ANA
AGÊNCIA NACIONAL DE ÁGUAS E SANEAMENTO BÁSICO

AS ÁGUAS CONECTAM E O SANEAMENTO TRANSFORMA

RESOLUÇÃO ANA Nº 253, DE 3 DE JULHO DE 2025
DOCUMENTO Nº 0063545

Dispõe sobre a política de segurança da informação e comunicação (POSIC), no âmbito da Agência Nacional de Águas e Saneamento Básico (ANA).

A DIRETORA-PRESIDENTE SUBSTITUTA 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 02501.003137/2024-86.

CONSIDERANDO o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que estabelece diretrizes sobre o tratamento de dados pessoais;

CONSIDERANDO o disposto na Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que regula o uso da internet no Brasil;

CONSIDERANDO a Instrução Normativa nº 5, de 30 de agosto de 2021, da Secretaria de Governo Digital, que dispõe sobre os requisitos mínimos de segurança da informação para a utilização de soluções de computação em nuvem pela administração pública federal;

CONSIDERANDO as boas práticas descritas nos padrões NIST SP 800-144, na norma ISO 27017, e nos *frameworks* COBIT 2019 e CIS Controls, que possuem o objetivo de orientar a elaboração de políticas de computação em nuvem, para uma construção de um ambiente mais seguro e robusto; e

CONSIDERANDO a necessidade de garantir a proteção das informações, a segurança dos ativos de tecnologia da informação e a continuidade dos serviços prestados pela ANA.

RESOLVE:

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicações (POSIC) e suas regras no âmbito da Agência Nacional de Águas e Saneamento Básico (ANA), conforme anexos desta Resolução.

Art. 2º Ficam revogadas:

I – a resolução ANA nº 1078, de 14 de setembro de 2015;

II – a resolução ANA nº 529, de 23 de maio de 2016;

III – a resolução ANA nº 1099, de 26 de junho de 2017 e

IV – a resolução ANA nº 38, de 24 de junho de 2019.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

(assinado eletronicamente)
ANA CAROLINA ARGOLO

ANEXO I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA ANA
CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A POSIC é uma declaração formal da ANA acerca do seu compromisso com a proteção dos ativos de informação, físicos e de *software*, de sua propriedade e sob sua guarda.

Art. 2º O objetivo da POSIC é estabelecer diretrizes e responsabilidades no que diz respeito ao manuseio, tratamento, controle e proteção dos ativos de informação, servindo de apoio à alta administração da instituição na implementação da gestão de Segurança da Informação e Comunicação (SIC).

Art. 3º O escopo da POSIC envolve aspectos estratégicos, estruturais, organizacionais e humanos, bem como elementos físicos e lógicos, preparando a base para elaboração dos demais documentos normativos.

Art. 4º A POSIC deve ser cumprida por todos que tenham acesso a quaisquer ativos de informação, físicos e de *software*, de sua propriedade e sob sua guarda, mesmo em trabalhos fora da Agência, como *home office*.

Art. 5º A POSIC deve estar em conformidade com requisitos legais, políticas, regras e normas de SIC.

Art. 6º Para os fins desta Resolução, considera-se o glossário de Segurança da Informação do Gabinete de Segurança Institucional – GSI aprovado pela Portaria GSI nº 93, de 18 de outubro de 2021.

Art.7º A ANA deve elaborar e monitorar normativos de cada tema exposto nesta Política.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 8º A POSIC é guiada pelos seguintes princípios, além dos princípios da administração pública:

I – criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

II – a disponibilidade: propriedade de que a informação esteja acessível e utilizável por uma pessoa física, sistema, órgão ou entidade;

III – a confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou credenciados;

IV – a integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;

V – a autenticidade: propriedade que garante a veracidade da informação, ou seja, garante a legitimidade; e

VI – o não repúdio ou irretratabilidade: é a garantia de que uma determinada ação realizada por um usuário não possa ser negada.

CAPÍTULO III

DAS DIRETRIZES GERAIS
SEÇÃO I
DAS RESPONSABILIDADES DO USUÁRIO

Art. 9º São responsabilidades do usuário:

I – participar de programas de conscientização e treinamento em Segurança da Informação para entender os riscos, as melhores práticas e políticas da ANA;

II – proteger suas credenciais de acesso e seguir as políticas de controle de acesso da ANA para garantir que apenas usuários autorizados tenham acesso aos sistemas e dados;

III – criar senhas fortes e exclusivas para suas contas e nunca as compartilhar com outras pessoas;

IV – proteger suas senhas contra acesso não autorizado;

V – proteger seus certificados digitais;

VI – usar os ativos de TI da ANA de forma apropriada e apenas para fins autorizados;

VII – proteger os dispositivos físicos, como *laptops, smartphones* e *tokens*, contra roubo ou acesso não autorizado. Isso inclui manter os dispositivos em locais seguros quando não estiverem em uso;

VIII – aplicar, quando for o caso, todas as atualizações e correções de segurança disponibilizadas pelos administradores da rede para garantir que os sistemas e aplicativos da ANA estejam protegidos contra vulnerabilidades desconhecidas;

IX – relatar imediatamente, por meio de abertura de chamado, no sistema disponibilizado pela STI, quaisquer incidentes de segurança, como: perda ou roubo de dispositivos, *e-mails* suspeitos, tentativas de *phishing* ou *malware* etc.; e

X – armazenar os arquivos de acordo com a política de backup da ANA.

Art. 10. É dever de todos os usuários da informação zelar pela SIC, não havendo o direito de alegar desconhecimento da POSIC e do termo de responsabilidade em anexo.

SEÇÃO II
DAS DIRETRIZES PARA O TRATAMENTO E GESTÃO DE ATIVOS

Art. 11. Os ativos de cada setor serão de responsabilidade do seu gestor, ou de alguém por ele designado, que ficará encarregado pela sua manutenção e documentação, bem como pela notificação de qualquer evento que aconteça.

Art. 12. Os usuários devem cumprir os requisitos de Segurança da Informação associados ao ativo e aos recursos de processamento da informação, bem como zelar pelos ativos empossados.

Art. 13. O uso de ativos fora da Agência, devem ser autorizados, seguindo procedimento interno.

Art. 14. Os ativos não mais utilizados pelos usuários, em meio eletrônico ou não, devem ser apagados ou destruídos conforme regras da legislação vigente.

Art. 15. Após o desligamento de colaboradores ou servidores, partes externas ou remoção de servidores a outros órgãos, a ANA deverá recolher todos os ativos físicos e informações sob custódia desses agentes.

Art. 16. Como ativo de *software*, a Agência veda a utilização ou instalação de *software* que possa de qualquer forma ferir as disposições desta POSIC, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes.

Art. 17. O normativo de Gestão de Ativos deverá conter procedimentos de criação, monitoramento e remoção de ativos, seja de TI ou de Informação, bem como complementar as diretrizes que estão minimamente expostas nesta Política.

SEÇÃO III
DOS SERVIÇOS DE REDE

Art. 18. Os serviços de rede no ambiente da ANA também constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem definidos em normas específicas.

Parágrafo único. Todo acesso externo à rede corporativa deverá ser, previamente, justificado pela área demandante e, autorizado pelo titular da área de TI ou ponto focal da área.

CAPÍTULO IV
DAS DIRETRIZES ESPECÍFICAS
SEÇÃO I
DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 19. A ANA manterá permanentemente um núcleo de tratamento e resposta a incidentes de SIC com a responsabilidade de receber, filtrar, classificar e responder às solicitações e alertas, além de realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa.

§ 1º A ANA possui uma Equipe de Tratamento e Respostas a Incidentes (ETIR) instituída pela Portaria ANA n° 402 de 15 de julho de 2022, que tem por missão receber, analisar e propor respostas a notificações e realização de ações e medidas necessárias para reforçar a resposta ou a postura da organização, na recuperação de incidentes cibernéticos.

§ 2º Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da ANA serão caracterizadas como um incidente de Segurança da Informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de Segurança da Informação dos itens afetados.

