

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES**RESOLUÇÃO INTERNA ANATEL Nº 184, DE 13 DE JANEIRO DE 2023**

Dispõe sobre Retenção, Descarte e Restauração de Dados da Agência Nacional de Telecomunicações - Anatel.

O CONSELHO DIRETOR DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES uso das atribuições que lhe foram conferidas pelo art. 133 do Regimento Interno da Anatel, aprovado pela [Resolução nº 612, de 29 de abril de 2013](#),

CONSIDERANDO os princípios, objetivos e diretrizes referentes à Política de Segurança da Informação e Comunicações da Anatel (POSIC/Anatel), aprovada pela Resolução Interna nº 17, de 18 de maio de 2021;

CONSIDERANDO o disposto na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a responsabilidade da Comissão de Segurança da Informação e Comunicações da Anatel (CSIC/Anatel) de propor normas e procedimentos inerentes à Segurança da Informação e Comunicações;

CONSIDERANDO a necessidade de preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações produzidas e custodiadas pela Anatel;

CONSIDERANDO as obrigações estabelecidas no Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, e suas alterações pelo Decreto nº 9.832, de 12 de junho de 2019;

CONSIDERANDO as orientações para Gestão de Segurança da Informação e Comunicações, que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta, contidas na Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 27 de maio de 2020, e em suas respectivas Normas Complementares;

CONSIDERANDO as orientações para Credenciamento de Segurança para o Tratamento de Informação Classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal, contidas na Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, e suas respectivas Normas Complementares;

CONSIDERANDO as orientações para execução dos processos relacionados à Gestão de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, contidas na Instrução Normativa nº 03 do Gabinete de Segurança Institucional, de 28 de maio de 2021;

CONSIDERANDO as recomendações constantes nas normas técnicas NBR ISO/IEC 27001:2013 – Sistema de Gestão de segurança da informação e NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação;

CONSIDERANDO a decisão tomada por meio do Circuito Deliberativo nº 12, de 12 de janeiro de 2023;

CONSIDERANDO o constante dos autos do Processo nº 53500.039267/2021-55,

RESOLVE:

Art. 1º Aprovar a Norma de Segurança para Retenção, Descarte e Restauração de Dados da Agência Nacional de Telecomunicações - Anatel.

Art. 2º Esta Resolução Interna entra em vigor em 1º de fevereiro de 2023.



Documento assinado eletronicamente por **Carlos Manuel Baigorri, Presidente**, em 13/01/2023, às 12:15, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da [Portaria nº 912/2017](#) da Anatel.



A autenticidade deste documento pode ser conferida em <http://www.anatel.gov.br/autenticidade>, informando o código verificador **9682145** e o código CRC **41F2BCBE**.

ANEXO

NORMA DE SEGURANÇA PARA RETENÇÃO, DESCARTE E RESTAURAÇÃO DE DADOS DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES - ANATEL

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Norma de Segurança se aplica aos usuários que realizem atividades que envolvam tratamento de dados custodiados pela Agência e seus registros eletrônicos ou físicos.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os fins desta Norma de Segurança, considera-se:

I - **appliance** de **backup** em disco: **hardware** especialmente desenvolvido para armazenar dados de **backup** em discos usualmente com deduplicação embutida;

II - **backup**: cópia de segurança de um dispositivo de armazenamento para outro para que possa ser restaurado em caso da perda dos dados originais;

III - **backup “off-site”**: localidade de armazenamento de **backup** diversa da origem dos dados;

IV - mídia: meio físico no qual efetivamente armazenam-se os dados de um **backup**;

V - restauração (**restore**): recuperação de dados a partir de um **backup** funcional armazenado; e,

VI - retenção: preservação de conteúdo de mídia por determinado período de tempo.

CAPÍTULO III

DAS DIRETRIZES

Seção I

Da Cópia de Segurança (**backup**) e da Restauração (**restore**) de Dados

Subseção I

Estratégia e Orientações

Art. 3º As ações de Tecnologia da Informação deverão alinhar-se à estratégia institucional e às melhores práticas, observada a seguinte estratégia geral de **backup e restore**:

I - o serviço de **backup** deverá ser orientado para a restauração das informações no menor tempo possível, principalmente nos casos de indisponibilidade de serviços que dependam da operação de **restore**;

II - os recursos adequados para a geração dos **backups** devem ser disponibilizados pela Superintendência de Gestão Interna da Informação - SGI para assegurar que todos os dados e aplicações essenciais possam ser recuperados após um incidente ou desastre; e,

III - as unidades gestoras dos sistemas, dados e infraestrutura de Tecnologia da Informação deverão estar atualizadas em relação às informações geradas pelo processo de **backup** e restauração.

§ 1º A estratégia de que trata o **caput** basear-se-á em 3 (três) etapas:

I - catalogação dos servidores de dados (banco de dados / aplicações / serviços);

II - levantamento dos requisitos dos ambientes; e,

III - implementação do processo de **backup e restore**.

