AGÊNCIA NACIONAL DE ASSISTÊNCIA TÉCNICA E EXTENSÃO RURAL

RESOLUÇÃO DIREX Nº 8/2026

Aprova a Política de Privacidade e Segurança da Informação no âmbito da Agência Nacional de Assistência Técnica e Extensão Rural (Anater).

A **DIRETORIA EXECUTIVA DA ANATER** , no uso das atribuições que lhe confere o artigo 19, inciso X, do Estatuto Social da Anater e de acordo com o constante no processo SEI nº 21490.000438/2026-31, resolve:

Art. 1º Aprovar, na forma do Anexo I desta Resolução, a Política de Privacidade e Segurança da Informação no âmbito da Agência Nacional de Assistência Técnica e Extensão Rural (Anater).

Art. 2º Os casos omissos serão solucionados pela Diretoria Executiva - Direx, com fundamento na legislação aplicável, nos princípios e nas diretrizes da Política de Privacidade e Segurança da Informação.

Parágrafo único. A Direx poderá expedir normas complementares para orientar a aplicação desta Política.

Art. 3º Integram a Política de Privacidade e Segurança da Informação, para todos os fins, os Anexos II a VI, que a complementam e possuem caráter normativo complementar e vinculante.

§ 1º As unidades da Anater deverão adotar e utilizar, conforme aplicável, os instrumentos constantes dos Anexos da Política:

I - Termo de Compromisso, Sigilo e Confidencialidade aplicável a pessoa física (Anexo II);

II - Termo de Compromisso, Sigilo e Confidencialidade aplicável a pessoa jurídica (Anexo III);

III - Formulário de Comunicação de Incidente de Segurança de Dados Pessoais à Autoridade Nacional de Proteção de Dados – ANPD (Anexo IV); e

IV - Comunicação ao Titular de Dados Pessoais em caso de Incidente de Segurança (Anexo V);

V - Termo de Consentimento para Uso de Imagem, Voz e Tratamento de Dados Pessoais (Anexo VI).

§ 2º Os modelos mencionados no *caput* poderão ser adaptados, conforme a finalidade e as especificidades do caso concreto, desde que preservados o conteúdo essencial e a finalidade dos instrumentos, observado o disposto na Política e na legislação aplicável, em especial a LGPD.

Art. 4º Esta Resolução entra em vigor na data de sua assinatura.

Brasília, data da assinatura eletrônica.

SÉRGIO ROSA

Diretor Administrativo

ISABEL CRISTINA LOURENÇO DA SILVA

Diretora Técnica

LOROANA COUTINHO DE SANTANA

Presidente

ANEXO I

POLÍTICA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Privacidade e Segurança da Informação (PPSI) da Anater, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e controles para:

I - proteção das informações institucionais;

II - tratamento adequado de dados pessoais;

III - mitigação de riscos de segurança;

IV - prevenção e resposta a incidentes; e

V - promoção da governança em segurança da informação.

§ 1º Esta Política aplica-se a todos os dados e informações tratados no âmbito da Agência, incluindo dados pessoais e dados pessoais sensíveis, bem como dados de crianças e adolescentes, nos termos da legislação vigente.

§ 2º As disposições desta Política possuem caráter transversal e deverão ser observadas em todas as políticas internas, contratos, projetos, programas, processos e demais instrumentos institucionais.

Art. 2º Esta Política aplica-se a:

I - todos os ativos de informação da Anater, incluindo dados, sistemas, aplicativos, dispositivos, redes e demais recursos de tecnologia da informação;

II - todas as atividades finalísticas, administrativas e de suporte da Agência que envolvam a coleta, recepção, produção, classificação, acesso, utilização, reprodução, processamento, armazenamento, eliminação, transmissão, arquivamento, modificação, avaliação, comunicação ou qualquer outra forma de tratamento de dados pessoais;

III - todos os usuários que, direta ou indiretamente, tenham acesso às informações da Agência, abrangendo empregados, colaboradores, estagiários, consultores, prestadores de serviço, parceiros e terceiros; e

IV - todas as unidades, instalações físicas e ambientes sob gestão ou utilização da Anater bem como às atividades realizadas em seu nome.

Art. 3º Os prestadores de serviços, parceiros e terceiros que atuem em nome da Anater sujeitam-se às disposições desta Política em todas as fases de execução de suas atividades, respondendo por eventuais incidentes de segurança decorrentes de ação ou omissão.

Art. 4º Os contratos, convênios e instrumentos congêneres deverão conter cláusulas específicas que assegurem, no mínimo:

I - a obrigatoriedade de observância desta Política e das normas complementares de segurança da informação;

II - a vedação à instalação, execução ou utilização de programas, sistemas ou rotinas não

autorizados pela Anater; e

III - a responsabilização do contratado por danos ou incidentes de segurança de dados decorrentes do descumprimento das diretrizes estabelecidas.

CAPÍTULO II
DOS TERMOS E DEFINIÇÕES

Art. 5º Para efeitos desta norma, considera-se:

I - agentes de tratamento: o controlador e o operador da Anater;

II - ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição;

III - arquivo de log: registra as atividades de um programa desde o momento em que é aberto;

IV - ativo: qualquer informação que tenha valor para a Instituição;

V - autenticidade: garantia de veracidade da fonte de informações. Por meio da autenticidade, é possível confirmar a identidade das pessoas ou entidades que prestam a informação;

VI - backup: processo de guardar informações importantes para recuperá-las futuramente no caso de algum problema ou necessidade;

VII - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

VIII - conflito de interesse: a situação que possa comprometer, influenciar ou afetar, de maneira imprópria, a objetividade e o julgamento técnico no desempenho das atribuições do encarregado;

IX - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

X - controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XI - correio eletrônico: meio de comunicação baseado no envio e na recepção de mensagens, via rede de computadores;

XII - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

XIII - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XIV - datacenter: ambiente projetado para concentrar os equipamentos de processamento e armazenamento de dados de uma empresa;

XV - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XVI - dispositivos móveis: quaisquer equipamentos eletrônicos portáteis para processamento de dados, armazenamento e comunicação, como notebooks, tablets, smartphones e consoles portáteis;

XVII - download: ato de baixar um arquivo ou documento de outro computador, via internet;

XVIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de

comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XIX - gestor: agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas de uso da informação;

XX - Incidente de segurança da informação: evento confirmado ou sob suspeita que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de informações ou ativos de informação da Anater.

XXI - Incidente de segurança com dados pessoais: incidente de segurança da informação que envolva, afete ou possa afetar dados pessoais tratados pela Anater, com potencial de acarretar risco ou dano relevante aos titulares.