§ 3º São responsabilidades e atribuições específicas da ETIR:

I – coordenar as atividades de tratamento e resposta a incidentes em redes computacionais;

II – apoiar a recuperação de sistemas;

III – realizar análise de ataques e intrusões;

IV – cooperar com outras equipes;

V – participar de comunidades e redes nacionais e internacionais;

VI – gerenciar incidentes de segurança em redes computacionais;

VII – investigar e avaliar danos decorrentes de quebras de segurança;

VIII – registrar todos os incidentes de segurança em redes de computadores, com a finalidade de assegurar registro histórico das atividades da ETIR; e

IX – realizar tratamento da informação de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

§ 4º Faz parte do escopo da equipe da ETIR propor medidas de prevenção para mitigar possíveis paralizações dos serviços de infraestrutura da ANA.

§ 5º As ações preventivas, dentre outras, referem-se às atividades de proteção da informação de forma preventiva e planejada;

§ 6º Externamente, a ETIR poderá se relacionar com:

I – as demais equipes de prevenção, tratamento e resposta a incidentes cibernéticos da

Administração Pública Federal; como o Centro de Tratamento de Incidentes de Redes do Governo - CTIR Gov, ou equivalente;

II – os órgãos, entidades e empresas, públicas ou privadas, que tenham relacionamentos com a ANA para o intercâmbio de informações; e

III – o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR).

§ 7º Todos os incidentes de Segurança da Informação, bem como as suspeitas de sua ocorrência, deverão ser imediatamente comunicados à unidade de Segurança da Informação, por meio da abertura de chamado no sistema disponibilizado pela STI.

§ 8º As soluções de contorno estabelecidas pela ETIR, a fim de mitigar a ocorrência de incidentes de segurança, deverão ser comunicadas ao Gestor de Segurança da Informação, que será responsável por sua avaliação e aprovação.

§ 9º As evidências dos incidentes de Segurança da Informação serão coletadas, armazenadas e apresentadas à ETIR, o mais brevemente possível após a sua ocorrência, conforme diretrizes da unidade de Segurança da Informação.

SEÇÃO II
DA GESTÃO DE RISCOS

Art. 20. A ANA deverá elaborar e manter Plano de Gestão de Riscos de Segurança da Informação e Comunicação (SIC) com base na legislação vigente, contendo necessariamente, lista das ameaças mais prováveis e suas ocorrências, classificação dos riscos e alternativas para mitigá-los.

§ 1º O processo de Gestão de Riscos de SIC deve estar alinhado ao planejamento estratégico da ANA e ao processo maior de gestão de riscos corporativos.

§ 2º A abordagem de Gestão de Riscos de SIC estará alinhada ao processo de gestão de risco de todas as áreas da ANA.

§ 3º O processo de gestão de riscos de SIC possibilitará a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

SEÇÃO III
DA GESTÃO DE CONTINUIDADE

Art. 21. A ANA deve adotar um conjunto de procedimentos emergenciais mediante a definição de um Sistema de Gestão de Continuidade em TIC, para a eventualidade da ocorrência de algum incidente de Segurança da Informação que possa causar interrupção na continuidade de processos organizacionais para a ANA, decorrentes de desastres ou falhas em recursos de TI.

§ 1º O Plano de Continuidade em TI abrange as estratégias necessárias à continuidade dos serviços essenciais para serviços de contingência, continuidade e recuperação.

§ 2º A ANA estabelecerá procedimentos a serem seguidos para minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

§ 3º O Plano de Continuidade de TI tem como objetivos:

I – traçar estratégias e planos de ação que garantam o funcionamento e a disponibilidade dos serviços essenciais da Superintendência de Tecnologia da Informação (STI) durante as mais diversas situações de falha e indisponibilidade dos serviços; e

II – uma vez identificadas falhas nos serviços de TIC, o Plano de Continuidade de TI será

acionado com vistas a prover medidas de proteção rápidas e eficazes para os processos de TI relacionados aos sistemas críticos, nos casos de incidentes graves ou desastres.

SEÇÃO IV
DA AUDITORIA E APROVAÇÕES DOS NORMATIVOS

Art. 22. Todos os ativos de informação, ativos de *software*, ativos físicos e serviços de rede no âmbito da ANA são passíveis de auditoria técnica a cargo da POSIC, desde que autorizada pelo Titular da STI.

§ 1º Cabe à Câmara de Governança Digital e Segurança da Informação e Comunicações (CGDI) propor políticas correlatas, planos de auditoria e conformidade para o efetivo cumprimento do estabelecido por esta POSIC, no âmbito da ANA, conforme disposto na Resolução ANA n° 184, de 15 de fevereiro de 2024.

§ 2º Cabe à STI definir e implementar métodos, técnicas, procedimentos, normas internas da TI e responsabilidades para a execução do estabelecido por esta POSIC, no âmbito da ANA.

§ 3º A STI deve manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados, armazenando os registros de auditorias (*logs*).

§ 4º A fim de preservar a integridade das informações institucionais, a imagem da organização, garantir a segurança dos sistemas, e para fins de apuração de prática indevida, poderão ser monitorados, de forma contínua, e gerados relatórios anuais dos seguintes conteúdos:

I – endereços de correio eletrônico;

II – s*ites* acessados;

III – arquivos residentes em recursos de TI e afins;

IV – arquivos na nuvem corporativa da ANA;

V – programas de computador (*software*); e

VI – bases específicas de controle (*logs*).

§ 5º A entrada e a saída de ativos de informação da ANA, inclusive publicação e disponibilização, serão registradas e autorizadas por autoridade competente mediante procedimento formal.

§ 6º No acesso aos sistemas da ANA:

I – os registros (*logs*) serão protegidos contra a falsificação e acesso não autorizado;

II – todas as atividades dos administradores e operadores do sistema serão registradas; e

III – é obrigatória a produção e manutenção, por período previamente determinado, registros (*logs*) que possam ser usados como trilha de auditoria, contendo atividades dos usuários, exceções e outros eventos de Segurança da Informação para auxiliar em futuras investigações e monitoramento de controle de acesso.

SEÇÃO V
DO CONTROLE DE ACESSO, DAS CONTAS E CREDENCIAMENTO DO USUÁRIO

Art. 23. A Agência deve implementar, acompanhar e avaliar as seguintes assertivas:

§ 1º A autorização, o acesso, o uso da informação e dos recursos de TI serão controlados e limitados ao cumprimento das atribuições de cada servidor e colaborador da ANA.

§ 2º As regras de controle de acesso serão implementadas em diferentes granularidades, desde a cobertura de redes a sistemas inteiros, além de considerar a localização do usuário e o tipo de conexão de rede que é usada para acesso, como no caso de usuários que residem fora do país.

§ 3º Sempre que houver mudanças nas atribuições de determinado usuário da ANA, será de responsabilidade da chefia imediata, solicitar a adequação imediata dos privilégios de acesso às informações e dos recursos de TIC.

Art. 24. A ANA deverá implementar, acompanhar e avaliar o processo de credenciamento, no qual deverá cumprir no mínimo, com as seguintes assertivas:

§ 1º A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso na ANA.

§ 2º A concessão de acesso ocorrerá somente após o processo de credenciamento do usuário pela área responsável.

§ 3º A área responsável deve realizar o credenciamento do usuário, bem como registrar e solicitar a concessão, alteração ou revogação das permissões de acesso junto à área de TI.

§ 4º A equipe de TI somente concederá ou modificará as permissões de acesso mediante procedimento formal da área responsável.

§ 5º A área de TI ao realizar o processo de credenciamento deve utilizar um identificador único para acesso, que deve ser pessoal e intransferível (exceto os casos em que o usuário exerça função de administração da rede local).

§ 6º O perfil de administrador de rede somente será concedido para servidores e colaboradores que executam tarefas específicas na administração dos recursos de TI que compõem a rede corporativa da ANA.

