Boletim de Serviço Eletrônico em 29/12/2021

Enap Escola Nacional de Administração Pública

RESOLUÇÃO Nº 27

Institui a nova Política de Segurança da Informação (POSIN) no âmbito da Fundação Escola Nacional de Administração Pública (Enap).

O CONSELHO DIRETOR DA FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP, no uso das atribuições que lhe confere o Estatuto aprovado pelo Decreto n° 10.369, de 22 de maio de 2020, e tendo em visto o disposto na Lei nº 12.527, de 18 de novembro de 2011, na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 9.637, de 26 de dezembro de 2018, no Decreto nº 10.222, de 5 de fevereiro de 2020, no Decreto nº 10.748, de 16 de julho de 2021, na Portaria Enap nº 556, de 19 de setembro de 2019, nas normas do Gabinete de Segurança Institucional da Presidência da República que dispõem sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, e conforme a deliberação ocorrida na 44ª reunião ordinária realizada em 20 de dezembro de 2021, e o constante dos autos do processo n° 04600.002238/2021-02, resolve:

Art. 1º Estabelecer a Política de Segurança da Informação (POSIN) no âmbito da Fundação Escola Nacional de Administração Pública (Enap), nos termos do Anexo a esta Resolução.

Art. 2º Fica revogada a Resolução Enap nº 12, de 31 de outubro de 2014.

Art. 3º Esta Resolução entrará em vigor em 4 de janeiro de 2022.

BRUNA SILVA DOS SANTOS
Presidente Substituta

ANEXO

Política de Segurança da Informação da Fundação Escola Nacional de Administração Pública (POSIN/Enap)

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação da Fundação Escola Nacional de Administração Pública (POSIN/Enap) estabelece diretrizes, orientações e define a estrutura de gestão da segurança e controle dos ativos de informação, objetivando garantir os princípios de segurança das

informações produzidas ou custodiadas pela Enap, abrangendo aspectos físicos, tecnológicos e humanos da organização.

§ 1º A POSIN observa os princípios, objetivos e diretrizes estabelecidos bem como as disposições constitucionais, legais e regimentais vigentes.

§ 2º A POSIN trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito da Enap, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e descarte - visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

§ 3º Normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinados à proteção dos ativos de informação e à disciplina de sua utilização, emanados no âmbito da Enap, devem ser observados em conjunto com esta Política.

Art. 2º A estrutura da Segurança da Informação da Enap é integrada por três instrumentos normativos, de níveis hierárquicos distintos:

I - política de segurança da informação: documento obrigatório que define a estrutura, as diretrizes e as obrigações referentes à segurança da informação que devem ser seguidas;

II - normas internas de segurança da informação: documentos que identificam as regras básicas de como devem ser implementados os controles definidos pela POSIN; e

III - procedimentos de segurança da informação: documentos que instrumentalizam as normas internas, permitindo a direta aplicação nas atividades da Enap.

CAPÍTULO II
DA FINALIDADE

Art. 3º A POSIN visa estabelecer e preservar os ativos de informação, tangíveis e intangíveis, quanto ao sigilo, integridade, disponibilidade e autenticidade, e tem os seguintes objetivos específicos:

I - definir as diretrizes para o tratamento que deve ser dado às informações produzidas, processadas, transmitidas e armazenadas no ambiente físico ou de tecnologia da informação da Enap;

II - fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação dentro da Enap;

III - possibilitar a implantação de iniciativas relativos à segurança da informação;

IV - possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo para a minimização dos riscos associados; e

V - fortalecer a cultura da segurança da informação na Enap.

Art. 4º A POSIN, demais normas internas e procedimentos complementares têm abrangência universal, e devem ser cumpridas por todos os servidores, colaboradores, estagiários, consultores externos e prestadores de serviço que exerçam atividades no âmbito da Enap ou quem quer que tenha acesso a dados ou informações no ambiente da Enap.