XXII - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXIII - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXIV - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XXV - pirataria digital: prática que envolve cópia ilegal de conteúdo, arquivo ou software protegido por direitos autorais;

XXVI - privacidade: direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas;

XXVII - recursos de tecnologia da informação: qualquer sistema, serviço, infraestrutura de Tecnologia da Informação ou instalações físicas direta ou indiretamente administrados, mantidos ou operados pela empresa;

XXVIII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XXIX - risco: combinação da probabilidade de ocorrência de um evento e de suas consequências;

XXX - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXI - serviços de streaming: modalidade de disponibilização de conteúdo multimídia em fluxo contínuo, por meio de redes de computadores, especialmente a internet, que permite o acesso ao conteúdo sem a necessidade de download integral prévio;

XXXII - sítio eletrônico: conjunto de páginas disponíveis na internet, contendo informações, imagens, vídeos, sons e outros conteúdos digitais, armazenados em servidores e acessíveis por meio de rede de computadores;

XXXIII - spam: mensagem eletrônica não solicitada, que geralmente é enviada para grande número de pessoas;

XXXIV - termo de compromisso, sigilo e confidencialidade: documento com validade jurídica, que acorda confidencialidade e não divulgação de informações confidenciais e atribui responsabilidades ao usuário;

XXXV - titular do dado: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXXVI - transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XXXVII - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição,

processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XXXVIII - upload: envio de arquivo de um computador para outro via internet;

XXXIX - usuário: empregados, colaboradores, consultores, temporários, estagiários, prestadores de serviços, parceiros, e demais usuários que estejam a serviço da Anater; e

XL - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III

DA ABRANGÊNCIA E OBJETIVOS

Art. 6º Esta Política tem por objetivos:

I - estabelecer um modelo de governança para a segurança da informação e o cumprimento de obrigações legais e contratuais relacionadas ao tratamento de dados pessoais no âmbito da Anater;

II - assegurar a proteção dos ativos de informação e dos dados pessoais sob sua responsabilidade;

III - reduzir a exposição a riscos e fortalecer a capacidade de prevenção, detecção e resposta a incidentes;

IV - promover o uso adequado e responsável dos recursos de tecnologia da informação;

V - assegurar a conformidade com a legislação e normas aplicáveis;

VI - fomentar a cultura institucional de segurança da informação e de proteção de dados pessoais entre empregados, colaboradores, estagiários, consultores, prestadores de serviço, parceiros e terceiros;

VII - garantir o tratamento de dados pessoais de forma transparente, ética, legítima e segura, respeitando os direitos dos titulares e os princípios da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD); e

VIII - definir responsabilidades institucionais no tratamento de dados pessoais, incluindo as atribuições do controlador, operador, encarregado e demais agentes internos ou externos envolvidos.

Parágrafo único. Para fins desta Política, consideram-se recursos de tecnologia da informação os equipamentos, sistemas, aplicações, redes e demais ativos de informação administrados ou utilizados pela Anater, cuja utilização e proteção deverão assegurar o tratamento adequado e seguro de dados pessoais, em conformidade com a LGPD e demais normas aplicáveis de segurança da informação e proteção de dados.

CAPÍTULO IV

DOS PRINCÍPIOS E DIRETRIZES

Seção I

Princípios

Art. 7º As ações observarão os seguintes princípios:

I - proteção da informação, considerando sua confidencialidade, integridade e disponibilidade;

II - continuidade dos processos e serviços essenciais;

III - proporcionalidade entre riscos e controles adotados;

IV - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V - observância da publicidade e transparência como preceito geral e do sigilo como exceção;

VI - responsabilização pelo uso e tratamento das informações;

VII - economicidade da proteção dos ativos de informação; e

VIII - conformidade com a legislação e normas aplicáveis.

Seção II

Diretrizes

Art. 8º A implementação da PPSI observará as seguintes diretrizes:

I - adoção de práticas de governança e gestão de riscos aplicadas à segurança da informação;

II - definição de papéis, responsabilidades e controles relacionados ao uso dos ativos de informação;

III - integração da segurança da informação aos processos, projetos e soluções institucionais;

IV - adoção de medidas proporcionais à criticidade dos ativos e aos riscos identificados;

V - monitoramento, registro e análise de eventos relacionados à segurança da informação;

VI - promoção de ações contínuas de capacitação e conscientização dos usuários; e

VII - melhoria contínua dos controles e processos de segurança da informação.

CAPÍTULO V

DA GOVERNANÇA

Seção I

Composição

Art. 9º A governança da PPSI é composta por:

I - Diretoria Executiva da Anater (Direx);

II - Unidade de Tecnologia da Informação;

III - Encarregado pelo Tratamento de Dados Pessoais;

IV - Ouvidoria; e

V - Unidades integrantes da estrutura organizacional da Anater.

§ 1º A estrutura de governança prevista neste Capítulo viabiliza o cumprimento das atribuições da Anatercomo controladora de dados pessoais, nos termos da legislação aplicável.

§ 2º As atribuições decorrentes da atuação da Anater como controladora, bem como dos operadores e do encarregado, serão exercidas em conformidade com a estrutura de governança prevista neste Capítulo.

Seção II

Competências

Art. 10. Compete à Direx:

I - formalizar e aprovar esta Política, bem como suas alterações e atualizações;

II - assegurar recursos para sua implementação;

III - estabelecer diretrizes para a atualização dos instrumentos de governança em privacidade e proteção de dados;

IV - deliberar sobre normas e ações de segurança da informação;

V - assegurar a proteção adequada dos dados tratados no âmbito institucional;

VI - assegurar a existência de canal para atendimento de titulares e comunicação institucional; e

VII - constituir grupos de trabalho ou comitês para temas relacionados à segurança da informação e à proteção de dados pessoais.

Parágrafo único. A criação de grupos de trabalho ou comitês será deliberada pela Direx, mediante justificativa e definição de escopo, objetivos e prazo, e sua composição e formalização ocorrerão por ato do(a) Presidente da Anater, nos termos das normas internas aplicáveis.

Art. 11. Compete à Unidade de Tecnologia da Informação:

I - coordenar a implementação e a manutenção da PPSI, assegurando a adoção de medidas preventivas e corretivas para mitigação de riscos;

II - propor a atualização desta Política e das normas internas correlatas, com base na evolução tecnológica e na análise de riscos;

III - assessorar a implementação das diretrizes de segurança da informação;

IV - promover a divulgação da Política de Segurança da Informação e das normas internas, bem como apoiar ações de conscientização dos usuários, em articulação com as unidades competentes;

V - configurar, atualizar e manter os ativos de tecnologia da informação, incluindo hardware e software, em conformidade com os padrões de segurança estabelecidos;

VI - implementar e manter mecanismos de proteção contra códigos maliciosos e outras ameaças à segurança da informação;

VII - gerenciar a capacidade dos recursos de tecnologia da informação relacionados ao processamento, armazenamento e comunicação de dados, com vistas à segurança e continuidade dos serviços;

VIII - controlar e administrar os acessos aos sistemas, redes e bases de dados, assegurando a identificação, autenticação e rastreabilidade dos usuários;

IX - realizar o monitoramento contínuo dos ambientes tecnológicos, incluindo redes, sistemas e serviços, com vistas à detecção e resposta a incidentes de segurança da informação;

X - registrar, tratar e comunicar incidentes de segurança da informação, observados os procedimentos estabelecidos;

XI - elaborar e disponibilizar relatórios gerenciais sobre a segurança da informação, contemplando eventos relevantes, riscos identificados e recomendações de melhoria;

XII - manter integração com a unidade responsável pela gestão de pessoas para fins de concessão, revisão e revogação de acessos, especialmente nos casos de desligamento ou movimentação de usuários;

XIII - atuar em conjunto com as unidades organizacionais na definição e adoção de procedimentos relacionados ao tratamento da informação, visando à efetividade dos controles de segurança; e

XIV - manter atualizados os procedimentos e controles de segurança da informação, em consonância com as diretrizes institucionais e a evolução do ambiente tecnológico.