SEÇÃO VI
DO USO DE CORREIO ELETRÔNICO INSTITUCIONAL

Art. 25. Todos os servidores da ANA possuirão um endereço de correio eletrônico institucional.

§ 1º O nome de usuário seguirá a nomenclatura padronizada pelas regras de formação de nomes para a composição de endereço eletrônico (*e-mail*) no Governo Federal, composto pelo nome seguido de ponto e de um sobrenome.

§ 2º O correio eletrônico corporativo é uma ferramenta comunicacional de trabalho de uso obrigatório no âmbito da ANA.

§ 3º O correio eletrônico corporativo é destinado para uso exclusivo em serviço e relacionado estritamente às atividades profissionais do usuário no âmbito da ANA.

§ 4º O correio eletrônico corporativo pode ser monitorado a qualquer tempo pela Administração, desde que autorizado pelo Titular da STI, não cabendo ao usuário do serviço alegar ofensa ao sigilo das comunicações via rede, seja em texto, imagem ou som.

SEÇÃO VII
CERTIFICADO DIGITAL

Art. 26. Os certificados digitais na ANA serão adquiridos pela Autoridade Certificadora – AC, credenciada pela Infraestrutura de Chaves Públicas Brasileira - (ICP-Brasil), garantindo que o documento com a assinatura digital tenha a mesma validade de um documento com assinatura física, regulamentado pelo Decreto nº 10.543, de 13 de novembro de 2020 (alterado pelo Decreto nº 11.797, DE 27 de novembro de 2023).

§ 1º O uso de Certificado Digital deverá seguir a Resolução ANA nº 500, de 11 de maio de 2015 e suas atualizações.

§ 2º O Certificado Digital é de uso pessoal, intransferível, cabendo ao usuário zelar pela confidencialidade da senha, bem como pela guarda e pela conservação do Certificado e do respectivo

suporte criptográfico, sob pena de responsabilidade civil, penal ou administrativa.

§ 3º Os Certificados Digitais utilizados no âmbito da ANA serão de pessoa física (e-CPF), de pessoa jurídica (e-CNPJ), e de equipamento (e-servidor) ou de aplicação (e-aplicação).

Art. 27. Os certificados digitais e-CPF serão emitidos conforme necessidades demandadas pelas atribuições exercidas pelo servidor.

§ 1º Por uma questão de Segurança da Informação, a posse do certificado digital e a senha são de uso pessoal e intransferível, por isso, nem a STI, nem a autoridade certificadora detém responsabilidade sobre o certificado digital.

§ 2º Em caso de bloqueio de uso errado da senha ou perda da mídia (*token*), durante o período de validade do certificado digital, o servidor arcará com os custos de reemissão do Certificado Digital por meio de Guia de Recolhimento da União - GRU.

Art. 28. Em caso de impossibilidade técnica temporária no uso dos certificados digitais, o documento com a assinatura digital tem a mesma validade de um documento com assinatura física.

Parágrafo único. Os documentos poderão ser assinados eletronicamente pelo GOV.BR, através da conta pessoal gov.br do servidor.

SEÇÃO VIII
CÓPIA DE SEGURANÇA (BACKUP)

Art. 29. Os procedimentos próprios ao serviço de backup (cópia de segurança) e restore (restauração de cópia de segurança) serão regulamentados, considerando as seguintes diretrizes:

§ 1º O serviço de backup e restore deve ser automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas “janelas de backup”, ou seja, nos períodos em que há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

§ 2º A solução de backup deverá ser mantida atualizada, considerando suas diversas características como, atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros.

§ 3º A administração das mídias de backup deverá ser contemplada nas políticas e normas complementares sobre o serviço, objetivando manter sua segurança e integridade.

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

§ 5º A execução de rotinas de backup e restore deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

§ 6º Toda informação custodiada pela área de tecnologia da ANA considerada crítica para a execução das atividades da ANA deverá possuir cópia de segurança e será armazenada em local protegido, compatível com o grau de segurança necessário.

§ 7º Os arquivos dos servidores e colaboradores armazenados nas pastas corporativas, caixas de correio eletrônico, bases de dados e os arquivos de sistemas terão suas regras estabelecidas na Política de Backup e Restore.

SEÇÃO IX
DATA CENTER

Art. 30. Os procedimentos para administração do centro de processamento de dados (*data center*) serão regulamentados mediantes as seguintes diretrizes gerais:

I – a gestão de dados e de serviços de *data center* é de competência exclusiva da área de TI;

II – o acesso físico ao *data center* deverá ser feito por sistema de autenticação forte, como

fechadura eletrônica com reconhecimento facial;

III – o acesso físico por meio de chave apenas poderá ocorrer em emergências, quando a segurança física do *data center* estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando;

IV – o acesso ao *data center* por visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor autorizado, que deverá preencher a solicitação de acesso prevista em norma complementar;

V – deverá ser executada, em frequência predeterminada, auditoria dos acessos ao *data center* – por meio de relatório do sistema de registro próprio;

VI – a lista de usuários com direito de acesso ao *data center* deverá ser constantemente atualizada. Ocorrendo o desligamento de usuários que possuam acesso ao *data center*, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de usuários autorizados; e

VII – a função de administrador do *data center* – incluindo seu sistema de autenticação forte – deverá ser atribuída exclusivamente a servidor público efetivo, preferencialmente vinculado à área de infraestrutura de TI da ANA.

SEÇÃO X
TRATAMENTO DA INFORMAÇÃO EM NUVEM

Art. 31. A ANA adotará soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

§ 1º O acesso à informação de armazenamento no ambiente de nuvem contratado será protegido de usuários externos e de pessoas não autorizadas, de forma a propiciar o isolamento adequado dos recursos utilizados pelos usuários do serviço de nuvem.

§ 2º A ANA fará a implantação do suporte aos mecanismos de Autenticação Multifator (MFA) ou criará uma alternativa que aumente o grau de segurança no processo de autenticação dos seus usuários no provedor de serviço de nuvem, de acordo com nível de criticidade da informação.

Art. 32. No tratamento da informação em ambiente de computação em nuvem, a ANA, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

I – informação sem restrição de acesso: pode ser tratada, a critério da ANA, em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC; e

II – informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:

a) informação classificada: é vedado o tratamento em ambiente de computação em nuvem;

b) conhecimento e informação contidos em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;

c) informação com restrição de acesso prevista em legislação vigente: a critério da ANA, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC; e

d) informação pessoal relativa à intimidade, vida privada, honra e imagem: a critério da ANA, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigentes e os riscos de SIC.

SEÇÃO XI
SEGURANÇA DE REDES

Art. 33. O acesso e uso da *internet* é facultado a todo usuário da rede local da ANA, em conformidade com os termos estabelecidos nesta Política.

§ 1º Todas as regras corporativas sobre uso de *internet* visam ao desenvolvimento de um comportamento ético e profissional, de modo que, embora a conexão direta e permanente da rede corporativa da ANA com a *internet* ofereça um grande potencial de benefícios, a proteção dos ativos de informação da ANA deve sempre ser privilegiada.

§ 2º Qualquer informação que seja acessada, transmitida, recebida ou produzida na *internet* está sujeita à divulgação e auditoria. Portanto, a ANA, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores.

§ 3º Os equipamentos, tecnologias e serviços fornecidos para o acesso à *internet* são de propriedade da ANA, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/*internet*, estejam eles em disco local, no *Desktop* ou em áreas privadas da rede, visando a assegurar o cumprimento da POSIC.

§ 4º É vedada a utilização da *internet* de forma a prejudicar a imagem da ANA ou que coloque em risco os ativos da rede local.

§ 5º O acesso à *internet* será monitorado por sistemas e ferramentas de Segurança da Informação sem necessidade de prévio consentimento do usuário.

§ 6º Serão armazenados *logs* de acesso à *internet* referentes aos endereços, horários, tempo de permanência, tipo de conteúdo e volume de informações trafegadas.

