do provedor garantias de segregação lógica dos dados da ANPD em relação a outros clientes. A *multitenancy* da nuvem não deve permitir risco de vazamento de dados entre organizações. Os contratos devem prever níveis de isolamento e, se possível, auditorias independentes atestando essa segregação (por exemplo, relatórios SOC 2).
- **Gerenciamento de Identidades e Acessos:** Todos os acessos de usuários da ANPD aos consoles e serviços de nuvem devem ser gerenciados através de controles de identidade federada e autenticação multifator, conforme as políticas de acesso da ANPD. Perfis de acesso devem ser bem definidos (admin, desenvolvedor, auditor, etc.), aplicando o princípio do menor privilégio no ambiente em nuvem. Registros de logs de autenticação e atividades privilegiadas devem ser mantidos e revisados periodicamente pela equipe de segurança.
- **Monitoramento e Resposta a Incidentes:** Em complementação aos processos internos de monitoramento, a ANPD deverá utilizar as ferramentas de **monitoramento nativo** oferecidas pelo provedor de nuvem (como logs de segurança, alertas de intrusão, varredura de configuração) para detectar incidentes ou comportamentos anômalos rapidamente. Incidentes de segurança em recursos de nuvem devem ser comunicados e tratados conforme Regulamento de Comunicação de Incidente de Segurança da ANPD (RESOLUÇÃO CD/ANPD N° 15/2024), envolvendo o provedor quando necessário para remediação.

## 6.7. Infraestrutura de TIC Necessária

Para fazer uso eficaz da computação em nuvem, a ANPD deverá assegurar que sua **infraestrutura de TIC local** atenda a requisitos mínimos. Em especial, é necessário ter conectividade de rede estável e de alta disponibilidade com a Internet, com

banda suficiente para gerenciar e utilizar os serviços de nuvem sem gargalos. Links redundantes de comunicação podem ser necessários para garantir acesso ininterrupto aos sistemas críticos que estejam em nuvem.

Adicionalmente, deve-se verificar a compatibilidade das estações de trabalho, equipamentos de rede e políticas de firewall da ANPD com as tecnologias de nuvem adotadas (por exemplo, liberação de portas/protocolos necessários, instalação de agentes de monitoramento, etc.). A área de TI deverá planejar eventuais **atualizações de infraestrutura** (como upgrade de links de Internet, aquisição de equipamentos SD-WAN, soluções de VPN, etc.) como parte integrante do projeto de adoção de nuvem, evitando que o benefício da nuvem seja limitado por deficiências na estrutura local

Diretrizes de Governança para o Uso da Nuvem

A ANPD deve definir claramente **papéis e responsabilidades** relacionados à governança e gestão da nuvem. Isso inclui designar:

- **Responsável de Negócio pelo Serviço em Nuvem:** área ou pessoa na ANPD responsável por validar os requisitos, acompanhar a implementação e colher os benefícios do serviço em nuvem (por exemplo, se for um sistema de fiscalização em nuvem, a Coordenação de Fiscalização da ANPD atuaria nesse papel).
- **Responsável Técnico (TI) pelo Serviço:** profissional(is) da área de TI encarregados de administrar tecnicamente o serviço na nuvem, gerenciar o contrato do provedor e assegurar que configurações e usos estejam conforme as diretrizes.
- **Equipe de Segurança da Informação:** deverá acompanhar desde a fase de planejamento para definir controles necessários, bem como monitorar continuamente aspectos de segurança e conformidade durante o uso da nuvem, em cooperação com o responsável técnico.
- **Comitê de Governança Digital (CGD):** órgão colegiado interno que aprovará esta estratégia e suas futuras revisões, bem como deliberará sobre questões de governança de TIC e segurança. O CGD deve incluir a pauta de computação em nuvem em suas agendas, garantindo supervisão de alto nível sobre a adoção e uso responsável da nuvem na ANPD.

Essas diretrizes de governança garantem que haja **accountability** no uso da nuvem, ou seja, que todas as partes envolvidas saibam suas obrigações e que exista supervisão adequada. Decisões como escolha de provedores, movimentação de dados sensíveis ou definição de países permitidos para armazenamento de dados em nuvem (residência dos dados) devem ser tomadas colegiadamente conforme as competências definidas pelo Comitê de Governança Digital.