Art. 12. Compete ao Encarregado pelo tratamento de dados pessoais:

I - receber, analisar e responder às solicitações dos titulares de dados pessoais, diretamente ou por intermédio da Ouvidoria, quando recebidas por aquele canal;

II - receber comunicações da Autoridade Nacional de Proteção de Dados – ANPD e orientar a adoção das medidas cabíveis;

III - orientar empregados, colaboradores e contratados quanto às práticas de proteção de dados pessoais e às diretrizes institucionais de privacidade;

IV - coordenar, sob a ótica da proteção de dados pessoais, a resposta institucional a incidentes de segurança que envolvam dados pessoais, em articulação com a Unidade de Tecnologia da Informação e demais áreas competentes;

V - apoiar a elaboração, revisão e atualização de instrumentos de governança em privacidade, incluindo relatórios de impacto à proteção de dados pessoais (RIPD), avisos de privacidade, normativos internos e cláusulas contratuais;

VI - elaborar o RIPD, o qual deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados;

VII - acompanhar e orientar a implementação de medidas de mitigação de riscos relacionados ao tratamento de dados pessoais;

VIII - promover a avaliação contínua do nível de maturidade em privacidade, orientando os gestores responsáveis quanto à conformidade com a legislação; e

IX - exercer outras atribuições previstas em normas legais e regulamentares aplicáveis.

§ 1º O Encarregado pelo Tratamento de Dados Pessoais atuará como canal de comunicação entre a Anater, os titulares de dados e a ANPD, sendo designado pelo(a) Presidente da Anater.

§ 2º A identidade e as informações de contato do Encarregado deverão ser divulgadas, de forma clara e acessível no sítio eletrônico da Anater.

§ 3º Nas hipóteses de ausência, impedimento ou vacância do Encarregado pelo Tratamento de Dados Pessoais, suas atribuições serão exercidas por substituto formalmente designado pelo(a) Presidente da Anater.

Art. 13. Compete à Ouvidoria:

I - receber e tratar manifestações relacionadas à proteção de dados pessoais, devendo encaminhá-las ao Encarregado pelo tratamento de dados pessoais para análise e manifestação técnica, quando envolverem direitos dos titulares previstos na LGPD;

II - atuar de forma articulada com o Encarregado (DPO) no atendimento às demandas relativas à privacidade;

III - encaminhar às unidades competentes as manifestações que envolvam incidentes de segurança da informação ou possíveis violações de dados pessoais;

IV - apoiar a transparência ativa e passiva quanto às práticas de proteção de dados; e

V - contribuir para a melhoria contínua dos serviços relacionados à privacidade e à segurança da informação, a partir das manifestações recebidas.

Art. 14. Compete às unidades integrantes da estrutura organizacional da Anater;

I - assegurar o cumprimento da PPSI no âmbito de suas unidades;

II - definir, validar e revisar periodicamente os perfis de acesso às informações e sistemas sob sua responsabilidade;

III - comunicar tempestivamente à Unidade de Tecnologia da Informação e ao Encarregado

de Dados a ocorrência ou suspeita de incidentes de segurança da informação ou vulnerabilidades identificadas;

IV - garantir que empregados, colaboradores e prestadores de serviços sob sua supervisão tenham ciência e recebam orientação quanto às diretrizes desta Política;

V - assegurar a incorporação de controles de segurança da informação nos processos, projetos e atividades de sua unidade;

VI - assegurar a adequada classificação, tratamento, uso e proteção das informações sob sua responsabilidade, em conformidade com as normas vigentes;

VII - solicitar a concessão, alteração e revogação de acessos de usuários, com base nos perfis previamente definidos e nas necessidades do serviço; e

VIII - atender, no âmbito de sua competência, às demandas decorrentes de auditorias, apurações e ações de resposta a incidentes de segurança da informação.

Art. 15. Compete aos usuários:

I - cumprir as diretrizes, normas e procedimentos estabelecidos nesta Política;

II - zelar pela confidencialidade, integridade e disponibilidade das informações e ativos de informação sob sua responsabilidade;

III - utilizar os recursos de tecnologia da informação de forma ética, responsável e exclusivamente para fins institucionais;

IV - manter sob sigilo suas credenciais de acesso, sendo vedado o compartilhamento com terceiros;

V - adotar boas práticas de segurança da informação, especialmente quanto ao uso de senhas, dispositivos e acesso a sistemas;

VI - comunicar imediatamente ao gestor de sua unidade a ocorrência ou suspeita de incidentes de segurança da informação ou situações que representem risco; e

VII - colaborar com ações de conscientização, capacitação e melhoria contínua da segurança da informação.

CAPÍTULO VI

DA CLASSIFICAÇÃO DA INFORMAÇÃO, PROPRIEDADE E CONTROLE DE ACESSO

Art. 16. A PPSI aplica-se a todas as informações produzidas, recebidas, armazenadas, processadas ou transmitidas no âmbito da Anater, independentemente do meio, suporte ou formato, incluindo meios digitais, físicos ou verbais.

§ 1º A gestão da informação observará, de forma equilibrada, os princípios da transparência, da segurança da informação e da proteção de dados pessoais, em conformidade com a legislação aplicável.

§ 2º As informações institucionais são de propriedade da Anater, sendo vedada sua utilização, reprodução ou divulgação sem autorização, nos termos desta Política e demais normativos aplicáveis.

§ 3º O acesso à informação não implica transferência de propriedade, nem confere ao usuário autorização para seu compartilhamento com terceiros.

§ 4º As credenciais de acesso e as informações constantes de sistemas e bases de dados, especialmente aquelas que contenham dados pessoais, possuem caráter confidencial, devendo seu acesso e utilização observar o dever de sigilo, condicionado à prévia assinatura de Termo de Responsabilidade e Confidencialidade, Anexos II, III e VI, sendo sua disponibilização restrita às hipóteses devidamente autorizadas por autoridade competente, nos termos da legislação e das normas internas aplicáveis.

Seção I

Da Classificação da Informação

Art. 17. As informações sob gestão da Anater deverão ser classificadas quanto ao grau de confidencialidade, observados os riscos institucionais, legais e operacionais associados ao seu tratamento.

§ 1º A classificação da informação observará, no mínimo, os seguintes níveis:

I - pública: informação de livre acesso, cuja divulgação não acarreta riscos à Instituição ou a terceiros;

II - restrita: informação cujo acesso deve ser limitado a pessoas autorizadas, em razão de interesse administrativo ou institucional; e

III - confidencial: informação cujo acesso não autorizado pode causar prejuízos à Anater, a seus parceiros ou a titulares de dados, incluindo dados pessoais protegidos por lei.

§ 2º A classificação deverá considerar, entre outros critérios, a sensibilidade da informação, o impacto em caso de acesso não autorizado, as obrigações legais e regulatórias e a necessidade de compartilhamento para execução das atividades institucionais.

§ 3º A classificação da informação deverá ser revisada periodicamente ou sempre que houver alteração relevante em seu contexto de uso ou sensibilidade.

Seção II

Do Controle de Acesso, Proteção e Uso da Informação

Art. 18. O acesso às informações e aos ativos de informação deverá observar:

I - o princípio do menor privilégio;

II - a necessidade de conhecimento para o desempenho das funções; e

III - a rastreabilidade dos acessos e das ações realizadas.

§ 1º O acesso deverá ser previamente autorizado, formalizado e periodicamente revisado.

§ 2º A Anater adotará medidas técnicas e administrativas destinadas à proteção das informações contra acessos não autorizados, perda, destruição, alteração ou qualquer forma de tratamento inadequado ou ilícito.

Art. 19. Os incidentes de segurança da informação deverão ser gerenciados de forma sistemática e contínua, contemplando, no mínimo, sua identificação, registro, classificação, análise, tratamento e acompanhamento, com vistas à mitigação de riscos, à redução de impactos e à melhoria contínua dos controles de segurança da informação.