§ 7º O acesso à rede corporativa da ANA, incluirá procedimentos e Autenticação Multifator (MFA) a fim de autorizar usuários a entrarem na rede.

§ 8º A área de TI é responsável por manter atualizada toda a segmentação e topologia de rede corporativa ofertada pela ANA.

§ 9º O uso de *firewalls* e dispositivos de segurança serão utilizados para proteger a rede contra ameaças externas.

§ 10 A STI utilizará ferramentas e soluções de Segurança da Informação, a fim de aplicar as melhores práticas no processo de monitoramento e análise do tráfego de rede em busca de atividades suspeitas.

§ 11 Dispositivos que acessam a rede da ANA, tais como: *desktops, laptops e tablets*, devem passar por um processo adicional de instalação e configuração segura que vise o aumento de sua proteção.

§ 12 Dispositivos particulares que acessam a rede da ANA, tais como: *desktops, laptops e tablets*, devem possuir instalado um antivírus atualizado, e se possível uso de *firewall*. Dispositivos patrimoniados pela ANA devem possuir antivírus corporativo atualizado e operacional.

§ 13 A rede corporativa sem fio deverá ser implementada de forma isolada das demais redes da ANA e deverão ser adotados mecanismos de autenticação centralizada com controles de acesso.

§ 14 Os servidores e colaboradores da ANA deverão utilizar o mesmo *login* e senha de acesso à rede corporativa da ANA.

Art. 34. É proibido utilizar a *internet* para acessar conteúdos digitais que contenham:

I – materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

II – arquivos que contenham informação criminosa ou ilegal;

III – arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares; e

IV – atividades relacionadas a jogos eletrônicos pela *internet*.

Art. 35. A ANA disponibilizará uma rede segregada da rede coorporativa para o acesso à *internet* por visitantes.

Parágrafo único. O acesso de visitantes à rede sem fio adotará os mesmos critérios de

segurança aplicados à rede corporativa.

SEÇÃO XII
DO USO DE DISPOSITIVOS MÓVEIS/PORTÁVEIS

Art. 36. O uso dos dispositivos móveis portáteis pelos servidores públicos usuários da rede da ANA deverá ser realizado no interesse da Agência.

§ 1º São considerados dispositivos móveis portáteis os *laptop*s e notebooks.

§ 2º Qualquer dispositivo móvel utilizado para acessar a rede corporativa da ANA deverá estar em conformidade com os padrões estabelecidos por esta Política.

§ 3º O uso de dispositivos móveis na ANA será pautado pela necessidade e interesse da Agência.

§ 4º Os dispositivos móveis devem ser utilizados somente pelos usuários que assumiram formalmente a responsabilidade pelo seu uso.

Art. 37. Quanto aos dispositivos móveis corporativos:

§ 1º Todos os dispositivos móveis corporativos devem ser inventariados.

§ 2º Os dispositivos móveis devem possuir somente os *softwares* homologados e instalados pela área de TI.

§ 3º O usuário não deve instalar ou desinstalar qualquer tipo de *software* nos dispositivos móveis.

§ 4º Os dispositivos móveis devem ser registrados como membros de um domínio de rede, sempre que tecnicamente possível.

§ 5º Os dispositivos devem oferecer mecanismos que garantam o controle de acesso e sigilo das informações neles armazenada, como por exemplo: senhas, usuários e senhas, *token*s, criptografia dos dados etc.

§ 6º É necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário ou dispositivo, às conexões de rede e recursos disponíveis.

§ 7º Os usuários da ANA devem adotar mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em casos de extravio. Um mecanismo é utilizar o salvamento dos dados em servidores de arquivos disponibilizados pela área de TI da ANA.

§ 8º É de uso exclusivo da área de TI o uso da conta “Administrativa”. O uso dessa conta é restrito às atividades de manutenção do equipamento.

§ 9º A utilização de contas com perfil de “Administrativo” nos dispositivos móveis só será autorizada quando devidamente formalizada e justificada à área de TI, podendo ser submetida à aprovação da DIREC.

Art. 38. Os usuários que utilizarem dispositivos móveis de sua propriedade dentro dos ambientes físicos ou virtuais da ANA deverão observar as seguintes diretrizes:

I – caso necessitem conectar seus dispositivos móveis à rede da ANA, devem respeitar os procedimentos de controle e concessão de acesso para visitantes;

II – é responsabilidade do usuário conhecer e cumprir as normas internas relativas ao uso da rede;

III – o visitante não poderá acessar a rede corporativa, exceto nos casos em que a UORG disponibilizar uma rede isolada específica para esta finalidade, sendo obrigatória a concordância e assinatura do Termo de Sigilo e Responsabilidade; e

IV - o usuário deve realizar uma varredura com o *software* antivírus disponível antes de gravar no equipamento portátil de TI qualquer informação que receba por *e-mail* ou mídias de armazenamento removíveis.

SEÇÃO XIII
DO ACESSO REMOTO

Art. 39. O acesso remoto, definido como a conexão entre uma rede de dados externa e a rede de dados da instituição, estará sujeito às seguintes diretrizes:

I – acesso remoto à rede de dados da ANA será permitido exclusivamente para fins de trabalho, e em caráter excepcional;

II – a solicitação de acesso remoto deverá ser formalizada junto à área de TI, acompanhada da justificativa da necessidade e do período de uso;

III – a área de TI será responsável pelo registro e monitoramento dos acessos remotos dos usuários;

IV – o acesso remoto será concedido por um período previamente definido;

V – toda conexão remota à rede da ANA deverá ser realizada por meio de canal criptografado e autenticação do usuário;

VI – a área de TI deverá informar aos usuários os requisitos mínimos de segurança para realização de acesso remoto;

VII – os recursos de TI utilizados no ambiente de trabalho remoto, como equipamentos em residências, deverão estar protegidos contra vírus, *software*s maliciosos e acessos não autorizados;

VIII – o acesso à rede da ANA será permitido apenas a partir de recursos de TI previamente cadastrados e homologados pela área de TI;

IX – quando os recursos tecnológicos forem de propriedade de terceiros, a área de TI deverá exigir que tais equipamentos atendam aos requisitos mínimos de segurança estabelecidos;

X – a área de TI deverá garantir a capacitação dos usuários quanto à utilização da solução de acesso remoto;

XI – serão implementados mecanismos de proteção adequados às redes de dados sob responsabilidade da respectiva UORG, bem como aos serviços a elas conectados; e

XII – o usuário será responsável por todas as operações realizadas por meio do acesso remoto, incluindo acessos, processamento e comunicação de dados.

Parágrafo único. O acesso remoto será concedido aos usuários mediante solicitação da chefia imediata, por meio da abertura de chamado na ferramenta de atendimento disponibilizada pela STI.

SEÇÃO XIV
DO USO DE RECURSOS DE TI

Art. 40. Os usuários são responsáveis por proteger os recursos de TI da ANA contra acesso, modificação, destruição ou divulgação não autorizada, e devem:

I – utilizar os recursos de TI colocados à sua disposição exclusivamente para os fins institucionais aos quais se destinam;

II – abster-se de abrir o gabinete dos *Desktops* o u *Laptops*, bem como de modificar qualquer configuração, seja de *hardware* ou *software*;

III – respeitar as configurações padronizadas, conforme definições da área de TI;

IV – encaminhar solicitação à área de TI para análise, sempre que houver a necessidade de alteração das configurações padronizadas;

V – nunca instalar ou executar *softwares* de sua propriedade, ou de terceiros, sem prévia homologação e autorização da área de TI;

VI – Desligar corretamente os *Desktops* o u *Laptops* ao final do expediente, conforme procedimentos estabelecidos pelo sistema operacional.

VII – conectar os *Desktops* e *Laptops* da ANA exclusivamente em pontos elétricos estabilizados, evitando o uso conjunto com outros equipamentos que não sejam recursos de TI.

VIII – armazenar arquivos com informações institucionais nos servidores de arquivos disponibilizados pela STI.