## 6.8. Princípios Norteadores da Estratégia de Nuvem

No contexto específico da estratégia de nuvem da ANPD, adotam-se alguns princípios norteadores práticos, alinhados às melhores práticas atuais de governo digital:

- **Cloud First:** Sempre que viável e seguro, a ANPD deverá privilegiar soluções em nuvem em vez de soluções locais, especialmente para novas necessidades. A computação em nuvem deve ser considerada como primeira opção tecnológica, adotando-se a seguinte ordem de prioridade quanto ao tipo de nuvem:
  1. Nuvem de Governo (Soberana): deverá ser a primeira alternativa considerada sempre que houver disponibilidade, em especial para sistemas críticos ou dados sensíveis, conforme diretrizes da Portaria SGD/MGI nº 5.950/2023 e demais normativos aplicáveis;
  2. Nuvem Privada: poderá ser utilizada quando a nuvem de governo não atender plenamente aos requisitos técnicos, operacionais ou regulatórios da ANPD;
  3. Nuvem Pública: será admitida apenas mediante justificativa técnica que demonstre segurança adequada, conformidade legal e ausência de opções mais aderentes à política pública de computação em nuvem.

A opção por manter soluções em infraestrutura própria (*on-premises*) deverá ocorrer somente em situações excepcionais, quando claramente demonstrados benefícios operacionais, limitações técnicas ou exigências legais específicas que inviabilizem o uso da nuvem. A decisão deverá ser formalmente justificada e aprovada conforme a governança interna.

- **Evitar o *Lift-and-Shift* Não Planejado:** Conforme já mencionado, migrar para a nuvem exige planejamento e adaptação. A ANPD adotará como princípio evitar migrações diretas sem otimização. Cada sistema passará por avaliação de *cloud readiness* e possíveis ajustes arquiteturais antes de sua transição ao ambiente de nuvem.
- **Multicloud e Interoperabilidade:** Sempre que fizer sentido, a ANPD buscará não depender exclusivamente de um único provedor de nuvem. A estratégia incentiva a possibilidade de um **ambiente multicloud**, tirando proveito de diferentes fornecedores para diferentes necessidades, e/ou o uso de um integrador (*broker*) para facilitar a gestão de múltiplas nuvens. Esse princípio visa reduzir risco de aprisionamento tecnológico e aumentar a flexibilidade para utilizar a melhor solução disponível em cada caso.

- **Portabilidade dos Dados:** A ANPD exigirá contratualmente que seus dados possam ser extraídos da nuvem em formatos abertos ou interoperáveis, de modo a facilitar migração futura ou criação de backups locais, fortalecendo a autonomia sobre as informações institucionais.
- **Segurança por Padrão:** Todo serviço de nuvem adotado deve vir já configurado, sempre que possível, seguindo o princípio de segurança por padrão (*secure by default*). Configurações iniciais inseguras devem ser evitadas. Por exemplo, se um novo armazenamento em nuvem for criado, o padrão deve ser com criptografia habilitada e acesso restrito, cabendo abertura gradual se necessário e não o contrário. Esse princípio norteará as implementações técnicas na ANPD.

## 6.9. Alinhamento com Outros Planos Estratégicos

Esta estratégia de nuvem está alinhada com os seguintes planos e instrumentos de planejamento da ANPD e do Governo Federal, garantindo coerência com as demais iniciativas de governança e TI:

- **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da ANPD:** As ações e metas definidas no PDTIC 2025-2028 da ANPD relacionadas à infraestrutura, sistemas e governança de TI consideram a adoção de computação em nuvem como meio para alcançar seus objetivos. A estratégia de nuvem provê diretrizes concretas para o cumprimento do PDTIC no que tange à modernização tecnológica e à transformação digital.
- **Planejamento Estratégico Institucional da ANPD:** A computação em nuvem será empregada como facilitadora para atingir metas institucionais, como melhoria do atendimento ao titular de dados, eficiência na fiscalização e promoção da cultura de proteção de dados. Esta estratégia guarda alinhamento com os objetivos estratégicos definidos no plano institucional, notadamente aqueles que dependem de soluções de TIC ágeis e escaláveis.
- **Plano Anual de Contratações (PAC):** As contratações de TIC previstas no PAC da ANPD deverão observar as diretrizes desta estratégia ao especificar e justificar aquisições de soluções em nuvem ou software. Assim, o PAC e a Estratégia de Nuvem estarão sincronizados, promovendo racionalização de gastos e aderência às normas do modelo de contratação do SISP.
- **Estratégia de Governo Digital (EGD) e Iniciativas de Governo como Plataforma:** A estratégia também observa os direcionadores da EGD vigente no que diz respeito à computação em nuvem, interoperabilidade e compartilhamento de serviços. A ANPD buscará utilizar serviços de nuvem de governo compartilhados quando disponíveis (por exemplo, soluções de



nuvem governamental ofertadas pela SGD) e contribuir para a integração de serviços na administração pública digital.

## 6.10. Linhas de Base e Metas de Benefícios Esperados

A ANPD definirá **linhas de base (baseline)** e **metas quantitativas** para os benefícios esperados com esta estratégia. Exemplos de métricas a serem acompanhadas: percentual de cargas de trabalho migradas para nuvem; redução percentual nos custos de infraestrutura de TI; tempo médio para disponibilizar um novo serviço de TI (*on-premises* vs. nuvem); índices de satisfação dos usuários internos com desempenho dos sistemas; melhoria nos indicadores de segurança (redução de incidentes ou vulnerabilidades devido à migração para ambientes mais seguros, etc.).

Junto a cada iniciativa de adoção de nuvem, devem ser estabelecidos indicadores de sucesso. Por exemplo, ao migrar determinado sistema para nuvem, espera-se aumentar sua disponibilidade de 95% para 99%, ou reduzir o tempo de processamento de relatórios em 30%. Essas metas deverão ser acompanhadas e reportadas periodicamente ao Comitê de Governança Digital da ANPD, para avaliar se a estratégia está de fato trazendo os resultados pretendidos. Caso os benefícios não estejam sendo atingidos, ajustes na execução ou mesmo na estratégia poderão ser deliberados. O monitoramento contínuo garantirá que a adoção de nuvem gere **valor mensurável**, como agilidade, redução de custos, aumento de resiliência e melhoria de segurança.

## 6.11. Capacitação da Equipe

A efetividade desta estratégia depende da **capacitação da equipe** da ANPD que gerenciará, operará ou usará os recursos de software e de computação em nuvem. A ANPD deverá investir no desenvolvimento de competências internas em computação em nuvem, incluindo treinamento técnico para a equipe de TI (por exemplo, em arquitetura de nuvem, administração de serviços AWS/Azure/GCP, gestão de contratos de nuvem, segurança em nuvem) e sensibilização dos usuários-chave sobre boas práticas de uso das novas ferramentas.

Em especial, a equipe de segurança da informação deve ser capacitada para lidar com controles de nuvem, gestão de identidades federadas, resposta a incidentes em ambiente cloud, etc. Da mesma forma, os gestores de contratos necessitam conhecer as peculiaridades dos modelos de precificação e métricas de nuvem. Caso haja falta de expertise interna inicialmente, a ANPD poderá considerar parcerias com órgãos que já possuem experiência ou contratação de consultoria especializada para transferência de conhecimento. A meta é que, a médio prazo, a ANPD disponha de uma equipe autônoma e habilitada para conduzir sua jornada na nuvem de forma segura e otimizada.

## 6.12. Portabilidade e Interoperabilidade

A ANPD deve considerar, desde o planejamento de suas soluções, medidas que facilitem a **portabilidade** e a **interoperabilidade** entre sistemas, dados e serviços em nuvem. Isso inclui: adotar padrões abertos e amplamente aceitos para armazenamento de dados (evitando formatos proprietários fechados); arquitetar aplicações de forma modular, de modo que componentes possam ser substituídos ou migrados com menor esforço; e preferir serviços de nuvem que ofereçam compatibilidade com múltiplas plataformas.