§ 1º O tratamento dos incidentes deverá observar abordagem baseada em risco, considerando a natureza, a criticidade e os impactos potenciais para a Anater, para seus ativos de informação e, quando aplicável, para os titulares de dados pessoais.

§ 2º Os incidentes que envolvam ou possam envolver dados pessoais deverão observar, adicionalmente, as diretrizes de proteção de dados pessoais, incluindo a avaliação, em prazo adequado, quanto à necessidade de comunicação à Autoridade Nacional de Proteção de Dados – ANPD e aos titulares, conforme Anexos IV e V.

§ 3º A Anater deverá estabelecer e manter procedimentos, atribuições e responsabilidades claramente definidos para o gerenciamento de incidentes de segurança da informação, incluindo, quando aplicável:

I - classificação e priorização dos incidentes;

II - registro de eventos, evidências e decisões adotadas;

III - definição e execução de medidas de contenção, tratamento e recuperação;

IV - avaliação de causas, riscos e impactos; e

V - implementação de ações corretivas e de melhoria.

§ 4º A Anater deverá dispor de procedimentos e instrumentos padronizados para o registro e a comunicação de incidentes de segurança da informação que envolvam dados pessoais, observado o disposto no Anexo IV desta Política.

Seção III

Do Tratamento de Dados Pessoais

Art. 20. O tratamento de dados pessoais no âmbito da Anater deverá estar fundamentado em base legal válida e identificada, observando os princípios da legalidade, finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização, com vistas à execução das competências institucionais.

Parágrafo único. As unidades organizacionais deverão manter registro das operações de tratamento sob sua responsabilidade, assegurando sua conformidade com a legislação e sua integração aos processos de gestão de riscos e de integridade.

Art. 21. As unidades organizacionais da Anater deverão assegurar o exercício dos direitos dos titulares de dados pessoais, nos termos da LGPD, por meio de canais formais, acessíveis e amplamente divulgados.

§ 1º A Agência manterá canal eletrônico específico para atendimento aos titulares, contendo orientações claras sobre:

I - apresentação de solicitações e manifestações;

II - exercício dos direitos previstos na LGPD; e

III - interação com temas relacionados à LGPD e à Lei de Acesso à Informação (LAI).

§ 2º As demandas serão tratadas conforme fluxos definidos em normativo interno, com atribuição de responsabilidades, prazos e instâncias de tratamento, sob coordenação da Ouvidoria, na qualidade de unidade responsável pela gestão do atendimento ao titular, com a participação do Encarregado de Dados, na função de orientação, supervisão e apoio técnico, bem como com o apoio das demais unidades competentes, incluindo as áreas jurídica e de tecnologia da informação, quando aplicável.

§ 3º As respostas aos titulares deverão ser fundamentadas e registradas.

Art. 22. O tratamento de dados pessoais sensíveis deverá observar rigorosamente as hipóteses legais e os requisitos previstos na LGPD, sendo vedada sua utilização para finalidades discriminatórias, ilícitas ou abusivas.

Parágrafo único. O tratamento de dados pessoais sensíveis deverá ser precedido de avaliação de riscos e da adoção de medidas técnicas e administrativas compatíveis com a natureza dos dados e os riscos envolvidos, inclusive nas operações de compartilhamento.

Art. 23. O tratamento de dados pessoais de crianças e adolescentes deverá observar as hipóteses legais aplicáveis, assegurando, em qualquer caso, o melhor interesse do titular, nos termos da LGPD.

Parágrafo único. Sempre que aplicável, deverá ser assegurada a obtenção e a verificação do consentimento específico e em destaque de pelo menos um dos responsáveis legais, bem como a adoção de medidas adequadas à proteção do titular.

Art. 24. O uso compartilhado de dados pessoais com entes públicos ou privados deverá observar a legislação aplicável e ser formalizado por instrumento específico que estabeleça, no mínimo:

I - a finalidade do compartilhamento;

II - a base legal aplicável;

III - as responsabilidades das partes;

IV - as medidas de segurança e proteção de dados; e

V - as regras de acesso, uso e guarda das informações.

§ 1º O compartilhamento dependerá de avaliação prévia quanto à sua necessidade, adequação e riscos envolvidos.

§ 2º As operações de compartilhamento deverão ser registradas e alinhadas aos processos de gestão de riscos e de integridade.

Art. 25. A transferência internacional de dados pessoais deverá observar os requisitos da LGPD e ser precedida de avaliação quanto ao nível de proteção de dados do país ou organismo de destino.

Parágrafo único. A transferência somente poderá ocorrer mediante fundamento legal aplicável e adoção de salvaguardas adequadas, quando necessário, devendo estar alinhada aos processos de gestão de riscos e de integridade da Anater.

CAPÍTULO VII

DA GESTÃO DE ATIVOS

Seção I

Utilização da estação de trabalho

Art. 26. A utilização da estação de trabalho pelos usuários, observará, no mínimo, os seguintes requisitos:

I - identificação única na rede corporativa, permitindo a rastreabilidade das ações nela realizadas;

II - responsabilidade integral do usuário pela estação de trabalho a ele disponibilizada, inclusive pelas ações executadas mediante suas credenciais de acesso;

III - acesso aos sistemas institucionais exclusivamente por meio de *login* individual e intransferível, sendo vedado o compartilhamento de credenciais;

IV - armazenamento de arquivos institucionais em ambientes de rede corporativa ou sistemas oficiais, observadas as diretrizes de segurança da informação;

V - zelo pela integridade, confidencialidade e disponibilidade das informações acessadas ou armazenadas na estação de trabalho;

VI - realização de manutenção periódica no diretório pessoal, evitando acúmulo de arquivos desnecessários;

VII - não instalar programas, afixar adesivos nem realizar quaisquer alterações nas estações de trabalho sem prévia autorização da área competente; e

VIII - não armazenar, nas estações de trabalho, arquivos de áudio, vídeo, imagens ou softwares protegidos por direitos autorais, bem como de conteúdo que configurem violação à legislação de propriedade intelectual ou pirataria digital.

§ 1º O usuário deverá, ao se ausentar da estação de trabalho, encerrar ou bloquear a sessão de acesso, de modo a prevenir o acesso indevido a sistemas, dados, documentos e demais informações institucionais, bem como desligar a estação de trabalho ao final do expediente.

§ 2º A senha de acesso à estação de trabalho é pessoal, confidencial e intransferível, sendo proibida sua divulgação sob qualquer hipótese, devendo ser alterada pelo usuário no primeiro acesso.

Seção II

Utilização da rede

Art. 27. A utilização da rede corporativa observará, no mínimo, os seguintes requisitos:

I - as credenciais de acesso à rede corporativa deverão ser mantidas em caráter confidencial, pessoal e intransferível, sendo o usuário integralmente responsável por seu uso;

II - é vedado acessar, armazenar, distribuir ou compartilhar conteúdo de natureza pornográfica, discriminatória ou incompatível com as atividades institucionais;

III - é vedado instalar, armazenar ou executar jogos de entretenimento nos equipamentos ou diretórios da rede corporativa;

IV - não serão permitidas alterações nas configurações de rede ou dos equipamentos que possam comprometer a segurança ou o funcionamento dos sistemas; e

V - são vedadas tentativas de acesso não autorizado a sistemas, redes, arquivos ou quaisquer recursos de tecnologia da informação.

Seção III

Utilização do correio eletrônico

Art. 28. O correio eletrônico institucional constitui ferramenta oficial de comunicação da Anater e deverá ser utilizado em conformidade com os princípios de segurança da informação, finalidade pública e responsabilidade.