IX – evitar o armazenamento de arquivos nos *Desktops*, pois esses equipamentos não possuem rotina de *backup*.

X – evitar tratar de assuntos sensíveis da ANA em locais públicos ou inadequados, limitando-se a discutir tais questões somente em ambientes que ofereçam a devida proteção; e

XI – colaborar ativamente na resolução de problemas e no aprimoramento dos processos de Segurança da Informação da ANA.

SEÇÃO XV
DA POLÍTICA DE MESA E TELA LIMPA

Art. 41. O usuário de recursos de TI da ANA deverá adotar a política de “mesa limpa e tela limpa”.

§1º A política de "mesa limpa e tela limpa" consiste em uma prática de Segurança da Informação destinada a proteger dados sensíveis e prevenir vazamentos de informações. Ela assegura que servidores e colaboradores mantenham suas áreas de trabalho físicas (mesa) e digitais (tela) livres de informações confidenciais quando não estiverem em uso, sendo uma prática recomendada por normas de Segurança da Informação, como a ISO 27001.

§ 2º Os usuários devem observar as seguintes recomendações:

I – limpar suas mesas regularmente, removendo todos os documentos ou materiais impressos que contenham informações sensíveis quando não estiverem em uso;

II – evitar deixar documentos sigilosos sobre as mesas, especialmente na ausência do usuário;

III – utilizar gavetas e armários com fechaduras para armazenar arquivos físicos contendo informações sensíveis; e

IV – bloquear a tela dos seus dispositivos (computadores, *laptop*s, *smartphones*, *tablets*) e fechar aplicativos ou documentos sensíveis sempre que não estiverem em uso.

SEÇÃO XVI
SEGURANÇA DE SISTEMAS E SOLUÇÕES

Art. 42. A segurança de sistemas e soluções observará o seguinte:

I – qualquer *software* que, por necessidade do serviço da UORG, necessitar ser instalado, deverá possuir prévia anuência da STI, solicitada por meio da abertura de chamado, a fim de verificar se as regras de segurança veiculadas pela solução estão sendo cumpridas;

II – fica permanentemente proibida a instalação de quaisquer *softwares* sem licença de uso;

III – instalação de *software* em sistemas operacionais será controlada de forma a garantir o controle sobre as aplicações instaladas;

IV – a implementação de mudanças será controlada por meio da abertura de chamado no sistema estabelecido pela STI, com a criação de uma Requisição de Mudança (RDM); e

V – as aplicações críticas da ANA serão analisadas criticamente e testadas quando sistemas operacionais forem alterados (novas versões ou instalação de patches), para garantir que não haverá

impacto adverso nas operações da ANA ou na segurança.

Art. 43. Cabe à área de TI da ANA, por meio de servidores designados, a supervisão e o monitoramento do desenvolvimento terceirizado de *software,* de forma a garantir que critérios de segurança, qualidade, conformidade e desempenho sejam devidamente implementados.

SEÇÃO XVII
PROTEÇÃO CONTRA MALWARE E ATAQUES CIBERNÉTICOS

Art. 44. Os recursos de TI da ANA deverão ser dotados de soluções para detecção e bloqueio de códigos maliciosos, contendo no mínimo as seguintes ferramentas:

I – *antispyware;*

II – *antimalware;*

III – *firewall;*

IV – IPS (*Intrusion Prevention System*); e

V – IDS (*Intrusion Detection System*).

Parágrafo único. A STI poderá adotar outras soluções e mecanismos complementares para detecção e bloqueio de ameaças, bem como medidas adicionais que fortaleçam a segurança dos sistemas e mitiguem vulnerabilidades associadas a códigos maliciosos ou tentativas de acesso não autorizado.

Art. 45. Com o objetivo de combater ataques cibernéticos e garantir a Segurança da Informação, a ANA adotará as seguintes medidas:

I – proibição expressa da utilização de *softwares* não autorizados;

II – restrição do registro das tentativas de acesso a *websites* maliciosos ou suspeitos, por parte dos usuários;

III – exigência de precauções por parte dos usuários, que deverão examinar com ferramenta antivírus, arquivos e *softwares* importados de redes ou mídias externas;

IV – instalação e atualização periódica de *software* de detecção e remoção de *malware*, para realizar a varredura de computadores e mídias magnéticas;

V – isolamento, na medida do possível, de ambientes críticos suscetíveis à contaminação por *malwares*, visando prevenir impactos negativos às atividades da instituição;

VI – configuração de varreduras automáticas e completas, a serem realizadas regularmente por soluções de *antimalware;*

VII – manutenção do *antimalware* sempre atualizado; e

VIII – reforço dos cuidados em casos de dispositivos infectados, com a implementação de medidas para evitar novas infecções.

Art. 46. Serão adotadas formas adicionais de autenticação das contas da ANA, como meio de proteção e prevenção contra vazamentos e acessos indevidos, tais como:

I – verificação em duas etapas, sempre que possível; e

II – trocar imediatamente as senhas ao suspeitar de vazamento ou uso em um dispositivo infectado e não salvar senhas no navegador.

Art. 47. É vedado o uso do privilégio de acesso da conta de administrador no ambiente de infraestrutura de TI da ANA para atividades cotidianas.

§ 1º Exceções devem ser aprovadas pela Diretoria Colegiada da ANA.

§ 2º A conta de administrador deve ser utilizada exclusivamente por colaboradores e servidores da área de infraestrutura e segurança de TI da STI.

Art. 48. Para prevenir e detectar o uso de *software* não autorizado, devem ser configurados controles por meio de *firewalls* de aplicação.

§ 1º *Firewall* contém regras pré-definidas que permitem:

I – autorizar a conexão (*allow*);

II – bloquear a conexão (*deny*); e

III – rejeitar o pedido de conexão sem avisar o emissor (*drop*).

§ 2º Deve-se adotar o modelo de política proibitiva que é o mais seguro e, também, comumente adotado pelos principais órgãos públicos.

§ 3º A equipe de Segurança da Informação determinará quais tipos de *firewall* serão utilizados, tais como:

I – *firewall* pessoal;

II – filtro de pacotes;

III – *proxy Servers;* e

IV – *gateway* de Aplicação.

Art. 49. A ANA adotará um Sistema de Detecção de Intrusos (IDS), um Sistema de Prevenção de Intrusos (IPS) e uma Zona Desmilitarizada (DMZ) bem configurada.

SEÇÃO XVIII
GESTÃO DA SEGURANÇA NAS COMUNICAÇÕES

Art. 50. As informações e símbolos institucionais da ANA somente devem ser divulgados com autorização da ASCOM da ANA ou de gestor por ela delegado.

§ 1º Os servidores da ANA não devem divulgar nos perfis pessoais de redes sociais imagens de servidores, objeto ou símbolo de identificação da ANA, sem prévia autorização da ASCOM.

§ 2º O servidor que vazar ou repassar, sem autorização, informações estratégicas, operacionais, de segurança e de inteligência da ANA estará sujeito às sanções administrativas, cíveis e penais cabíveis.

SEÇÃO XIX
REDES SOCIAIS

Art. 51. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações da ANA, deve estar em consonância tanto com a POSIC quanto com os objetivos estratégicos da instituição.

§ 1º Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo.

§ 2º Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente da ANA.

§ 3º É vedada a terceirização completa da administração e da gestão de perfis de órgãos e entidades da ANA nas redes sociais.

§ 4º O perfil institucional da ANA deve ser protegido por meio das seguintes ações preventivas:

I – não divulgar informações que possam tornar o perfil vulnerável;

II – publicar apenas informações demandadas pela ANA;

III – publicar apenas informações públicas, nos termos da Lei nº 12.527 de 2011; e

IV – alterar as configurações padrões de privacidade, para que sejam acessíveis as informações somente aos interessados.

