RESOLUÇÃO ANA Nº 254, DE 3 DE JULHO DE 2025
DOCUMENTO Nº 0064252

Aprova a Política de Backup e suas regras no âmbito da Agência Nacional de Águas e Saneamento Básico (ANA).

A DIRETORA-PRESIDENTE DA AGÊNCIA NACIONAL DE ÁGUAS E SANEAMENTO BÁSICO - ANA, no uso da atribuição que lhe confere o art. 140, inciso III, do Anexo I da Resolução ANA nº 242, de 24 de fevereiro de 2025, publicada no DOU de 27 de fevereiro de 2025, que aprovou o Regimento Interno da ANA, torna público que a DIRETORIA COLEGIADA, em sua 1010ª Reunião Administrativa Ordinária, realizada em 30 de junho de 2025, considerando o disposto no art. 3º, e no uso das atribuições que lhe confere o art. 12, I, da Lei nº 9.984, de 17 de julho de 2000, e com base nos elementos constantes do processo nº 02501.006264/2024-37.

Resolve:

Art. 1º Aprovar a Política de Backup e suas regras no âmbito da Agência Nacional de Águas e Saneamento Básico (ANA), conforme anexos desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

(assinado eletronicamente)
VERONICA SÁNCHEZ DA CRUZ RIOS

ANEXO I
POLÍTICA DE BACKUPS DA ANA

CAPÍTULO I
DO ESCOPO

Art. 1º A Política de Backups tem como objetivo estabelecer diretrizes, competências e responsabilidades para garantir a segurança, a proteção e a disponibilidade dos ativos de dados digitais sob a custódia da área de Tecnologia da Informação e formalmente definidos como essenciais à salvaguarda na ANA, assegurando a continuidade do negócio em casos de indisponibilidade ou perda decorrente de erro humano, ataques, catástrofes naturais ou outras ameaças.

Art. 2º Esta norma aplica-se a todos os dados digitais no âmbito da ANA, incluindo aqueles armazenados fora da Agência, seja em serviços de nuvem pública ou privada.

§ 1º Consideram-se dados críticos, no contexto da gestão de backups, os bancos de dados, os dados e arquivos digitais armazenados na estrutura física do serviço de armazenamento e compartilhamento de arquivos administrado pela área de TI, o conteúdo web armazenado nos servidores que hospedam o Portal da ANA e demais sítios das áreas administrativas da Agência, bem como os dados digitais dos demais servidores alocados fisicamente no parque computacional da ANA.

§ 2º A Equipe de Tratamento e Resposta de Incidentes Cibernéticos (ETIR) é responsável por definir quais recursos, sistemas operacionais, máquinas virtuais, softwares, sistemas de informação e serviços de TI terão backups realizados.

§ 3º A salvaguarda dos dados digitais pertencentes aos serviços de TI da ANA, mas custodiados por entidades públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre as partes envolvidas.

§ 4º Os procedimentos configurados no sistema de gestão de backups administrado pela área de TI não abrangem:

I – Dados armazenados nos discos locais de desktops e/ou dispositivos pessoais; e

II – Dados armazenados nos servidores utilizados pelas áreas finalísticas da ANA sem o prévio conhecimento da área de TI.

CAPÍTULO II
DAS DIRETRIZES GERAIS

Art. 3º As diretrizes gerais constituem os pilares da gestão de backups na ANA, orientando a elaboração de normas internas complementares, planos, procedimentos, ações e controles que garantam a observância dos princípios básicos de gestão de backups.

Parágrafo único. Esta política deve estar alinhada com a Política de Segurança da Informação e Comunicação (POSIC) da ANA.

Art. 4º Os procedimentos relativos ao serviço de backup (cópia de segurança) e restore (restauração de cópia de segurança) serão regulamentados considerando as seguintes diretrizes gerais:

§1º O serviço de backup e restore deve ser automatizado por sistemas informacionais específicos, prevendo a execução agendada fora do horário de expediente regular da Agência, durante as chamadas "janelas de backup", períodos de baixa ou nenhuma atividade de usuários e processos automatizados nos sistemas de informática.

§2º A solução de backup deverá ser mantida atualizada em todas as suas características,

incluindo correções, novas versões, ciclo de vida, garantias e melhorias.