§ 1º Admite-se o uso pessoal eventual, desde que não prejudique o desempenho das atividades, não comprometa a segurança da informação nem cause sobrecarga indevida à rede ou prejuízo à Instituição ou a terceiros.

§ 2º Não se admite a utilização do correio eletrônico para:

I - acessar ou tentar acessar caixas postais de terceiros sem autorização;

II - enviar mensagens em massa não autorizadas (spam), ressalvadas as comunicações institucionais, devendo, quando aplicável, ser utilizado o campo de cópia oculta (CCO) para resguardar a privacidade dos destinatários;

III - utilizar endereços de e-mail não autorizados para envio de comunicações institucionais;

IV - divulgar ou compartilhar informações institucionais sem a devida autorização;

V - transmitir conteúdos que possam comprometer a imagem institucional ou gerar responsabilização à Anater;

VI - disseminar arquivos, códigos ou programas que representem risco à segurança da informação, inclusive aqueles capazes de executar ações maliciosas nos sistemas;

VII - praticar ações que possibilitem acesso não autorizado a sistemas, redes, dados ou informações;

VIII - burlar mecanismos de segurança da informação, internos ou externos;

IX - realizar práticas de monitoramento indevido, espionagem ou assédio a usuários internos ou externos;

X - veicular conteúdos ilícitos, ofensivos, discriminatórios, difamatórios, degradantes, obscenos, violentos ou incompatíveis com os princípios institucionais;

XI - divulgar conteúdo de natureza político-partidária ou que contrarie os interesses institucionais; e

XII - encaminhar materiais protegidos por direitos autorais sem a devida autorização.

§ 3º Os registros de acesso e uso do correio eletrônico poderão ser monitorados e auditados para fins de segurança da informação e conformidade.

§ 4º As mensagens institucionais deverão conter assinatura padronizada, conforme orientação da área competente.

Seção IV

Utilização de redes sociais

Art. 29. O uso de redes sociais pelos usuários da Anater deverá observar os princípios da segurança da informação, da proteção de dados pessoais, da ética e da responsabilidade, especialmente quando houver vinculação, direta ou indireta, à Agência.

§ 1º O uso de redes sociais em caráter pessoal é livre, devendo, contudo, o usuário atuar com diligência para evitar:

I - associação indevida de opiniões pessoais à posição institucional da Anater;

II - divulgação de informações institucionais não públicas ou classificadas;

III - exposição de dados pessoais em desconformidade com a legislação aplicável; e

IV - situações que possam comprometer a segurança da informação ou gerar riscos institucionais.

§ 2º A manifestação em nome da Anater e a divulgação de conteúdos institucionais em redes sociais somente poderão ocorrer por meio de canais oficiais ou mediante autorização da área competente.

§ 3º É vedado:

I - divulgar ou compartilhar informações internas, sigilosas ou de acesso restrito;

II - utilizar indevidamente nome, logotipo, identidade visual ou qualquer elemento que induza representação institucional sem autorização;

III - apresentar-se como representante da Anater sem delegação formal;

IV - divulgar conteúdos que possam comprometer a segurança da informação ou ensejar responsabilização institucional; e

V - associar, de forma explícita ou implícita, a imagem, o nome ou a atuação institucional da Anater a posicionamentos de natureza político-partidária.

§ 4º O disposto no inciso V do § 3º não impede a divulgação, pelos canais oficiais da Anater, de informações institucionais relativas a políticas públicas, programas, ações governamentais ou atos normativos, desde que observados os princípios da legalidade, impessoalidade e finalidade institucional, vedada a promoção de agentes políticos, partidos ou candidaturas.

§ 5º As disposições deste artigo não impedem a manifestação pessoal de natureza política por parte dos usuários, desde que não haja vinculação indevida à Anater nem utilização de informações ou recursos institucionais.

§ 6º A menção ao vínculo profissional com a Anater em perfis pessoais não implica representação institucional, devendo o usuário, quando necessário, deixar claro o caráter estritamente pessoal de suas manifestações.

§ 7º As disposições deste artigo não têm por finalidade restringir a liberdade de expressão dos usuários, mas orientar condutas para a proteção da informação, dos dados pessoais e da imagem institucional, nos termos da legislação aplicável.

§ 8º Eventuais medidas de monitoramento limitar-se-ão a situações relacionadas à segurança da informação e à proteção institucional, observados os princípios da necessidade,

proporcionalidade e respeito à privacidade.

Seção V

Utilização de dispositivos móveis

Art. 30. A utilização de dispositivos móveis no âmbito da Anater deverá observar os requisitos de segurança da informação e as diretrizes estabelecidas nesta Seção, considerando a natureza e a titularidade dos equipamentos.

§ 1º Os dispositivos móveis institucionais serão configurados, gerenciados e mantidos pela Unidade de Tecnologia da Informação, de modo a assegurar sua integração e conformidade com a rede corporativa.

§ 2º Incumbe ao usuário de dispositivo móvel institucional:

I - observar os mesmos padrões de segurança aplicáveis aos equipamentos fixos;

II - adotar mecanismos de proteção dos dados e do equipamento, tais como senhas, bloqueios e outros recursos disponíveis;

III - preservar a confidencialidade das informações, especialmente quando da utilização de redes externas;

IV - manter, sempre que possível, cópias de segurança dos dados armazenados; e

V - comunicar imediatamente à Unidade de Tecnologia da Informação quaisquer incidentes, incluindo perda, furto, roubo, falhas ou comportamentos anômalos do equipamento.

§ 3º Na utilização de dispositivos móveis em redes externas, o usuário deverá adotar cautelas adicionais para evitar exposição indevida de informações institucionais, incluindo a preservação das configurações originais e a comunicação de eventuais irregularidades à área competente.

§ 4º Compete à área de Tecnologia da Informação:

I - realizar a manutenção dos dispositivos móveis institucionais;

II - promover a recuperação de configurações e a correção de falhas, quando necessário; e

III - realizar, a qualquer tempo, inspeções para verificação da conformidade e da segurança dos equipamentos.

§ 5º A utilização de dispositivos móveis particulares por usuários ou visitantes nas dependências da Anater condiciona-se à observância dos requisitos de segurança da informação.

§ 6º A conexão de dispositivos particulares à rede corporativa dependerá de análise e autorização prévia da área de Tecnologia da Informação, observado, no mínimo:

I - a inexistência de programas maliciosos;

II - a adoção de mecanismos atualizados de proteção, como antivírus; e

III - a vedação de práticas que comprometam a segurança da rede ou de outros dispositivos conectados.

Seção VI

Acesso à internet

Art. 31. O acesso à internet no âmbito da Anater destina-se prioritariamente à execução das atividades institucionais, devendo observar os princípios de segurança da informação, uso adequado dos recursos e responsabilidade do usuário.

§ 1º O uso da internet para fins pessoais admite-se de forma excepcional, desde que

realizado fora do horário de expediente ou em intervalos e que não comprometa a segurança da informação, o desempenho da rede ou as atividades institucionais.

§ 2º Não se admite a utilização da internet para:

I - divulgação ou compartilhamento de informações confidenciais em ambientes externos, como fóruns, listas de discussão ou serviços de comunicação;

II - acesso a conteúdos incompatíveis com o ambiente institucional, tais como material pornográfico, jogos, apostas, bate-papo ou similares;

III - utilização de softwares ou serviços que comprometam a segurança da rede, inclusive ferramentas de compartilhamento de arquivos; e

IV - práticas que possam comprometer a integridade, a disponibilidade ou o desempenho da rede corporativa.