SEÇÃO XX
SEGURANÇA DE TELECOMUNICAÇÕES

Art. 52. Para garantir a segurança das telecomunicações no desempenho de suas atividades, a ANA deverá:

I – acompanhar os processos licitatórios, garantindo que os materiais e equipamentos cotados atendam às especificações do projeto, sem comprometer a segurança;

II – realizar, de forma preventiva e corretiva, varreduras em sistemas de telecomunicações internos e externos, assegurando a proteção pessoal e das instalações físicas;

III – implementar, de forma preventiva e corretiva, procedimentos de vigilância eletrônica que garantam segurança pessoal e das instalações físicas; e

IV – garantir a proteção e a funcionalidade dos sistemas e processos de comunicação interna e externa da ANA.

Art. 53. Quando ocorrerem desastres naturais, acidentes, outras emergências ou o risco de que tais fenômenos aconteçam, compete à ANA:

I – priorizar as comunicações essenciais, cujo conteúdo seja necessário para a prevenção ou recuperação de incidentes, segurança dos transportes, comunicações, recursos de força elétrica e manutenção da ordem pública;

II – manter adequadamente os recursos de telecomunicações, garantindo o sigilo das comunicações;

III – adotar as medidas para prevenir a divulgação não intencional de outras comunicações durante o uso normal, no ponto de conexão entre os equipamentos terminais de usuários de serviços de telecomunicações e circuitos de telecomunicações; e

IV – adotar medidas para prevenir acessos não autorizados, destruição e falsificação de registros e dados armazenados em recursos de telecomunicações.

SEÇÃO XXI
SEGURANÇA DE RECURSOS HUMANOS

Art. 54. Em relação à segurança em Recursos Humanos, a POSIC deve observar os seguintes procedimentos:

I – o desligamento da ANA, resultará na revogação de todos os direitos de acesso e uso dos ativos a eles atribuídos; e

II – o afastamento, cessão, mudança de responsabilidade, lotação ou alteração nas atribuições implicará na revisão imediata dos direitos de acesso e de uso dos ativos da ANA.

Parágrafo único. A ANA deverá promover continuamente ações de divulgação e conscientização de todos os mencionados nesta Política, por meio de programas de comunicação, sensibilização e capacitação em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança na autarquia.

SEÇÃO XXII
SEGURANÇA EM SERVIÇOS TERCEIRIZADOS

Art. 55. Usuário terceirizado é o prestador de serviço terceirizado, o consultor externo, o estagiário, o contratado temporário, o menor aprendiz ou o participante de grupos deliberativos esporádicos, de empresas formalmente contratadas, que possam fazer uso dos recursos ou acessem informações e sistemas informacionais da ANA.

§ 1º A ANA deverá em seus relacionamentos contratuais com terceiros, definir, especificamente, quais serviços e atividades serão autorizados para acesso e manuseio por terceiros.

§ 2º Deverá ser considerado, sempre, o menor perfil de privilégio para acesso às informações da ANA.

§ 3º Toda atualização da POSIC da ANA, bem como de seus procedimentos, sistemas e processos, serão repassados a terceiros contratados a fim de se manter alinhado o conhecimento e implementação de mudanças de segurança necessárias à ANA.

Art. 56. Os contratos de prestação de serviço devem possuir cláusulas que garantam a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações e recursos de TI da ANA.

§ 1° Os contratos de prestação de serviço devem conter cláusulas que especifiquem a necessidade da assinatura do Termo de Sigilo e Confidencialidade por parte de todos os seus prestadores de serviços.

§ 2° Todos os contratos de prestação de serviços firmados pela ANA, conterão cláusula específica sobre obrigatoriedade de atendimento a esta POSIC, bem como suas normas decorrentes.

Art. 57. As realocações e desligamentos de prestadores de serviços serão comunicados previamente ao gestor do contrato na ANA, ou ao responsável designado pelas chefias imediatas destes prestadores.

§ 1° O gestor do contrato ou responsável designado deverá adotar providências para serem realizadas as alterações e os cancelamentos de acessos aos ativos disponibilizados àqueles profissionais.

§ 2° O processo de mudança ou encerramento da contratação deverá proteger os interesses da ANA.

SEÇÃO XXIII
AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Art. 58. Todos os sistemas de informação adquiridos ou desenvolvidos para uso da ANA, devem ter sua continuidade garantida independentemente de eventuais mudanças na relação com o fornecedor.

§ 1º Todo desenvolvimento de sistemas de informação para a ANA deve ser realizado com base em uma Metodologia de Desenvolvimento de Sistemas.

§ 2º Todo projeto de sistema de informação antes da sua concepção, inclusive aquele desenvolvido pelo usuário, deve ser submetido à área de TI para avaliação/homologação dos aspectos de Segurança da Informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

§ 3º Os sistemas e aplicações que serão implantados em produção poderão, a critério da STI, ser submetidos a uma análise técnica prévia, incluindo a realização de testes de vulnerabilidade, conforme as necessidades da área de negócio.

§ 4º Os sistemas de informação classificados como críticos deverão ser desenvolvidos levando em consideração requisitos para sua contingência.

§ 5º Todos os usuários candidatos a utilizar um sistema devem ser treinados e capacitados para exercer suas atividades.

Art. 59. Requisitos de segurança devem ser implementados na definição dos novos sistemas.

§ 1º Poderá ser realizada análise de risco para o levantamento de requisitos de segurança no processo de desenvolvimento de sistemas, de acordo com a coordenação de sistemas.

§ 2º Os requisitos de segurança estarão em todas as fases de criação dos sistemas, ou seja, definição, projeto, desenvolvimento, implantação e manutenção.

Art. 60. Devem ser incorporados controles apropriados em projetos de aplicações para

assegurar o processamento correto.

§ 1º Os controles devem incluir os dados de entrada, o processamento interno e os dados de saída.

§ 2º Controles adicionais para sistemas que processem informações sensíveis, valiosas ou críticas ou que nessas exerçam algum impacto devem ser determinados com base em requisitos de segurança e análise/avaliação de riscos.

§ 3º Devem ser incorporadas nas aplicações checagens de validação com o objetivo de detectar qualquer corrupção de informações por erros ou por ações deliberadas.

§ 4º Devem ser identificados e implementados requisitos e controles apropriados para garantir a autenticidade e proteger a integridade das mensagens em aplicações.

Art. 61. Sobre a segurança em processo de desenvolvimento e de suporte, a área de TI deve supervisionar o processo desde o seu planejamento até a implementação no caso de desenvolvimento de *softwares* por terceiros.

§ 1º Deve ser implementado controle de versão para garantir a gestão dos códigos fontes.

§ 2º Deve ser realizada a análises de riscos a fim de detectar falhas nos sistemas que possam comprometer a Segurança da Informação.

§ 3º Devem ser protegidas as informações envolvidas em transações *online*, a fim de prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

SEÇÃO XXIV
CRIPTOGRAFIA

Art. 62. Devem ser elaboradas e implementadas políticas de utilização de criptografia em sistemas, arquivos e pastas, com o intuito de garantir a confidencialidade das informações, conforme privilégio de acesso de cada usuário.

§ 1º As chaves utilizadas nas soluções de criptografia deverão ser armazenadas em servidores de rede com nível de segurança elevado.

§ 2º Os dados de backup deverão ser protegidos contra alterações não autorizadas e sua transmissão pela rede deverá ser protegido por criptografia.

§ 3 º O usuário deverá atentar-se para as demais normas que versam sobre a transferência de informações confidenciais, restritas ou pessoais.

SEÇÃO XXV
SEGURANÇA DOS ARQUIVOS DO SISTEMA

Art. 63. A segurança de arquivos de sistema abrange um conjunto de medidas e práticas destinadas a proteger os arquivos do sistema operacional e outros arquivos críticos, evitando que sejam modificados, corrompidos ou acessados por usuários não autorizados.

§ 1º Os conjuntos de dados utilizados nos testes da fábrica de *software* devem ser distintos dos utilizados no ambiente de produção.

§ 2º O acesso aos códigos-fonte dos sistemas deve ser rigorosamente controlado e autorizado pela área de TI.