Além disso, deve-se avaliar a viabilidade de **estratégias multicloud** ou de contingência, por exemplo, manter backups críticos em um segundo provedor de nuvem ou em infraestrutura própria, prontamente utilizáveis em caso de falha grave ou interrupção prolongada no provedor principal. A interoperabilidade também se aplica à integração da ANPD com plataformas governamentais: assegurar que soluções em nuvem da Autoridade possam se comunicar com outros sistemas governamentais (ex.: gov.br, barramentos de dados do governo, sistemas do MJSP, etc.) de forma segura e padronizada. Em suma, a ANPD deve evitar dependência tecnológica excessiva e garantir que seus ativos digitais possam transitar entre ambientes conforme necessário, sem impacto à missão institucional.

## 6.13. Requisitos Regulatórios e de Conformidade

A ANPD, sendo ela própria o órgão central de interpretação da LGPD, deve servir de modelo no cumprimento de **requisitos regulatórios e de conformidade** no uso de software e serviços de nuvem. Isso significa observar atentamente:

- **Legislação de Proteção de Dados:** A Lei Geral de Proteção de Dados (LGPD) e normativos emanados pela própria ANPD em relação à proteção de dados pessoais. Todo contrato de nuvem da ANPD deve prever cláusulas claras sobre o papel do fornecedor como operador de dados, deveres de confidencialidade, medidas de segurança, notificação de incidentes de segurança envolvendo dados pessoais e cooperação com a ANPD no atendimento a direitos dos titulares, conforme aplicável.
- **Legislação de Licitações e Contratos (Lei nº 14.133/2021):** assegurar que as contratações de nuvem sigam os ditames da nova Lei de Licitações, incluindo planejamento (Estudo Técnico Preliminar específico para cada contratação de nuvem, gerenciamento de riscos, justificativas técnicas e de custo), seleção da melhor proposta e gestão contratual rigorosa. A Portaria SGD/MGI nº 5.950/2023, que norteia esta estratégia, está em consonância com a Lei 14.133 e oferece um modelo padronizado para essas contratações, o qual deve ser observado.

- **Normas de Segurança da Informação do GSI/PR:** cumprimento integral das Instruções Normativas listadas nas referências (IN GSI/PR nº 1/2020, nº 5/2021, etc.), bem como das políticas e guias do Gabinete de Segurança Institucional, especialmente no que tange a uso de nuvem. Por exemplo, a IN GSI/PR nº 5/2021 já estabelece diversos controles mínimos que a ANPD deve garantir. Esta estratégia incorpora tais controles e os reforça quando necessário, dada a criticidade dos dados tratados.
- **Normas de Acessibilidade Digital e Transparência:** garantir que as soluções em nuvem voltadas ao público (por exemplo, serviços on-line que a ANPD venha a oferecer hospedados em nuvem) atendam aos requisitos de acessibilidade e às diretrizes de governo digital (e.g., interoperabilidade, dados abertos, etc.), bem como que os contratos com fornecedores prevejam aderência à Lei de Acesso à Informação no que couber (por ex., fornecimento de relatórios e informações sobre o ambiente contratado quando solicitado) .

Em suma, nada na adoção de nuvem deve fazer a ANPD incorrer em descumprimento de dispositivos legais ou normativos. Pelo contrário, a nuvem deve ser uma aliada para se obter maior conformidade (ex.: registros de log mais completos para auditoria, facilidade em aplicar criptografia, etc.).

#### 6.14. Estratégia de Saída (*Exit Strategy*)

Desde o planejamento inicial de cada contratação de nuvem, a ANPD deve considerar a **estratégia de saída**, ou seja, como proceder caso futuramente seja necessário migrar os sistemas e dados hospedados em nuvem para um ambiente alternativo. A análise de dependências deve identificar componentes proprietários ou serviços específicos do provedor que possam dificultar a migração. Deve-se preferir arquiteturas portáteis e, quando isso não for possível, prever no contrato mecanismos de transição.