§ 3º Compete à Unidade de Tecnologia da Informação:

I - implementar mecanismos de controle e restrição de acesso a conteúdos, serviços ou domínios que comprometam a segurança ou o uso adequado da rede;

II - definir e homologar os navegadores e demais ferramentas autorizadas para acesso à internet; e

III - monitorar o uso da rede, observadas as normas de segurança da informação e de proteção de dados.

§ 4º A utilização de serviços que demandem elevado consumo de banda, tais como streaming, dependerá de autorização prévia da área competente, mediante justificativa de necessidade institucional.

Seção VII

Acesso aos sistemas informatizados

Art. 32. O acesso e a utilização dos sistemas informatizados da Anater condicionam-se à necessidade de serviço, à autorização prévia e à observância das normas internas e da legislação aplicável.

§ 1º O acesso aos sistemas deverá ocorrer no estrito exercício das atribuições do usuário ou por determinação expressa de superior hierárquico, vedada sua utilização para fins alheios ao interesse institucional.

§ 2º As credenciais de acesso são pessoais, confidenciais e intransferíveis, cabendo ao usuário zelar por seu sigilo e uso adequado.

§ 3º O usuário responde pelas ações realizadas com suas credenciais, inclusive quanto ao acesso, à manipulação e ao tratamento de dados, informações e sistemas.

§ 4º No caso de serviços executados por terceiros, a responsabilidade pelo uso adequado dos acessos concedidos caberá ao gestor da área contratante.

§ 5º Incumbe ao usuário:

I - atuar em conformidade com suas atribuições e com os procedimentos estabelecidos;

II - zelar pela integridade, confidencialidade e disponibilidade dos dados, informações e sistemas; e

III - comunicar imediatamente ao gestor imediato ou à área competente quaisquer indícios de irregularidades, falhas ou vulnerabilidades identificadas.

§ 6º É vedada a exploração de falhas ou vulnerabilidades dos sistemas, ainda que para fins de teste ou demonstração, sem autorização formal da área competente.

Seção VIII

Acesso ao Datacenter

Art. 33. O acesso ao Datacenter da Anater é restrito e condicionado à autorização da Unidade de Tecnologia da Informação, devendo observar os requisitos de segurança física e lógica aplicáveis.

§ 1º O acesso será realizado mediante identificação e registro em sistema de controle, sendo todas as entradas e saídas registradas e passíveis de auditoria.

§ 2º A entrada de terceiros, inclusive prestadores de serviço e visitantes:

I - dependerá de autorização prévia da Unidade de Tecnologia da Informação;

II - deverá ocorrer sob acompanhamento de pessoa autorizada; e

III - será registrada com a identificação do visitante, a finalidade, a data e o horário do acesso.

§ 3º As atividades realizadas no Datacenter deverão preservar as condições adequadas de funcionamento dos equipamentos, devendo ser previamente comunicadas à área competente quando puderem gerar resíduos ou interferências no ambiente.

§ 4º Não se admite a entrada de alimentos, líquidos ou substâncias que possam comprometer a segurança e a integridade do ambiente.

§ 5º A instalação, retirada ou realocação de equipamentos deverá ser previamente autorizada e devidamente registrada, com a indicação da data, horário, identificação do equipamento e justificativa da intervenção.

Art. 34. Os procedimentos de backup dos sistemas e dados institucionais serão gerenciados pela Unidade de Tecnologia da Informação, com vistas à continuidade dos serviços e à proteção das informações.

§ 1º As rotinas de backup deverão ser programadas, preferencialmente, para horários de menor impacto operacional.

§ 2º As mídias de backup deverão ser submetidas a controles periódicos de integridade e armazenadas em local seguro, distinto do Datacenter, de modo a assegurar a recuperação dos dados.

§ 3º Poderá ser adotada solução de armazenamento externo para guarda de cópias históricas, observadas as normas técnicas aplicáveis.

§ 4º Os procedimentos de backup deverão ser testados periodicamente, mediante simulação de restauração em ambiente apropriado, com registro dos resultados.

§ 5º As mídias defeituosas ou irrecuperáveis deverão ser descartadas mediante registro formal, assegurada a rastreabilidade das ações realizadas.

CAPÍTULO VIII

DA RESPONSABILIZAÇÃO E PENALIDADES

Art. 35. O descumprimento das disposições desta Política e das normas dela decorrentes caracteriza infração funcional e sujeita o agente às medidas administrativas cabíveis, sem prejuízo das responsabilidades civil e penal previstas na legislação vigente.

Art. 36. A responsabilização observará as seguintes regras:

I - o usuário responde pelas ações realizadas com suas credenciais de acesso, ainda que decorrentes de uso indevido por terceiros, quando não resguardado o dever de sigilo;

II - o uso inadequado, negligente ou imprudente dos recursos de tecnologia da informação será passível de apuração;

III - os gestores de unidades respondem pela supervisão e pelo cumprimento das disposições desta Política em suas áreas; e

IV - terceiros, prestadores de serviço e colaboradores externos sujeitam-se às mesmas regras, por intermédio do gestor do contrato ou instrumento congênere.

Art. 37. Constituem infrações, sem prejuízo de outras previstas em norma específica:

I - o compartilhamento ou a divulgação indevida de credenciais de acesso;

II - o acesso não autorizado a sistemas, redes, dados, documentos ou informações institucionais;

III - a tentativa de burlar controles de segurança da informação;

IV - a divulgação ou o uso indevido de informações institucionais;

V - a utilização dos recursos de tecnologia da informação para fins ilícitos ou incompatíveis com as atividades institucionais; e

VI - a omissão na comunicação de incidentes de segurança da informação.

Art. 38. As infrações serão apuradas por meio de procedimentos internos de verificação, assegurado o devido processo, podendo incluir:

I - análise de registros de acesso e rastreabilidade das ações (logs);

II - auditorias periódicas ou extraordinárias; e

III - apuração administrativa, nos termos da legislação aplicável.

Art. 39. As medidas administrativas aplicáveis poderão incluir, conforme a gravidade da infração:

I - advertência;

II - suspensão ou restrição de acesso aos sistemas e recursos de tecnologia da informação;

III - comunicação à chefia imediata e às instâncias competentes; e

IV - instauração de procedimento disciplinar.

Art. 40. O acesso aos recursos de tecnologia da informação da Anater fica condicionado à ciência e à concordância com esta Política, formalizadas por meio de termo de compromisso, sigilo e confidencialidade, conforme Anexos II e III.

§ 1º A obrigação de observância desta Política deverá ser comunicada aos empregados no ato de sua contratação e reforçada por meio de ações periódicas de orientação e capacitação.

§ 2º Nos contratos firmados com pessoas jurídicas ou prestadores de serviço que tenham acesso a ativos de tecnologia da informação, deverá constar cláusula específica de sigilo e confidencialidade como condição para concessão de acesso.

Art. 41. A utilização dos recursos de tecnologia da informação deverá observar padrões de legalidade, ética e finalidade institucional, sendo admitido o uso pessoal de forma excepcional, desde que não prejudique o desempenho dos sistemas, serviços ou atividades da Anater.

Art. 42. O usuário deverá adotar cautelas necessárias à proteção das informações institucionais, especialmente quanto à sua visualização, armazenamento ou compartilhamento, de modo a evitar acesso indevido por pessoas não autorizadas.