§3º A administração das mídias de backup deverá estar contemplada em normas complementares ao serviço, garantindo sua segurança e integridade.

§4º As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente em estruturas que contemplem cofres e salas-cofre.

§5º A execução das rotinas de backup e restore deverá ser rigidamente controlada, documentada e auditada, em conformidade com as normas e procedimentos aplicáveis.

§6º Toda informação custodiada pela área de Tecnologia da Informação e considerada crítica para a execução das atividades da Agência deverá possuir backup e ser armazenada em local protegido, compatível com o nível de segurança exigido.

§7º Os arquivos dos servidores e colaboradores armazenados em pastas corporativas, caixas de correio eletrônico, bases de dados e arquivos de sistemas terão suas regras estabelecidas nesta Política.

Art. 5º A execução do serviço de backup deverá considerar a definição de horário, periodicidade, quantidade de cópias necessárias para garantir a disponibilidade da informação e tempo de retenção das cópias armazenadas.

§1º A organização das cópias de backup deverá seguir critérios de data e tipo de cópia (completa, diferencial e incremental).

§2º A periodicidade dos testes de backup e restore será estabelecida em normas e procedimentos específicos.

§3º Toda alteração, inclusão ou exclusão de informações nos serviços de backup deverá ser oficialmente comunicada pela área demandante, garantindo que apenas informações pertinentes e necessárias à execução dos serviços da ANA sejam copiadas, vedando-se a realização de cópias de informações não essenciais às atividades da Agência.

§4º Os arquivos armazenados nos discos de computadores de uso pessoal da ANA (desktops, notebooks e outros dispositivos) não serão abrangidos pela Política de Backup e Restore, sendo a cópia de segurança de responsabilidade do usuário.

§5º Recomenda-se que cada usuário da ANA efetue o backup de suas pastas corporativas por meio dos serviços de armazenamento em nuvem disponibilizados pela Agência.

§6º Os resultados dos testes de backup e restore deverão ser documentados e validados pela equipe responsável, garantindo sua validade dentro do período estabelecido.

CAPÍTULO III
DA GESTÃO DE BACKUPS

Art. 6º O gerenciamento de backups é um aspecto crítico da segurança da informação e da continuidade dos serviços de TI, devendo ser executado conforme os recursos disponibilizados pela ANA.

§ 1º A gestão de backups deve contemplar a recuperação de desastres e a contingência dos serviços de TI para cenários em que a infraestrutura principal esteja inacessível.

§ 2º O processo de recuperação e restauração de dados deve ser continuamente estabelecido, mantido e documentado.

§ 3º A solução automatizada para a gestão de backups deve ser implementada e mantida de forma contínua.

§ 4º Os dados críticos devem ser devidamente identificados para orientar as estratégias de criação e restauração de backups.

§ 5º Devem ser implementados mecanismos de controle de acesso físico e lógico para garantir a proteção das cópias de segurança.

§ 6º Sempre que possível, os backups devem ser criptografados para assegurar a

confidencialidade dos dados.

§ 7º A salvaguarda dos dados digitais pertencentes à ANA, mas custodiados por entidades públicas ou privadas, incluindo serviços em nuvem, deve estar formalmente garantida por meio de acordos ou contratos que regulamentem a relação entre as partes envolvidas.

SEÇÃO I
DO PLANEJAMENTO

Art. 7º As estratégias de backup de dados devem definir quais informações devem ser protegidas por meio de cópias de segurança.

§ 1º Na ANA, foram estabelecidos os seguintes dados a serem protegidos:

I – Informações e documentos de identificação pessoal de servidores, estagiários, voluntários e prestadores de serviço;

II – Registros financeiros da ANA;

III – Processos administrativos;

IV – Documentos administrativos, incluindo políticas, procedimentos, registros de reuniões, contratos, acordos com fornecedores e demais documentos relacionados à gestão administrativa da ANA; e

V – Configurações de sistemas de tecnologia, como servidores, bancos de dados e quaisquer outras configurações de TI consideradas críticas para a continuidade das operações.

SEÇÃO II
DA CRIAÇÃO

Art. 8º A criação de estratégias de backups deve garantir que os dados estejam protegidos e possam ser recuperados de maneira confiável quando necessário.