Art. 5º A POSIN, as normas internas e os procedimentos de segurança da informação devem ser divulgados a todos os usuários da Enap, devendo estar disponível em local público de maneira que seu conteúdo possa ser consultado a qualquer momento, por qualquer usuário, em caráter de transparência pública.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para fins desta resolução entende-se por:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II - ativo: qualquer coisa que tenha valor para a organização;

III - ativos da informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas e redes de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

V - comitê de governança digital: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

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

VII - conscientização: atividade que tem por finalidade orientar sobre o que é segurança da informação levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade;

VIII - desastre: evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

IX - 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;

X - equipe de prevenção, tratamento e resposta a Incidentes cibernéticos: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

XI - firewall: recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um a conjunto de redes, ou a partir dela;

XII - gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem;

XIII - gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

XIV - gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica,

segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, às tecnologias da informação e comunicação;

XV - gestor de segurança da informação: pessoa responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

XVI - incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

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

XVIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIX - plano de continuidade de negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XX - plano de gerenciamento de incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XXI - POSIN: acrônimo de política de segurança da informação;

XXII - plano de tratamento dos riscos: processo e implementação de ações de segurança da informação para evitar, reduzir, reter ou transferir um risco;

XXIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XXIV - recurso: é um meio de qualquer natureza (humano, físico, tecnológico, financeiro, de imagem de mercado, de credibilidade, entre outros) que permite alcançar aquilo a que se propõe;

XXV - risco (conceito geral): possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade;

XXVI - riscos (de segurança da informação): potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

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

XXVIII - 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;

XXIX - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XXX - tratamento de incidentes: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXI - usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade;

XXXII - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 7º A segurança da informação está orientada pelos princípios da confidencialidade, da disponibilidade, da integridade e da autenticidade.

Art. 8º A POSIN/Enap está orientada pelos seguintes princípios:

I - responsabilidade: preservação da integridade e tratamento adequado da informação.

II - clareza: as regras que se fundam nesta POSIN devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão;

III - publicidade: transparência às informações, respeitando a privacidade do cidadão;

IV - auditabilidade: todos os eventos significativos dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;

V - resiliência: os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VI - substituição da segurança em situações de emergência: controles de segurança devem ser desconsiderados somente de formas pré determinadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em situações de emergência.

CAPÍTULO V
DAS COMPETÊNCIAS

Art. 9º A estrutura para a gestão de segurança da informação da Enap deve ser composta pelo:

I - gestor de segurança da informação;

II - comitê de governança digital;

III - equipe de prevenção, tratamento e resposta a incidentes cibernéticos;

IV - proprietário das informações;

V - usuário das informações.

Gestor de Segurança da Informação

Art. 10. O gestor de segurança da informação será designado pelo Comitê de Governança Digital da Enap - CGD/Enap, nos termos do art. 2º, inciso III, alínea "a" da Portaria Enap nº 556, de 2019, dentre os servidores públicos civis ocupantes de cargo efetivo e militares de carreira do órgão ou entidade, com formação ou capacitação técnica compatível às suas atribuições.

Art. 11. O Gestor de Segurança da Informação da Enap é o responsável por coordenar a implantação e manutenção da infraestrutura necessária à Equipe de Prevenção, Tratamento e Resposta a

Incidentes Cibernéticos (ETIR) e por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe, bem como prover a infraestrutura necessária.

Comitê de Governança Digital

Art. 12. O Comitê de Governança Digital da Enap (CGD/Enap), de caráter permanente, natureza deliberativa e tipo estratégico, possui finalidade e competências definidas pela Portaria Enap nº 556, de 19 de setembro de 2019.

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Art. 13. A ETIR é responsável pela tomada das decisões sobre o tratamento dos incidentes e sobre as medidas técnicas a serem adotadas na recuperação dos danos e na prevenção contra novos incidentes, podendo, durante um incidente de segurança da informação, se tal se justificar, tomar as decisões sobre as medidas de tratamento, recuperação e prevenção, atuando conforme previsto em seu ato de instituição.

Do Proprietário das Informações

Art. 14. O proprietário das informações, no contexto desta POSIN, é responsável pela autorização do acesso às informações, considerando as políticas vigentes dentro da Enap, tendo amplo domínio sobre as informações geradas em sua área de negócio e atuação, identificando-as e categorizando-as conforme critérios definidos por esta política.

Do Usuário das Informações

Art. 15. Usuário das informações é qualquer indivíduo com acesso às informações da Enap, seja servidor ou equiparado, empregado ou prestador de serviços, habilitado pela administração para acessar os ativos de informação, e cuja responsabilidade é cumprir com as regras de segurança da informação determinadas por esta POSIN.

CAPÍTULO VI
DAS DIRETRIZES GERAIS

Art. 16. A Segurança da Informação deve ser responsabilidade de todos, baseada em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso dos ativos de informação.

Art. 17. Os dirigentes das unidades e demais chefias da Enap assumem o compromisso de atuarem junto ao CGD/Enap, naquilo que por ventura sejam solicitados, e de desenvolverem suas atividades de forma colaborativa em estrita observância às orientações determinadas pelo Comitê, naquilo que tange à segurança da informação, objetivando minimizar as vulnerabilidades e ameaças que possam comprometer o negócio da instituição.