§ 1º É vedada a divulgação de informações institucionais fora do âmbito profissional, salvo quando autorizada ou em decorrência de obrigação legal ou decisão de autoridade competente.

§ 2º Todo incidente que possa comprometer a segurança da informação deverá ser comunicado imediatamente à Unidade de Tecnologia da Informação, ainda que haja dúvida quanto à sua relevância ou impacto.

Art. 43. Os sistemas, projetos e soluções de tecnologia da informação deverão incorporar requisitos de segurança desde sua concepção, abrangendo, no mínimo, as fases de planejamento, desenvolvimento, testes e homologação.

Art. 44. Os pontos de acesso às informações institucionais deverão dispor de mecanismos de controle e registro de atividades, com vistas à prevenção, detecção e apuração de acessos indevidos ou perdas de informação.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 45. A implementação das disposições desta Política observará o princípio da gradualidade, considerando a análise de riscos, o nível de maturidade institucional e a disponibilidade de recursos institucionais.

§ 1º A Unidade de Tecnologia da Informação, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, elaborará, no prazo de até 120 dias, Plano de Adequação contendo diagnóstico, ações, prazos e prioridades para o atendimento desta Política.

§ 2º Durante a execução das medidas previstas no Plano de Adequação, a avaliação da conformidade observará o cumprimento das ações e metas estabelecidas, consideradas a adoção de medidas proporcionais aos riscos identificados, o nível de maturidade institucional e a capacidade operacional da Anater.

§ 3º A avaliação de eventuais responsabilidades considerará, entre outros aspectos, a existência de meios e condições para o cumprimento das obrigações, o estágio de implementação das medidas previstas no Plano de Adequação e a atuação diligente das unidades responsáveis.

§ 4º O prazo para implementação integral desta Política será de até 24 (vinte e quatro) meses, contados da aprovação do Plano de Adequação pela Direx, sem prejuízo da adoção imediata das medidas necessárias à mitigação de riscos relevantes.

Art. 46. Esta Política deverá ser revisada e atualizada periodicamente, ou sempre que eventos relevantes assim o exigirem, de modo a assegurar sua aderência às necessidades institucionais e às melhores práticas de segurança da informação.

Parágrafo único. A Política de que trata o *caput* deverá ser divulgada no sítio eletrônico da Anater e nos canais internos de comunicação, de forma a assegurar o conhecimento pelos públicos interno e externo, observado o disposto nesta Política e Anexos.

ANEXO II

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE (PESSOA FÍSICA) - MODELO

Eu,_____, CPF ____.____.____-____, declaro haver lido e concordado com a Política de Privacidade e Segurança da Informação da Agência Nacional de Assistência Técnica e Extensão Rural (Anater), composta por diretrizes gerais, normas, procedimentos e regras, comprometendo-me a observá-las e segui-las.

Declaro, também, estar ciente de que os acessos por mim realizados a sistemas, redes, dados, documentos ou informações institucionais, bem como o conteúdo das mensagens enviadas via correio eletrônico corporativo, são monitorados automaticamente.

Brasília, _____ de _____ de _____.

_____

Assinatura

ANEXO III

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE (PESSOA JURÍDICA) - MODELO

A Agência Nacional de Assistência Técnica e Extensão Rural (Anater), situada no SAUN, Quadra 05, Lote C, Torre "D", 4º andar, Asa Norte - Brasília/DF
CEP 70.040-250, inscrita no CNPJ sob o n° 24.203.514/0001-02, e, de outro lado, _____, situada à _____, inscrita no CNPJ sob o n° _____ , doravante denominadas PARTES, sendo esta última denominada PARTÍCIPE;

Considerando:

I - que, em razão do instrumento jurídico nº ____(mencionar se contrato, convênio, acordo, ajuste ou instrumento congênere), doravante denominado INSTRUMENTO PRINCIPAL, o PARTÍCIPE poderá ter acesso a informações classificadas como confidenciais ou sigilosas da Anater;

II - a necessidade de estabelecer regras para o uso, tratamento e proteção dessas informações, em conformidade com a Política de Privacidade e Segurança da Informação da Anater;

Resolvem celebrar o presente TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, mediante as seguintes cláusulas:

CLÁUSULA PRIMEIRA – DO OBJETO

O presente Termo tem por objeto disciplinar o acesso, o uso, o tratamento e a proteção das informações a que o PARTÍCIPE tiver acesso em decorrência da execução do INSTRUMENTO PRINCIPAL.

CLÁUSULA SEGUNDA – DO ESCOPO DAS INFORMAÇÕES E DOS ATIVOS DE INFORMAÇÃO

O acesso pelo PARTÍCIPE será restrito às atividades necessárias à execução do INSTRUMENTO PRINCIPAL, abrangendo dados, informações e ativos de informação da Anater, independentemente do meio ou formato, incluindo, mas não se limitando a:

I - dados pessoais e dados pessoais sensíveis;

II - informações institucionais, técnicas, administrativas ou estratégicas;

III - sistemas de informação, aplicações, bancos de dados e ambientes tecnológicos;

IV - informações armazenadas ou transmitidas por meios eletrônicos;

V - informações armazenadas em qualquer tipo de mídia;

VI - comunicações formais ou informais, inclusive eletrônicas; e

VII - documentos físicos ou digitais.

Parágrafo único. Consideram-se ativos de informação todos os recursos que suportam o tratamento da informação, incluindo equipamentos, sistemas, serviços, bases de dados e infraestruturas tecnológicas.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DO PARTÍCIPE

O PARTÍCIPE obriga-se a:

I - observar integralmente a Política de Privacidade e Segurança da Informação da Anater e as normas complementares aplicáveis;

II - utilizar as informações exclusivamente para a execução do INSTRUMENTO PRINCIPAL, vedado qualquer uso para finalidade diversa;

III - identificar formalmente os profissionais autorizados a acessar informações da Anater, responsabilizando-se por seus atos;

IV - dar ciência e obter compromisso formal de seus empregados, prepostos e eventuais terceiros quanto ao cumprimento deste Termo e das normas aplicáveis;

V - manter o sigilo sobre quaisquer informações a que tiver acesso, não as divulgando sem autorização da Anater, ressalvadas as hipóteses legalmente previstas;

VI - abster-se de instalar, executar ou utilizar programas, sistemas, dispositivos ou rotinas não autorizados pela Anater;

VII - adotar medidas técnicas e administrativas adequadas à proteção das informações, compatíveis com os riscos envolvidos;

VIII - comunicar imediatamente à Anater a ocorrência ou suspeita de incidentes de segurança da informação;

IX - responder pelos danos e incidentes decorrentes do descumprimento das obrigações previstas neste Termo, na Política e nas normas aplicáveis, inclusive aqueles causados por seus empregados, prepostos ou terceiros sob sua responsabilidade.

CLÁUSULA QUARTA – DA RESPONSABILIZAÇÃO

O PARTÍCIPE responderá, nos termos da legislação aplicável, pelos danos decorrentes do uso indevido ou tratamento inadequado das informações, sem prejuízo das sanções previstas no INSTRUMENTO PRINCIPAL.

CLÁUSULA QUINTA – DA VIGÊNCIA

O presente Termo vigorará durante a execução do INSTRUMENTO PRINCIPAL e permanecerá válido enquanto perdurar o dever de sigilo das informações acessadas.

CLÁUSULA SEXTA – DA VINCULAÇÃO

Este Termo vincula-se ao INSTRUMENTO PRINCIPAL, independentemente de sua natureza jurídica.

E por estarem assim justas e acordadas, as partes assinam o presente termo em duas vias de igual teor e forma.