§ 3º O acesso aos arquivos armazenados nos servidores de arquivos da ANA deverá ser autorizado pela autoridade máxima da área responsável, ou por usuários previamente autorizados para essa finalidade.

§ 4º A STI é responsável por autorizar o acesso dos novos usuários da ANA aos arquivos de suas respectivas unidades, podendo delegar essa responsabilidade aos pontos focais das unidades.

SEÇÃO XXVI
SEGURANÇA DE NAVEGAÇÃO

Art. 64. A segurança de navegação refere-se a práticas e estratégias adotadas para proteger os usuários da ANA contra roubos *online*, fraudes e outras ameaças digitais.

Art. 65. Os usuários deverão cumprir os seguintes pontos:

I – verificar a URL dos *sites*;

II – evitar a reutilização de senhas;

III – desabilitar o preenchimento automático de formulários ou a função de "lembrar senha";

IV – ler as políticas de privacidade dos *sites*;

V – ativar bloqueadores de *pop-ups*;

VI – restringir a coleta de dados por *sites*;

VII – limpar regularmente o histórico de navegação; e

VIII – utilizar a navegação anônima ou privativa sempre que possível.

SEÇÃO XXVII
INTELIGÊNCIA ARTIFICIAL (IA)

Art. 66. A ANA utilizará normas internacionais que regulamenta o uso da IA, como a ABNT NBR ISO/IEC 38507.

Art. 67. A Agência deverá trabalhar na implementação de normas adequadas que auxiliam para uma governança eficaz da IA, com foco em responsabilidade social, gestão de riscos, viés e qualidade.

Art. 68. A ANA deverá garantir uma supervisão eficaz da governança da IA implementando controles adequados para assegurar que as políticas e práticas adotadas estejam alinhadas com os objetivos estratégicos e os valores da instituição.

Art. 69. A ANA terá as seguintes estratégias em relação à regulação e ao uso ético da IA:

I – estabelecer, de maneira multissetorial, espaços para a discussão e definição de princípios éticos a serem observados na pesquisa, no desenvolvimento e no uso da IA;

II – estimular ações de transparência e de divulgação responsável quanto ao uso de sistemas de IA;

III – desenvolver técnicas para identificar e tratar o risco de viés algorítmico;

IV – elaborar política de controle de qualidade de dados para o treinamento de sistemas de IA;

V – criar parâmetros sobre a intervenção humana em contextos de IA em que o resultado de uma decisão automatizada implica um alto risco de dano para o indivíduo; e

VI – incentivar a exploração e o desenvolvimento de mecanismos de revisão apropriados em diferentes contextos de utilização de IA.

Art. 70. A POSIC aplicará governança de IA no âmbito da ANA, obedecendo às seguintes diretrizes:

I – promover o desenvolvimento de padrões voluntários e consensuais para gerenciar os riscos associados aos aplicativos de IA;

II – estimular o uso de conjuntos de dados representativos para treinar e testar modelos;

III – melhorar a qualidade dos dados disponíveis, de modo a facilitar a detecção e correção

de vieses algorítmicos;

IV – desenvolver diretrizes para a elaboração de Relatórios de Impacto de Proteção de Dados (RIPD);

V – elaborar campanhas educacionais e de conscientização;

VI – apresentar relatórios com estatísticas e resultados do serviço implementado; e

VII – estabelecer mecanismos supervisores para monitorar o uso da IA para atividades de segurança.

SEÇÃO XXVIII
PROPRIEDADE DA INFORMAÇÃO

Art. 71. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela ANA é considerada parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade, considerando os seguintes dispositivos:

I – toda informação criada ou custodiada que for manuseada, armazenada, transportada ou eliminada pelo colaborador e agente público da ANA, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e nas regulamentações em vigor, conforme a classificação das informações, sem prejuízo da autoria, conforme definido em lei e de acordo com as diretrizes de Classificação da Informação da ANA;

II – quando da obtenção de informação de terceiros com direitos de uso restrito, o gestor da informação deve providenciar, junto à concedente, a documentação formal atinente aos direitos de acesso, antes de seu uso;

III – na cessão de bases de dados custodiadas ou de informação de propriedade da ANA a terceiros, o gestor da informação deve providenciar a documentação formal relativa à autorização de acesso às informações, conforme as diretrizes de Classificação da Informação da ANA;

IV – deve-se estabelecer procedimentos apropriados para garantir a conformidade dos requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e o uso de produtos de *software*s proprietários de acordo com as diretrizes de aquisição, desenvolvimento e manutenção de sistemas;

V – o armazenamento e o processamento de informações baseado em computação em nuvem devem obedecer às diretrizes e normas complementares dessa POSIC e a legislação brasileira, que deve prevalecer sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem;

VI – a informação hospedada na estrutura do Datacenter da ANA deve fazer uso de solução de backup (cópia de segurança) com locais, frequência e demais diretrizes previstas em norma complementar; e

VII – deve-se estabelecer procedimentos de privacidade e proteção de dados que estejam em conformidade com as exigências das legislações relevantes, regulamentações e cláusulas contratuais de acordo com as diretrizes de proteção de dados pessoais da ANA.

Parágrafo único. Os dados privados, pessoais e sensíveis do titular, de crianças e adolescentes devem ser processados de forma legal, justa e transparente em relação aos seus titulares.

SEÇÃO XXIX
CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Art. 72. Toda informação deverá ser protegida durante seu acesso, tráfego, uso, armazenamento e descarte, conforme sua classificação em níveis de sigilo, de acordo com o estabelecido pelos normativos vigentes.

Parágrafo único. As orientações, regras e responsabilidades relativas à classificação, reclassificação, desclassificação, tratamento e descarte das informações produzidas ou custodiadas pela

ANA no exercício de suas competências serão regulamentadas em normas complementares.

Art. 73. A classificação e o tratamento da informação devem seguir os seguintes requisitos e critérios:

I – considerar o valor, os requisitos legais, a sensibilidade e a criticidade da informação para a ANA;

II – definir e implementar um conjunto adequado de procedimentos para rotulação e tratamento das informações, conforme critério de classificação adotado pela ANA; e

III – garantir que toda informação criada, manuseada, armazenada, transportada ou eliminada pela ANA seja classificada com base nos princípios de confidencialidade, integridade e disponibilidade.

Art. 74. A classificação e o tratamento de informação devem:

I – estar alinhados à legislação específica sobre a proteção de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (APF), em especial a Lei nº 12.527, de 2011, o Decreto nº 7.845, de 2012, e a Portaria ANA nº 468, de 5 de dezembro de 2023;

II – ser implementados e mantidos em conformidade com a legislação vigente, assegurando a aplicação dos controles de segurança adequados a cada informação custodiada ou de propriedade da ANA, ao longo de seu ciclo de vida; e

III – observar as diretrizes específicas de classificação da informação estabelecidas pela ANA.

Art. 75. As informações sob gestão da ANA devem ser protegidas contra acessos e usos indevidos, sendo que aquelas classificadas como de alta criticidade exigirão medidas especiais de tratamento, conforme diretrizes de classificação da informação da ANA.

Parágrafo único. A ANA por meio do gestor responsável pelo tratamento e classificação das informações deverá avaliar e definir os procedimentos necessários para garantir o cumprimento das disposições desta seção.

SEÇÃO XXX
TECNOLOGIAS DISRUPTIVAS

Art. 76. As tecnologias disruptivas devem ser consideradas pela ANA como ferramentas estratégicas para modernizar processos, substituindo métodos tradicionais por soluções mais eficientes, ágeis e seguras.

§ 1º A adoção dessas tecnologias deve permitir o armazenamento seguro e otimizado de dados, bem como sua integração com *softwares* avançados de leitura, possibilitando a categorização, distribuição e avaliação das informações geridas pela ANA.

§ 2º Entre as tecnologias disruptivas a serem exploradas, destaca-se a *Internet* das Coisas (IoT), uma rede expansiva de dispositivos conectados à *internet*, que viabiliza a intercomunicação entre aparelhos e otimiza a execução de atividades institucionais.