§ 1º Sempre que possível, as cópias de dados e informações institucionais devem ser realizadas regularmente e de forma automatizada, conforme cronograma estabelecido, garantindo a disponibilidade dos dados mais recentes para recuperação.

§ 2º A segmentação de dados deve ser aplicada sempre que viável, considerando quais informações devem ser armazenadas localmente, em nuvem ou em outros dispositivos de armazenamento.

§ 3º As estratégias de backup devem especificar o objetivo da cópia de segurança, incluindo frequência, tempo de recuperação (RTO) e ponto de recuperação (RPO).

§ 4º Para a definição das estratégias de backup, o administrador responsável deve realizar uma avaliação das necessidades, identificando dados e sistemas críticos, requisitos de retenção e metas de recuperação.

§ 5º Cópias de segurança integrais dos servidores e máquinas virtuais que hospedam sistemas críticos para a ANA devem ser realizadas regularmente.

SEÇÃO III
DA RETENÇÃO

Art. 9º A retenção de backups deve considerar o tempo de armazenamento das cópias de segurança antes de seu descarte.

§ 1º Devem ser estabelecidas políticas de retenção de dados para definir por quanto tempo os backups serão mantidos, levando em conta os requisitos regulatórios e legais aplicáveis.

§ 2º A ANA deve reter as versões dos arquivos, permitindo a recuperação total de sistemas, recursos ou serviços de TI, conforme os recursos tecnológicos disponíveis.

§ 3º Sempre que possível, as estratégias de retenção devem observar as seguintes recomendações:

I – Diária: 7 dias da semana;

II – Semanal: 4 últimas semanas;

III – Mensal: 12 últimos meses; e

IV – Um backup anual.

SEÇÃO IV
DA RESTAURAÇÃO

Art. 10. A recuperação/restauração de dados é um processo crítico que deve ser executado para assegurar a continuidade dos serviços de TI após a perda de informações essenciais devido a falhas de software, hardware, erros humanos, ataques cibernéticos ou desastres naturais.

§ 1º Os servidores da área de TI devem ser treinados para realizar a restauração de dados de forma eficaz e segura.

§ 2º Um plano de recuperação de dados deve ser definido, documentado e revisado continuamente, incluindo os procedimentos necessários para restaurar backups em caso de falhas ou eventos catastróficos.

§ 3º Ao elaborar o plano de recuperação e restauração de dados, deve-se determinar e priorizar a ordem dos sistemas e dados a serem restaurados, com base na Análise de Impacto ao Negócio (BIA).

§ 4º Deve ser estabelecido e mantido um ambiente isolado para restauração de dados, distinto do ambiente de produção, que deve ser mantido atualizado.

§ 5º Os procedimentos de restauração de dados devem estar alinhados com a POSIC e em conformidade com a LGPD e com os planos institucionais.

§ 6º Antes de iniciar a restauração de dados, o administrador de backups deve verificar a integridade dos backups para certificar-se de que os dados não estejam corrompidos e que estejam disponíveis para a restauração.

§ 7º Testes regulares de recuperação de dados devem ser realizados para garantir que os backups sejam funcionais e que os procedimentos de recuperação sejam eficazes.

§ 8º Todas as etapas do processo de restauração de dados, incluindo datas, horas e detalhes específicos sobre cada ação realizada, devem ser documentadas.

SEÇÃO V
DOS TESTES

Art. 11. Os testes de restauração de backups devem garantir que, em caso de falhas ou perda de dados, estes possam ser recuperados.

§ 1º Um plano de testes deve ser estabelecido e mantido, incluindo todos os detalhes necessários, como quais backups serão testados, quais sistemas ou dados serão restaurados e qual procedimento será realizado.

§ 2º Um ambiente deve ser configurado, separado do ambiente de produção, para a execução dos testes, a fim de evitar qualquer impacto nos sistemas de produção.

§ 3º Procedimentos para testes de recuperação de dados devem ser estabelecidos e mantidos, a fim de garantir que os backups sejam eficazes e que a recuperação seja possível quando

necessário.

§ 4º Testes de restauração de dados devem ser realizados de forma a identificar problemas antes de ser necessário restaurar dados em uma situação de crise.

§ 5º Os testes devem ser realizados por amostragem, em servidores diferentes dos utilizados nos ambientes de produção, observando-se os recursos humanos de TI e as tecnologias disponíveis, a fim de verificar o sucesso dos backups.