§ 2º As unidades gestoras de sistemas e dados serão responsáveis por mapear as dependências de funcionamento das aplicações, serviços e bases de dados.

Art. 4º As ações de Tecnologia da Informação relativas ao **backup e restore** de dados deverão seguir as seguintes orientações:

I - a administração dos **backups** deverá ser orientada para que as atividades respeitem as janelas de execução, inclusive prevendo a ampliação da capacidade dos dispositivos de armazenamento;

II - os dispositivos de armazenamento dos **backups** (fitas ou **appliance** de **backup** em disco), dos sistemas classificados como críticos, deverão ser acondicionados em ambiente com estrutura obediente à norma ABNT NBR ISO/IEC 27002:2013, em localidade diversa da origem dos dados (**backup "offsite"**);

III - os ambientes de armazenamento de dados e de cópias de segurança deverão estar situados em locais distintos, com pelo menos uma cópia dos dados produtivos, de forma a mitigar a possibilidade de que os danos de um desastre ocorrido no site principal afetem o site secundário;

IV - as mídias defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros;

V - os procedimentos de **backup** serão realizados, diariamente, preferencialmente durante o período noturno, entre 20h (vinte horas) e 6h (seis horas) do dia seguinte;

VI - os arquivos e documentos corporativos gerados pelos usuários e que necessitem integrar a rotina de **backup** deverão ser armazenados nos repositórios corporativos;

VII - os administradores de sistemas em conjunto com os administradores de **backup** deverão realizar testes periódicos de restauração, no intuito de averiguar os processos de **backup** e estabelecer melhorias;

VIII - os arquivos armazenados nas estações de trabalho não integram o escopo do processo de **backup** e não estarão disponíveis para recuperação, em caso de perda temporária ou definitiva do arquivo; e,

IX - as ações de Tecnologia de Informação que envolvam a geração de cópias de segurança e a restauração de dados deverão vincular-se às boas práticas derivadas da observância dos normativos internos e externos.

Subseção II

Dos Papéis e Competências

Art. 5º A execução das ações de Cópia de Segurança e Restauração de Dados da Anatel pautar-se-á na definição e distribuição de competência e responsabilidades entre as unidades organizacionais da Agência e será composto pelos seguintes agentes:

I - Comissão de Segurança da Informação e Comunicações;

II - Superintendência de Gestão Interna da Informação - SGI; e,

III - Curadorias de Dados.

Art. 6º O alinhamento da governança de TIC às estratégias e diretrizes relacionadas à cópia de segurança e restauração de dados da Anatel é de responsabilidade da Comissão de Segurança da Informação e Comunicações e da Superintendência de Gestão Interna da Informação - SGI, que prestarão todo o suporte necessário à tomada de decisão dos processos de **backup** e restauração objeto desta Resolução Interna.

Art. 7º Compete à Comissão de Segurança da Informação e Comunicações:

I - aprovar a proposta de diretrizes referentes a ações e projetos de **backup** e **restore** dos dados gerados ou sob a guarda da Anatel;

II - avaliar e decidir sobre questões de segurança vinculadas às cópias de segurança, respeitando o disposto na Política de Segurança da Informação e Comunicações - POSIC/Anatel e suas normas complementares; e,

III - avaliar a conformidade da execução das diretrizes estabelecidas nesta Norma de Segurança.

Art. 8º Compete à Superintendência de Gestão da Informação - SGI:

I - estabelecer as regras para a gestão das cópias de segurança e restauração de dados;

II - prevenir a divulgação não autorizada, modificação, remoção, eliminação, descarte ou destruição dos dados armazenados nos **backups**;

III - elaborar e publicar procedimentos de comunicação de falhas de **backup**;

IV - elaborar e publicar procedimentos de recuperação de incidentes de **backup**;

V - elaborar e publicar procedimentos de descarte de dispositivos de armazenamento de dados fora do prazo de retenção e/ou inservíveis;

VI - elaborar o catálogo do cenário atual da solução de **backup**, que inclua inventário dos ativos disponíveis para armazenamento, servidores envolvidos nos processos de **backup** e softwares utilizados, com a finalidade de se ter conhecimento dos riscos aos quais os dados estão sujeitos, os problemas e demais não conformidades encontradas;

VII - definir um período de retenção das cópias dos logs das operações de **backup**, para fins de futuras investigações e monitoramento de controle de acesso das ferramentas de **backup** e restauração;

VIII - armazenar as cópias de segurança dos dados classificados como críticos em uma localidade remota, a uma distância segura para mitigar os danos de um desastre ocorrido no site principal; e,

IX - realizar testes de restauração em periodicidade a ser definida.

Art. 9º Compete à Curadoria de Dados participar da elaboração dos Planos de Recuperação de Desastres e de Recuperação de Incidentes.

Parágrafo único. Na ausência de designação formalizada do curador, as responsabilidades

deverão ser desempenhadas pelos gestores de sistemas.

Art. 10. As solicitações de restauração de dados deverão ser realizadas diretamente para a Superintendência de Gestão Interna da Informação - SGI.