§ 3º A ANA deve utilizar essas inovações para aprimorar a qualidade e reduzir o custo dos serviços prestados ao cidadão, promovendo uma gestão pública mais eficiente, eficaz, efetiva e inovadora.

CAPÍTULO V
PAPÉIS E RESPONSABILIDADES DE CADA UORG

Art. 77. A estrutura de Gestão de Segurança da Informação na ANA será composta pelo Gestor de Segurança da Informação (GSI), pela CGDI e pela ETIR.

§ 1º De forma complementar, a atribuição de responsabilidades para Segurança da

Informação no âmbito da ANA será exercida pela:

I – Superintendência de Tecnologia da Informação (STI): executa atividades pertinentes à segurança lógica do ambiente e dos recursos de processamento da informação;

II – Comissão Permanente de Avaliação de Documentos Sigilosos – (CPADS): responsável pela verificação do cumprimento das determinações legais pertinentes ao acesso a documentos de caráter sigiloso e pela análise periódica dos documentos sob custódia da ANA, submetendo à Diretoria proposta motivada de classificação dos documentos a terem tratamento sigiloso na organização, bem como dos procedimentos a serem adotados na sua tramitação e os prazos para sua desclassificação;

III – Superintendência de Administração, Finanças e Gestão de Pessoas (SAF): executa atividades pertinentes à segurança física e patrimonial do ambiente e dos recursos de processamento da informação;

IV – Coordenação-Geral de Gestão de Pessoas (CGGEP): executa ações de treinamento e desenvolvimento referentes à SIC, bem como os referentes a recursos humanos que interajam com os recursos de processamento da informação;

V – Assessoria de Comunicação (ASCOM): executa atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela POSIC; e

VI – Auditoria Interna (AUD): executa abordagem sistemática e disciplinada para avaliação e melhoria da efetividade dos processos de SIC.

CAPÍTULO VI
DAS PENALIDADES

Art. 78. Qualquer ação que viole esta POSIC, suas diretrizes, normas ou procedimentos, bem como que infrinja os controles de SIC, será devidamente apurada, aplicando-se aos responsáveis as sanções penais, administrativas e civis cabíveis.

Parágrafo único. O usuário será responsabilizado criminal, disciplinar e civilmente por eventuais prejuízos causados à instituição, podendo, inclusive, ser desligado. Além disso, serão aplicáveis as disposições das seguintes normas:

I – Estatuto do Servidor Público Federal (Lei nº 8.112, de 11 de dezembro de 1990);

II – Código Penal (Decreto-Lei nº 2.848, de 7 de setembro de 1940);

III – Código Civil (Lei nº 10.406, de 10 de janeiro de 2002);

IV – Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018);

V – Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014); e

VI – demais legislações vigentes ou futuras que regulem a matéria.

CAPÍTULO VII
DA POLÍTICA DE PROTEÇÃO DE DADOS

Art. 79. A Política de Proteção de Dados visa estabelecer diretrizes e compromissos instrucionais sobre o tratamento de dados pessoais, nos meios físicos e digitais, para proteção dos direitos fundamentais de liberdade, segurança e de privacidade no âmbito da ANA pelo seguinte arcabouço legal:

I – Portaria ANA nº 385, de 20 de outubro de 2021; e

II – Portaria ANA nº 468, de 5 de dezembro de 2023.

CAPÍTULO VIII
DIVULGAÇÃO E CONSCIENTIZAÇÃO

Art. 80. A divulgação das regras e orientações de Segurança da Informação aplicadas aos

usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na *Intranet*, seminários de conscientização e quaisquer outros meios, com vistas à criação de uma cultura de Segurança da Informação no âmbito da ANA.

Parágrafo único. Cabe ao Gestor de SIC providenciar a divulgação interna da POSIC e das normas dela decorrentes, inclusive com publicação na *intranet* da ANA, e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados ao SIC.

CAPÍTULO IX
ATUALIZAÇÃO E VALIDADE

Art. 81. A SIC, tanto em meio digital quanto físico, deve ser continuamente monitorada e aprimorada, sendo periodicamente revisada e atualizada para assegurar a melhoria contínua da qualidade dos processos internos.

Parágrafo único. A POSIC deverá ser revisada sempre que se fizer necessário, em função de alterações na legislação pertinente ou nas diretrizes políticas do Governo Federal, ou ainda conforme os seguintes critérios:

I – nível de aprovação: pelo Comitê de Segurança da Informação e Comunicação (CSIC), representado pela Câmara de Governança Digital e Segurança da Informação e Comunicações (CGDI); e

II – periodicidade de revisão: sempre que aplicável, não podendo exceder o prazo de três anos.

ANEXO II
TERMO DE SIGILO E RESPONSABILIDADE

Nome do Colaborador:

Matrícula:

Cargo/Função:

Cláusula Primeira – Declaro ter conhecimento da Política de Segurança da Informação e Comunicações (POSIC) adotada pela ANA para utilização dos bens e recursos de informação, e comprometo-me ao seu fiel cumprimento e observância das normas a ela inerentes, em toda a sua abrangência.

Cláusula Segunda– Reconheço que todos os sistemas existentes na ANA, bem como todas as informações registradas em suas bases de dados, são de propriedade ou de direito de uso exclusivos da ANA, sendo vedada a sua cópia ou distribuição sem autorização prévia e formal.

Cláusula Terceira – Comprometo-me a manter sigilo absoluto sobre os sistemas e informações a mim confiados a que venha a ter conhecimento em função da execução de atividades desenvolvidas por mim para atendimento dos objetivos da ANA.

Cláusula Quarta – Estou ciente de que os *softwares* fornecidos pela ANA devem ser utilizados apenas nos equipamentos da ANA, salvo nas hipóteses previstas em Norma Complementar à POSIC. Ademais, não me é permitido instalar qualquer *software* de terceiros que não tenha sido prévia e formalmente autorizado pela equipe de Segurança da Informação.

Cláusula Quinta – Autorizo a ANA, em caráter irretratável e irrevogável, a ter acesso irrestrito a todas as correspondências enviadas e recebidas nos endereços eletrônicos disponibilizados pela Autarquia. Estou ciente e concordo que a utilização do correio eletrônico deve ocorrer em consonância com o disposto na POSIC e em suas Normas Complementares.

Cláusula Sexta – Estou ciente e concordo que a utilização da *internet* deve ocorrer em consonância com o disposto na POSIC.

Cláusula Sétima – Estou ciente de que a ANA pode monitorar o uso, por parte do colaborador, das informações e dos recursos de TI da ANA, conforme previsto na POSIC e nas suas Normas Complementares, sem prejuízo das ações disciplinares que possam ser tomadas.

Cláusula Oitava – Comprometo-me a manter as informações e recursos de TI a mim confiados protegidos de acessos indevidos, procurando cumprir as políticas e orientações de uso elencados na POSIC.

Cláusula Nona – Estou ciente de que as senhas de acesso aos sistemas e a ambientes físicos têm caráter confidencial, pessoal e intransferível, sendo minha responsabilidade zelar pelo seu sigilo.

Cláusula Décima – Declaro que tenho o conhecimento de que todas as minhas ações nos sistemas da ANA podem ser registradas e posteriormente averiguadas por essa Autarquia, sem prejuízo das ações disciplinares que possam ser tomadas.

Cláusula Décima Primeira – Declaro, estar ciente da obrigação de preservar os recursos a mim confiados e que o descumprimento dos itens constantes desta declaração e das normas de segurança e comunicação da POSIC serão considerados atos de negligência.

_____
Assinatura do Agente público/Colaborador
(assinado eletronicamente)
(NOME EM MAIÚSCULAS)

Documento assinado eletronicamente por **Ana Carolina Argolo Nascimento de Castro**, **Diretora**, em 04/07/2025, às 17:24, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ana.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0063545** e o código CRC **1D1008D5**.

Referência: Processo nº 02501.003137/2024-86 SEI nº 0063545