Art. 18. A utilização dos ativos de informação deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Do Tratamento da Informação

Art. 19. Toda informação criada, adquirida ou custodiada pelos servidores, colaboradores, estagiários, consultores externos e prestadores de serviço que exerçam atividades no âmbito da Enap ou quem quer que tenha acesso a dados ou informações no ambiente da instituição, no exercício de suas atividades, é considerada um bem e deve ser protegida de acordo com as regulamentações de segurança existentes com o objetivo de minimizar riscos às atividades e serviços prestados pela Enap, preservando sua imagem.

Art. 20. Quaisquer informações produzidas ou custodiadas pela Enap deverão atender aos critérios objetivos estabelecidos nesta POSIN com vistas ao prévio conhecimento dos usuários quanto aos direitos e obrigações.

Da Segurança Física e do Ambiente

Art. 21. A Enap, representada pela ETIR e com aprovação do CGD, deverá adotar medidas de segurança em seu parque tecnológico, de acessos aos ativos de informação sensíveis (dados) ou não-sensíveis (hardware), pessoais ou institucionais, visando a proteção física dos equipamentos, dos estabelecimentos, das áreas e do ambiente operacional, na tentativa de dissuadir, impedir, detectar, defender, atrasar e bloquear os riscos decorrentes de ações criminosas, operacionais e naturais.

Da Gestão de Incidentes em Segurança da Informação

Art. 22. Procedimentos formais para prevenção, auditoria, detecção, notificação e tratamento de incidentes de segurança deverão ser estabelecidos de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da Enap.

§ 1º Os incidentes de segurança deverão ser registrados e analisados periodicamente, servindo de subsídio para correções nos procedimentos e controles de segurança vigentes.

§ 2º O CGD/Enap e ETIR, deverão, dentro de suas competências, adotar medidas de tratamento de incidentes de segurança ocorridos na instituição.

Da Gestão de Ativos

Art. 23. O CGD/Enap deve instituir normas internas e procedimentos de segurança da informação que garantam a adequada gestão dos ativos de informação da Enap.

Art. 24. Ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos de informação da Enap, em níveis compatíveis ao seu grau de importância para a consecução das atividades e objetivos estratégicos do órgão.

Art. 25. Os ativos de informação devem ser associados a controles de segurança implementados, independentemente do meio em que se encontram, devendo ser protegidos contra divulgação, modificações, remoção ou destruição não autorizadas.

Art. 26. As pessoas que possuem acesso aos ativos de informação da organização devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.

Do Uso de Recursos Operacionais e de Comunicação

Art. 27. O uso de recursos operacionais da Enap por seus servidores, deve ser direcionado para a realização das atividades profissionais desempenhadas pelo órgão, nos limites dos princípios da ética, razoabilidade e legalidade, conforme as normas internas de segurança da informação existentes.

Dos Controles de Acesso

Art. 28. A Enap, representada pela ETIR e com aprovação do CGD, deve sistematizar a concessão e revogação de acesso como forma de evitar a quebra de segurança da informação.

Art. 29. O acesso físico às instalações da Enap deverá garantir a segurança dos seus servidores, usuários da Escola e a proteção dos seus ativos.

Da Gestão de Riscos

Art. 30. A Enap, representada pela ETIR e com aprovação do CGD, deverá estabelecer metodologia que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação, a monitoração e a avaliação periódica dos riscos de segurança da informação.

Art. 31. As unidades administrativas da Enap, com apoio do CGD/Enap, deverão implementar e executar as atividades de gestão dos riscos de segurança da informação associados aos ativos de informação sob sua responsabilidade.

Art. 32. Os riscos deverão ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades administrativas e dos ativos relacionados, gestores e fiscais de contrato, bem como os fornecedores e custodiantes, os responsáveis por manter os níveis apropriados de segurança da informação na entrega dos serviços.

Art. 33. As normas e procedimentos da Enap devem considerar controles para a troca de informações, tanto internamente quanto externamente, de forma a manter o nível adequado de segurança da informação.

Da Gestão de Continuidade

Art. 34. O CGD/Enap, em conformidade com todas as áreas responsáveis pelos ativos de informação, deverá instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços da Enap.

Art. 35. Com o objetivo de evitar situações de interrupção e manter em funcionamento os ativos e sistemas de informação da Enap, o CGD/Enap deverá manter um programa de gestão da continuidade de negócios.

Da Auditoria e Conformidade

Art. 36. Os mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de segurança da informação em vigor, deverão ser elaborados e implementados.