§ 6º Os testes devem levar em consideração as políticas de retenção de dados, para garantir que se saiba quanto tempo os backups devem ser mantidos e como devem ser excluídos.

§ 7º Sempre que possível, os testes devem simular cenários de falhas, como exclusões acidentais, corrupção de dados ou ataques de malware.

§ 8º Sempre que possível, deve-se realizar testes de restauração de sistemas completos em máquinas virtuais ou hardware de teste, para garantir que os sistemas possam ser reconstruídos com sucesso.

§ 9º Sempre que possível, deve-se avaliar o tempo necessário para restaurar dados e sistemas, a fim de determinar se os backups podem ser restaurados dentro do período aceitável.

§ 10 Os resultados dos testes devem ser documentados, incluindo quaisquer problemas encontrados e as etapas tomadas para resolvê-los.

SEÇÃO VI
DA AUDITORIA E CONFORMIDADE

Art. 12. A auditoria e conformidade de dados devem garantir que a cópia de dados seja realizada de forma adequada, segura e em conformidade com regulamentos e políticas internas pertinentes.

§ 1º Os procedimentos de backup devem ser regularmente auditados para assegurar que estejam em conformidade com a legislação vigente.

§ 2º Registros das atividades de backup, incluindo datas, horas, tipo de dados copiados e quaisquer ações realizadas durante o processo de backup, devem ser mantidos continuamente.

§ 3º Verificações regulares de integridade dos backups devem ser realizadas para identificar qualquer corrupção de dados ou problemas de armazenamento.

§ 4º Os backups devem estar em conformidade com os regulamentos de privacidade de dados e segurança da informação.

§ 5º A área de TI deve manter registros de backups e testes de restauração para demonstrar conformidade com esta política.

§ 6º Os registros de backups devem conter, no mínimo, o tipo de sistema/serviço que teve seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso.

§ 7º Um sistema de monitoramento da execução dos backups deve ser implementado e mantido para acompanhar o status da realização da atividade, permitindo a identificação de problemas e a tomada de medidas corretivas de forma ágil.

§ 8º Alertas e notificações sobre falhas na realização de cópias de segurança devem ser configurados no sistema de gestão de backup, de modo que a equipe de TI seja informada imediatamente em caso de falhas ou problemas de integridade do backup.

SEÇÃO VII
DO DESCARTE

Art. 13. O descarte de dados deve ser realizado de forma segura, observando os requisitos

definidos na legislação pertinente.

§ 1º A equipe responsável pelo descarte de backups deve ser treinada, a fim de garantir que estejam cientes dos procedimentos e da importância da eliminação segura dos dados.

§ 2º As regras de descarte de backups devem ser revisadas periodicamente, com o objetivo de assegurar que estejam alinhadas com as necessidades atuais da organização e com as mudanças nas regulamentações de privacidade de dados e segurança da informação.

§ 3º A eliminação de backups deve estar em conformidade com as leis e regulamentos de privacidade de dados, além de considerar a sustentabilidade ambiental.

§ 4º Sempre que possível, métodos seguros de descarte devem ser utilizados, como a destruição física de discos rígidos ou mídias de armazenamento, trituradoras de papel e desmagnetização de discos, entre outros.

§ 5º Backups contendo dados sensíveis ou confidenciais devem ser tratados com segurança durante o processo de descarte.

Art. 14. No caso de documentos arquivísticos, a eliminação deve ser efetuada de maneira a garantir a impossibilidade de recuperação posterior de qualquer documento descartado.

Parágrafo único. Todas as cópias dos documentos eliminados, incluindo cópias de segurança e cópias de preservação, independentemente do suporte, devem ser destruídas.

CAPÍTULO IV
DOS TIPOS DE BACKUP

Art. 15. A seleção dos tipos de backups integra a definição da estratégia de proteção de dados de uma organização. Na ANA, as estratégias de backup devem ser estabelecidas e mantidas conforme os seguintes tipos de backup:

I – Completo: backup que copia todos os arquivos, pastas ou volumes para destinos estabelecidos, como servidores, sistemas ou nuvem computacional;

II – Incremental: backup que copia apenas os dados alterados ou adicionados desde o último backup completo ou incremental já realizado; e

III – Diferencial: backup que compara o conteúdo do backup existente com o último evento para gravar somente as alterações realizadas.