Brasília, _____ de _____ de _____.

_____

Nome Completo

Cargo

_____

Nome Completo

Cargo

PARTÍCIPE

_____

Nome Completo

TESTEMUNHA

_____

Nome Completo

TESTEMUNHA

ANEXO IV

FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) - MODELO

Comunicação

Tipo de comunicação:

☐ Completa

☐ Parcial

Para comunicação parcial:

☐ Preliminar

☐ Complementar

Critério para a comunicação:

☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐ Não tenho certeza sobre o nível de risco do incidente de segurança.

Agente de tratamento

O notificante é:

☐ Controlador

☐ Operador

Se operador, informar se já houve comunicação ao controlador:

[Resposta]

Dados do agente de tratamento:

Número do CPF ou CNPJ:

Nome ou Razão Social:

Natureza da Organização (Pública ou Privada):

Endereço:

Cidade:

Estado:

CEP:

Telefone:

E-mail:

Dados do notificante:

Nome:

E-mail:

Telefone:

Dados do encarregado:

☐ Mesmos dados do notificante.

Outro notificante, preencher os dados abaixo:

Nome:

E-mail:

Telefone:

Incidente de segurança

Descreva de forma resumida como o incidente de segurança de dados pessoais ocorreu.

[Resposta]

Quando o incidente ocorreu?

[Data e hora]

☐ Não tenho conhecimento. Justifique: [Resposta]

☐ Não tenho certeza. Justifique: [Resposta]

Quando a organização teve ciência do incidente de segurança?

[Data e hora]

Descreva como a organização teve ciência do incidente de segurança.

[Resposta]

Se a comunicação inicial do incidente não foi comunicada no prazo sugerido de 3 dias úteis após ter tomado ciência do incidente, justifique os motivos.

[Resposta]

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

[Resposta]

Qual a natureza dos dados afetados?

☐ Origem racial ou étnica.

☐ Convicção religiosa.

☐ Opinião política.

☐ Filiação a sindicato.

☐ Filiação a organização de caráter religioso, filosófico ou político.

☐ Dado referente à saúde.

☐ Dado referente à vida sexual.

☐ Dado genético ou biométrico.

☐ Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).

☐ Dado financeiro.

☐ Nomes de usuário ou senhas de sistemas de informação.

☐ Dado de geolocalização.

Outros: [Resposta]

Qual a quantidade de titulares afetados?

[Resposta]

Qual a categoria dos titulares afetados?

☐ Funcionários

☐ Prestadores de serviço

☐ Clientes

☐ Consumidores

☐ Usuários

☐ Pacientes de serviço de saúde

☐ Crianças ou adolescentes

Outros: [Resposta]

Medidas de segurança utilizadas para a proteção dos dados

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a recorrência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

[Resposta]

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

[Resposta]

Riscos relacionados ao incidente de segurança

Quais as prováveis consequências do incidente de segurança para os titulares afetados?

[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

[Resposta]

Comunicação aos titulares

Os titulares foram comunicados sobre o incidente de segurança de dados pessoais?

☐ Sim

☐ Não

Se sim, informar:

data da comunicação:

canal utilizado:

público:

conteúdo da mensagem enviada:

medidas orientadas aos titulares:

Se não, justificar de forma fundamentada a razão da não comunicação.

ANEXO V

COMUNICAÇÃO AO TITULAR DE DADOS PESSOAIS EM CASO DE INCIDENTE DE SEGURANÇA - MODELO

Assunto: Comunicação de incidente de segurança envolvendo dados pessoais

Prezado(a) Senhor(a),

1. A Agência Nacional de Assistência Técnica e Extensão Rural (Anater) informa a ocorrência de incidente de segurança da informação que pode ter afetado dados pessoais sob sua titularidade, no contexto das atividades institucionais desta Agência.

2. Em atenção ao dever de transparência previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), apresentamos, a seguir, as informações disponíveis até o momento:

2.1. **O que ocorreu**

[Descrição objetiva e clara do incidente]

2.2. **Quais dados podem ter sido afetados**

[Indicar categorias de dados, evitando detalhamento excessivo que gere risco adicional]

2.3. **Quando a Anater tomou ciência do incidente**

[Data ou período]

2.4. **Medidas já adotadas pela Anater**

[Providências de contenção, mitigação e apuração]

2.5**. Possíveis riscos ao titular**

[Descrição clara e proporcional dos riscos identificados]

2.6. **Medidas recomendadas ao titular (quando aplicável)**

[Orientações práticas, como alteração de senha, atenção a comunicações suspeitas, etc.]

2.7. **Canal de atendimento para esclarecimentos adicionais, o(a) titular poderá contatar a Anater por meio do canal:**

[informar canal institucional]

3. **O contato com o Encarregado pelo Tratamento de Dados Pessoais também poderá ser realizado pelo endereço:**

[informar e-mail ou outro canal oficial]

4. Registra-se que a Anater permanece adotando as medidas necessárias para a adequada apuração, tratamento do incidente e mitigação de seus eventuais efeitos.

Atenciosamente,

ANEXO VI

TERMO DE CONSENTIMENTO PARA USO DE IMAGEM, VOZ E TRATAMENTO DE DADOS PESSOAIS - MODELO

Eu, _____, CPF nº _____, participante/beneficiário(a) das ações, programas, projetos ou atividades executadas pela Agência

Nacional de Assistência Técnica e Extensão Rural – Anater, DECLARO que fui devidamente informado(a) e AUTORIZO, de forma livre, informada e inequívoca, nos termos da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), a coleta, o tratamento e a utilização dos meus dados pessoais, imagem, voz, fotografias, vídeos e relatos institucionais produzidos no âmbito das atividades promovidas pela Anater.

A presente autorização possui finalidade exclusivamente institucional, educacional, técnica, informativa, de monitoramento, transparência, prestação de contas, divulgação de resultados e comprovação da execução das ações e contratos vinculados à assistência técnica e extensão rural – Ater.

Os dados e materiais poderão ser utilizados pela Anater em:

I – relatórios técnicos e administrativos;

II – sistemas internos de acompanhamento e monitoramento;

III – publicações institucionais;

IV – sítios eletrônicos e redes sociais institucionais;

V – materiais educativos e informativos;

VI – eventos, apresentações e ações de divulgação institucional;

VII – processos de fiscalização, auditoria e prestação de contas junto aos órgãos de controle.

A Anater compromete-se a realizar o tratamento dos dados em conformidade com os princípios da finalidade, adequação, necessidade, segurança e transparência previstos na LGPD, adotando medidas razoáveis para proteção das informações pessoais.

O titular poderá, a qualquer momento, solicitar informações, correção, limitação ou revogação deste consentimento, mediante requerimento formal à Anater, observadas as hipóteses legais de manutenção de dados necessárias ao cumprimento de obrigação legal, regulatória ou de interesse público.

A presente autorização é concedida gratuitamente, sem qualquer ônus ou expectativa de remuneração.

Brasília, _____ de _____ de _____.

_____

Nome Completo

_____

Assinatura

Documento assinado eletronicamente por **Loroana Coutinho de Santana**, **Presidente**, em 22/05/2026, às 17:45, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sérgio Rosa**, **Diretor (a)**, em 22/05/2026, às 18:49, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Isabel Cristina Lourenço da Silva**, **Diretora Técnica**, em 22/05/2026, às 23:13, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **52902926** e o código CRC **2A2F4CE3**.

Referência: Processo nº 21490.000037/2026-81 SEI nº 52902926