Parágrafo único. O CGD/Enap deverá instituir normas complementares internas a fim de manter registros como mecanismo de auditoria que possibilite o rastreamento, acompanhamento, controle e verificação de acesso aos serviços, sistemas de informação e rede interna, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Administração Pública Federal.

Art. 37. O cumprimento desta POSIN deverá ser avaliado constantemente, por meio de verificações de auditoria e conformidade realizadas pelo CGD/Enap.

Art. 38. Os controles de segurança da informação devem ser analisados criticamente e verificados em períodos regulares pelo CGD/Enap, garantindo proteção contra violação de requisitos de segurança da informação, objetivando a garantia de conformidade legal da Enap.

Da Classificação da Informação Conforme a ISO 27001

Art. 39. As informações custodiadas ou de propriedade da Enap devem ser classificadas levando-se em consideração seu valor, criticidade, sensibilidade e requisitos legais e receber o nível de proteção condizente com sua classificação, conforme normas e legislações específicas em vigor, especialmente a ISO 27001.

Art. 40. O CGD/Enap, juntamente com o gestor de segurança da informação, são os responsáveis por atribuir o nível de classificação das informações sob suas responsabilidades, conforme a ISO 27001.

Art. 41. A classificação deve ser respeitada durante todo o ciclo de vida da informação.

Da Sensibilização, Conscientização e Capacitação

Art. 42. A Enap desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos seus servidores sobre os cuidados e deveres relacionados à segurança da informação.

Art. 43. Os investimentos em capacitações em segurança da informação deverão ser estabelecidos de forma planejada e contemplados no Plano Anual de Capacitação da Enap - PACE, com base na priorização dos riscos a serem tratados, considerando a probabilidade, severidade e relevância destes.

CAPÍTULO VII
DAS BOAS PRÁTICAS COM A LGPD

Art. 44. Os usuários devem observar as disposições sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme estabelecido na Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais - LGPD.

Art. 45. Os usuários devem observar medidas de segurança, técnicas e administrativas referentes à proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme a LGPD e orientações dispostas no Programa de Governança em Privacidade da Enap, aprovado pela Resolução Enap nº 18, de 20 de julho de 2021.

CAPÍTULO VIII
DAS NORMAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

Art. 46. Esta POSIN deve ser observada complementarmente com as normas internas de segurança da informação que tratam especificamente da gestão de recursos relacionados aos ativos de informação.

Art. 47. Em nenhuma hipótese será permitido o descumprimento das normas internas de segurança da informação pela alegação de desconhecimento das mesmas.

CAPÍTULO IX
DAS PENALIDADES

Art. 48. O descumprimento das disposições constantes nesta POSIN e nas normas internas de segurança da informação, caracteriza infração funcional a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 49. O usuário que fizer uso de forma indevida ou não autorizada dos ativos de informação, bem como agir em desacordo com os termos desta política, ficará sujeito à aplicação das penalidades previstas na Lei nº 8.112, de 11 de dezembro de 1990 e na legislação pertinente, garantidos a ampla defesa e o contraditório.

CAPÍTULO X
DAS ATUALIZAÇÕES

Art. 50. A periodicidade para a revisão da POSIN e das normas internas de segurança da informação não deve exceder ao período de 02 (dois) anos, podendo ser revisada, sempre que necessário, por deliberação do CGD/Enap.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 51. Os usuários da Enap devem observar as diretrizes e responsabilidades estabelecidas nesta POSIN, nas normas e procedimentos complementares e as melhores práticas de segurança da informação recomendadas por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões e normas de segurança.

Art. 52. Qualquer ocorrência de incidentes de segurança da informação devem ser comunicados pelos usuários aos gestores responsáveis pelos ativos da informação.

Art. 53. Todos os usuários da Enap são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como crachá, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

Art. 54. Os contratos, convênios, acordos e instrumentos congêneres devem observar, no que couber, as seguintes diretrizes:

I - conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIN;

II - prever a obrigação da outra parte de divulgar esta POSIN e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na Enap;

III - nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 55. Ações que violem esta POSIN ou que quebrem os controles de segurança da informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor.

Documento assinado eletronicamente por **Bruna Silva dos Santos**, **Presidente(a) Substituto(a)**, em 28/12/2021, às 19:17, conforme horário oficial de Brasília e Resolução nº 9, de 04 de agosto de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.enap.gov.br/autenticidade, informando o código verificador **0534859** e o código CRC **74B50481**.

Referência: Processo nº 04600.002238/2021-02 SEI nº 0534859