Art. 16. A definição da frequência dos backups impacta diretamente a capacidade da organização de recuperar dados em caso de perda. Nesse sentido, a frequência para a realização dos backups deve ser determinada com base nas necessidades específicas da ANA e no impacto da perda de dados.

§ 1º As estratégias de backup devem ser programadas preferencialmente de forma automática, em horários de menor ou nenhuma utilização dos recursos, serviços, sistemas e rede computacional.

§ 2º Os backups devem ser realizados conforme as seguintes frequências:

I – Diariamente: backups de dados, bases de dados e sistemas críticos, iniciados preferencialmente a partir das 23 horas;

II – Mensalmente: backups de bases de dados e sistemas críticos, realizados até o último dia do mês, preferencialmente a partir das 23 horas;

III – Semestralmente: backups de máquinas virtuais/servidores e infraestrutura de rede, realizados até o último dia do semestre, preferencialmente a partir das 23 horas; e

IV – Anualmente: backups de máquinas virtuais/servidores e infraestrutura de rede, realizados até o último dia do ano, preferencialmente a partir das 23 horas.

CAPÍTULO V
DA PERIODICIDADE

Art. 17. Os dados críticos, tais como banco de dados, arquivos de dados e sistemas críticos devem ter backups realizados considerando as estratégias a seguir:

I – os backups diários deverão ser executados de segunda à domingo, preferencialmente a partir das 23 horas, em modo incremental, diferencial e completo, com retenção de 7 dias, conforme disponibilidade de recursos tecnológicos;

II – os backups semanais deverão ser executados nos finais de semana, iniciando aos sábados e domingos, em modo completo de acordo com a especificidade de cada serviço ou sistema de informação, conforme disponibilidade de recursos tecnológicos;

III – os backups mensais deverão ser executados no último dia do mês, em modo completo, com retenção nos 12 (doze) últimos meses, quando houver recursos disponíveis; e

IV – os backups completos anuais deverão ser executados no mês de dezembro, com retenção do último ano, quando houver recursos tecnológicos disponíveis.

CAPÍTULO VI
DO USO DA REDE

Art. 18. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados, assegurando que o tráfego gerado por essas atividades não ocasione indisponibilidade dos demais serviços de TI, evitando problemas de desempenho da rede e garantindo a integridade dos dados armazenados.

§ 1º As estratégias de backup devem ser elaboradas levando em consideração a largura de banda disponível, a frequência das cópias e os requisitos de retenção de dados.

§ 2º A execução das rotinas de backup deve ser agendada, preferencialmente, em períodos de menor tráfego na rede, fora do horário comercial, a fim de minimizar impactos no desempenho dos sistemas.

§ 3º Devem ser empregadas técnicas de compactação e deduplicação para reduzir o volume de dados transferidos, otimizando o uso da largura de banda.

§ 4º Os dados devem ser criptografados para garantir a segurança durante a transferência pela rede.

§ 5º A priorização de dados críticos deve ser estabelecida para viabilizar sua recuperação de forma mais ágil, quando necessário.

§ 6º Ferramentas de monitoramento de rede devem ser implementadas para acompanhar o consumo de largura de banda durante a realização dos backups, permitindo a identificação de gargalos e problemas de desempenho.

§ 7º A segmentação da rede deve ser considerada como estratégia para isolar o tráfego de backup das demais atividades, evitando interferências.

§ 8º Testes de carga devem ser realizados periodicamente para avaliar o impacto das rotinas de backup na rede e possibilitar ajustes na programação e nas configurações, conforme necessário.

CAPÍTULO VII
DO ARMAZENAMENTO

Art. 19. Os backups devem ser armazenados em locais isolados dos sistemas de produção, garantindo sua proteção contra eventos que possam comprometer os sistemas primários, como ataques de ransomware, podendo envolver armazenamento em nuvem computacional, locais físicos separados ou

outras estratégias de isolamento.

§ 1º Os backups devem ser armazenados de forma segura, assegurando proteção contra acesso não autorizado e ameaças cibernéticas.