Elementos de uma estratégia de saída incluem: rotinas de **backup** periódicas dos dados críticos da ANPD armazenados em local seguro fora do ambiente principal do provedor (por exemplo, em outro provedor ou *on-premises*); cláusulas contratuais garantindo assistência do fornecedor na migração de volta ou para terceiros, incluindo prazo de fornecimento de dados após término contratual; manutenção de documentação completa das configurações de nuvem para reimplantar o ambiente em outro lugar se preciso . Em casos críticos, a ANPD pode considerar **contratos de apoio** ou redundância: por exemplo, ter um contrato secundário que permita ativação emergencial de serviços semelhantes em outro provedor, caso o principal falhe.

Ao longo do uso da nuvem, a ANPD deve evitar tornar-se excessivamente dependente de tecnologias proprietárias sem planejamento de saída. A cada novo serviço contratado, questionar: “Se amanhã precisarmos trocar este serviço ou provedor, estamos preparados?”. Essa mentalidade preventiva garantirá maior **resiliência estratégica**, evitando aprisionamento tecnológico e assegurando continuidade do negócio em qualquer cenário.

### 6.15. Análise de Riscos

A gestão de riscos deve permear toda a estratégia de uso de nuvem da ANPD. Devem ser consideradas as diretrizes de gerenciamento de riscos constantes no modelo de contratação de nuvem do SISP (Portaria SGD/MGI nº 5.950/2023) e em normativos correlatos. Para cada iniciativa de computação em nuvem, a ANPD deverá:

- Identificar os riscos potenciais (ex.: indisponibilidade do provedor, vazamento de dados, aumentos inesperados de custos, falhas de compliance, etc.);
- Avaliar a probabilidade e impacto de cada risco sobre as atividades-fim da ANPD (por exemplo, um incidente de segurança em sistemas de nuvem poderia comprometer investigações ou exposição indevida de dados sensíveis de cidadãos);
- Definir **tratamentos ou controles** para mitigar os riscos inaceitáveis: planos de contingência, controles adicionais de segurança, seguros, redundâncias, entre outros. Muitos desses controles já foram elencados nas diretrizes acima (backup, redundância, seleção criteriosa de fornecedor, etc.), devendo compor formalmente o Plano de Gerenciamento de Riscos da contratação ou projeto;
- Aprovar os níveis de risco residuais: a alta administração da ANPD, aconselhada pelo Comitê de Governança Digital, deverá explicitamente aceitar os riscos que permanecerem após mitigação, assegurando que estejam dentro do apetite de risco institucional.

Esse processo deve estar documentado e atualizado. A cada revisão desta estratégia ou contratação relevante, os riscos devem ser reavaliados, inclusive à luz de mudanças no cenário tecnológico ou normativo. Por exemplo, novos tipos de ameaças cibernéticas ou mudanças na legislação de proteção de dados podem introduzir riscos antes inexistentes que precisarão de novas medidas de controle.

Adicionalmente, a ANPD acompanhará as orientações e relatórios governamentais de riscos em TIC (como aqueles produzidos pelo TCU ou SGD) para incorporar lições aprendidas de outros órgãos. A constante vigilância em riscos garantirá uma

postura **proativa** e **preventiva**, minimizando a ocorrência de incidentes que possam afetar a missão institucional ou a imagem da ANPD.

## 7. Responsabilidades

Para a boa execução desta estratégia, ficam estabelecidas as seguintes responsabilidades no âmbito da ANPD, em consonância com as estruturas de governança vigentes:

- **Alta Administração da ANPD:** é responsabilidade da alta administração assegurar e patrocinar a implementação desta estratégia, provendo o suporte necessário. Em especial, **garantir recursos orçamentários e humanos** adequados para as iniciativas de computação em nuvem. **Comitê de Governança Digital (CGD):** Órgão colegiado interno responsável por aprovar este documento e suas atualizações, bem como supervisionar sua execução. **Coordenação-Geral de Tecnologia da Informação (CGTI):** Unidade técnica de TI da ANPD responsável pelo planejamento, contratação, operação e manutenção dos serviços de computação em nuvem. Compete à CGTI conduzir os estudos técnicos preliminares e processos de contratação conforme as diretrizes desta estratégia; administrar os contratos vigentes com provedores de nuvem, monitorando níveis de serviço e conformidade; implementar os procedimentos e controles técnicos necessários no ambiente de nuvem; e fornecer suporte às demais áreas no uso eficiente e seguro das soluções. A CGTI atuará como ponto focal técnico, garantindo que a infraestrutura e configurações estejam adequadas e que os usuários internos sejam atendidos em suas demandas relacionadas à nuvem.
- **Gestor de Segurança da Informação (GSI) da ANPD:** Profissional ou equipe designada para gerir a segurança da informação no órgão (conforme IN GSI/PR nº 1/2020). Compete ao GSI coordenar a elaboração e revisão das normas internas relacionadas ao uso seguro de computação em nuvem, em conjunto com a TI, além de **supervisionar a aplicação** dessas normas na prática. O gestor de SI deve assegurar comunicação efetiva com o(s) provedor(es) de nuvem quanto a incidentes e níveis de serviço de segurança acordados; supervisionar a implementação de medidas corretivas pelo provedor quando falhas de segurança forem identificadas; e reportar ao CGD e alta administração sobre o status da segurança dos ambientes em nuvem. Também inclui comunicar incidentes relevantes às autoridades competentes (como o Gabinete de Segurança Institucional, em casos de incidentes graves, e o próprio Conselho Diretor da ANPD, se for o caso). Em suma, o GSI é o guardião da segurança e conformidade dentro da estratégia

de nuvem, garantindo que esta seja implantada **sem comprometer a proteção de dados e informações**.

- **Demais Áreas Usuárias e Gestores de Processos:** Cada área da ANPD que venha a utilizar serviços em nuvem (por exemplo, para sistemas finalísticos de fiscalização, atendimento ao público, ou sistemas administrativos) tem o dever de utilizar tais serviços de acordo com as diretrizes desta estratégia e as normas internas estabelecidas. Os gestores dessas áreas devem garantir que suas equipes cumpram os procedimentos de segurança (como uso adequado de senhas, classificação de informações colocadas na nuvem, etc.) e reportem à TI quaisquer necessidades ou problemas. Devem participar ativamente do planejamento das soluções que atendem seu negócio, auxiliando na identificação de requisitos e na avaliação de riscos relacionados à confidencialidade ou sensibilidade de seus dados. A colaboração entre área usuária e TI é fundamental para que a solução em nuvem atenda plenamente aos objetivos.

## 8. Disseminação, Revisão e Atualização da Estratégia

Esta Estratégia de Uso de Software e Serviços de Computação em Nuvem, por se tratar de um documento estratégico da ANPD, **deverá ser amplamente divulgada** no âmbito interno, garantindo que todos os servidores e colaboradores pertinentes tenham conhecimento de suas diretrizes. A divulgação poderá incluir comunicados internos, workshops de apresentação e publicação no portal de governança da ANPD para consulta.

A estratégia será um documento dinâmico: **revisões periódicas** serão realizadas para mantê-la atualizada em face de evoluções tecnológicas, mudanças regulatórias ou novas orientações do órgão central (SGD/MGI). Recomenda-se revisão ao menos bienal, não excedendo 2 (dois) anos sem atualização. Revisões também podem ser desencadeadas a qualquer tempo caso ocorram fatores relevantes, tais como: alterações significativas na legislação de proteção de dados ou segurança (que demandem novos controles); mudanças nas políticas de governo digital; aprendizado oriundo de incidentes ou auditorias; ou disponibilidade de novas ofertas de nuvem governamental. Qualquer atualização deverá ser aprovada pelo Comitê de Governança Digital da ANPD.

As **novas contratações** de software e serviços de computação em nuvem a partir da publicação desta estratégia **devem obrigatoriamente observar** suas diretrizes e orientações, bem como o modelo padronizado de contratação definido pela Portaria SGD/MGI nº 5.950/2023. No caso de situações não previstas ou excepcionais, estas serão analisadas pelo CGD, que poderá deliberar soluções ad

hoc, sempre documentando a decisão e incorporando o aprendizado em versões futuras do documento.