§ 2º Com o objetivo de prover redundância de dados e sistemas e garantir a continuidade do negócio em caso de desastre, a ANA deve, sempre que possível, adotar os seguintes locais para armazenamento de cópias de segurança:

I – Local: armazenamento dentro da sala segura da ANA, como discos rígidos ou servidores dedicados, proporcionando recuperação ágil, porém suscetível a falhas locais, como incêndios, tempestades, inundações ou roubo;

II – Nuvem computacional: armazenamento em servidores remotos de data centers de provedores de serviço ou instituições parceiras, oferecendo escalabilidade, redundância e proteção contra desastres locais, mas exigindo largura de banda para a transferência de dados; e

III – Híbrido: combinação do backup local com o armazenamento em nuvem, permitindo rápida recuperação de dados locais aliada à proteção contra desastres proporcionada pelo ambiente em nuvem.

CAPÍTULO VIII
DOS PROCEDIMENTOS DE BACKUP

Art. 20. Os procedimentos para a realização de backups e restauração de dados devem, sempre que possível, ser automatizados e devidamente documentados, observando os requisitos de privacidade e segurança da informação, sendo atualizados sempre que ocorrer:

I – Desenvolvimento de novas aplicações;

II – Criação ou disponibilização de novos locais de armazenamento de dados ou arquivos;

III – Identificação de novos arquivos relevantes para o funcionamento do serviço;

IV – Instalação ou configuração de novos bancos de dados;

V – Instalação de novos aplicativos; e

VI – Inclusão de outras informações que exijam proteção por meio de backups.

Parágrafo único. Em caso de falha em algum procedimento de backup ou impossibilidade de sua execução, o administrador de backup deve adotar as providências necessárias para garantir a salvaguarda das informações por meio de outro mecanismo, como a reexecução do backup em horário comercial ou a cópia dos dados para outro servidor.

CAPÍTULO IX
DOS PLANOS DE BACKUP

Art. 21. A ANA deve estabelecer planos de backup específicos para cada recurso, base de dados, sistema de informação e serviço de TI, garantindo sua efetividade mediante a observância, no mínimo, dos seguintes aspectos:

I – Identificação dos arquivos de dados, diretórios, serviços e sistemas a serem copiados;

II – Definição das bases de dados que devem ser incluídas no backup;

III – Determinação dos arquivos de configuração a serem copiados;

IV – Especificação dos arquivos de logs do sistema que devem ser preservados;

V – Detalhamento dos procedimentos necessários para a recuperação dos backups;

VI – Definição da frequência para a realização das cópias de segurança;

VII – Estabelecimento do tipo de cópia a ser realizada (completa, diferencial ou incremental);

VIII – Determinação do tempo de retenção dos backups;

IX – Consideração dos requisitos específicos de segurança da informação aplicáveis;

X – Definição do local de armazenamento dos backups; e

XI – Planejamento dos procedimentos de testes e recuperação das cópias de segurança.

Parágrafo único. Os Curadores de Dados de Negócio devem ser consultados para garantir que os dados sob responsabilidade de suas respectivas áreas organizacionais estejam devidamente contemplados no plano de ba*ckup*.

CAPÍTULO X
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Art. 22. Cada unidade é responsável por definir os procedimentos relativos ao backup e à restauração de dados. No processo de gerenciamento de backups, são estabelecidos os seguintes papéis e responsabilidades:

I – Responsável pela unidade: servidor encarregado da gestão da equipe na unidade, com as seguintes atribuições:

a) Definir procedimentos e orientações complementares para a aplicação das disposições estabelecidas nesta política;

b) Estabelecer e manter atualizado o plano de gestão de backups da unidade; e

c) Gerenciar a realização de testes periódicos de restauração, a fim de avaliar a efetividade dos processos de backup e promover melhorias.

II – Administrador de backup: servidor da área de TI responsável pela definição, manutenção, testes e auditoria de backups, sendo suas atribuições:

a) Propor e manter atualizadas as diretrizes e os procedimentos relativos aos serviços de backup e restauração de dados;

b) Propor soluções para a cópia de segurança das informações digitais institucionais produzidas ou custodiadas pela ANA; e

c) Definir modelos de documentos para todo o processo de gestão de backups.

III – Responsável pelo serviço: pessoa encarregada de definir os dados que devem constar nos backups periódicos, com as seguintes responsabilidades:

a) Definir, em conjunto com a área de negócios, os requisitos de backup e retenção de dados para os sistemas ou serviços desenvolvidos ou implantados na ANA;

b) Informar ao Administrador de Backup qualquer inclusão, alteração ou exclusão de procedimentos e rotinas de backup do serviço;

c) Verificar periodicamente a rotina do serviço, identificando eventuais falhas que possam interferir nos procedimentos de backup;

d) Acompanhar, em conjunto com o Administrador de Backup, a execução das rotinas de backup do serviço, mitigando inconsistências;

e) Comunicar ao Administrador de Backup qualquer mudança no serviço, como alteração de endereço de servidor, credenciais de acesso ou outras modificações que possam impactar a rotina de backup;

f) Propor ajustes para o aperfeiçoamento da política de backup;

g) Realizar testes periódicos de restauração de dados, em conjunto com o Administrador de Backup, para assegurar a eficácia dos procedimentos;

h) Responder formalmente por eventuais danos decorrentes da perda de dados do serviço;

i) Armazenar os backups em local apropriado;

j) Realizar manutenções periódicas nos dispositivos de backup;

k) Comunicar ao responsável pelo serviço eventuais falhas ou anomalias identificadas nos procedimentos de backup e restauração;

l) Restaurar os backups quando necessário;

m) Configurar e manter atualizado o software de gerenciamento de backups;

n) Criar e manter procedimentos relativos aos serviços de backup e restauração, assegurando o cumprimento das normas aplicáveis;

o) Desenvolver e manter scripts para backup e restauração de dados;

p) Garantir a realização de backups dos sistemas formalmente solicitados;

q) Criar e testar scripts de criação e restauração de dados;

r) Monitorar periodicamente os relatórios gerados pelo software de backup;

s) Gerenciar mensagens e logs diários dos backups, tratando eventuais falhas para garantir a continuidade dos procedimentos;

t) Propor melhorias na política de backup;

u) Documentar os processos de geração, teste, armazenamento e recuperação das cópias de segurança corporativa;

v) Manter documentação referente aos backups, incluindo planos operacionais, registros de execução, monitoramento e testes;

w) Realizar e controlar o inventário de backups; e

x) Executar testes periódicos de restauração, em conjunto com o responsável pelo serviço, para avaliar a efetividade dos procedimentos e implementar melhorias.

IV – Usuário: pessoa que utiliza os recursos, sistemas e serviços disponibilizados pela ANA, tendo as seguintes responsabilidades:

a) realizar periodicamente backup dos dados armazenados em equipamentos da ANA sob sua responsabilidade;

b) higienizar o servidor de arquivos da ANA, removendo arquivos desnecessários e, no caso de múltiplas versões, mantendo apenas a versão mais recente; e

c) descartar arquivos com mais de cinco anos que não possuam utilidade para a unidade ou para efeitos regulatórios, ressalvados os documentos arquivísticos produzidos ou recebidos no curso das atividades institucionais, cujo prazo de guarda e destinação constam na Tabela de Temporalidade e Destinação de Documentos das Atividades-meio e Fim da ANA, conforme disposto na Resolução ANA nº 752, de 8 de maio de 2017, ou norma que vier a sucedê-la.

CAPÍTULO XI
DAS PENALIDADES

Art. 23. O descumprimento desta política estará sujeito a investigação e poderá resultar na aplicação de sanções administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Parágrafo único. Os casos omissos não contemplados neste documento serão submetidos à análise e decisão da Câmara de Governança Digital e Segurança da Informação e Comunicações (CGDI).

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 24. Esta política, assim como os documentos derivados dela, deverá ser revisada, aprovada e atualizada sempre que houver alterações na legislação da administração pública federal, mudanças nas políticas e normas internas da ANA, ou sempre que a CGDI considerar necessário.

Art. 25. As regras, procedimentos, medidas e controles para a gestão de backups serão detalhados em normas internas complementares, as quais especificarão suas particularidades e procedimentos relacionados à segurança da informação, alinhados às diretrizes emanadas pela CGDI e aos respectivos planos institucionais e à estrutura organizacional da ANA.

§ 1º Esta política, suas atualizações e as normas internas complementares devem ser amplamente divulgadas a todos os usuários, a fim de promover sua observância, seu conhecimento e a formação de uma cultura em relação ao backup dos dados.

§ 2º A alta administração deverá disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

Art. 26. Esta política entra em vigor na data de sua publicação.