DIÁRIO OFICIAL DA UNIÃO

Publicado em: 13/03/2025 | Edição: 49 | Seção: 1 | Página: 3

Órgão: Presidência da República/Advocacia-Geral da União

PORTARIA NORMATIVA AGU Nº 166, DE 12 DE MARÇO DE 2025

Institui a Política de Segurança da Informação da Advocacia-Geral da União - POSIN-AGU.

O ADVOGADO-GERAL DA UNIÃO, no uso das atribuições que lhe confere o art. 4º, caput, incisos I, XIII e XVIII, da Lei Complementar nº 73, de 10 de fevereiro de 1993, e tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, e o que consta no Processo Administrativo nº 00400.002104/2023-41, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Segurança da Informação da Advocacia-Geral da União - POSIN-AGU, com a finalidade de estabelecer:

I - as regras gerais sobre a gestão da segurança da informação, de modo a garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações produzidas ou custodiadas pela Advocacia-Geral da União, independentemente da forma ou meio em que sejam apresentadas ou compartilhadas; e

II - o modelo de governança de segurança da informação que orientará a execução da política no âmbito da Advocacia-Geral da União.

Parágrafo único. O disposto nesta Portaria Normativa se aplica aos:

I - órgãos previstos no art. 2º do Anexo I ao Decreto nº 11.328, de 1º de janeiro de 2023; e

II - usuários de informação da Advocacia-Geral da União.

Art. 2º A segurança da informação, no âmbito da Advocacia-Geral da União, abrange:

I - a segurança cibernética;

II - a segurança física dos equipamentos de tecnologia da informação e comunicação; e

III - a segurança física e a proteção de dados.

Art. 3º São objetivos da POSIN-AGU:

I - estabelecer os princípios e as diretrizes para a proteção dos ativos de informação e do conhecimento gerado ou recebido pela Advocacia-Geral da União;

II - proteger os dados e as informações de forma a garantir a continuidade do negócio e o aumento do retorno sobre os investimentos em tecnologia da informação e comunicação;

III - fixar os princípios, as diretrizes e as regras destinados à gestão eficiente dos riscos e à efetividade das ações previstas nesta Portaria Normativa; e

IV - definir as competências e responsabilidades quanto à segurança da informação.

Art. 4º Para os efeitos desta Portaria Normativa e de suas normas complementares, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Art. 5º As ações de segurança da informação de que trata esta Portaria Normativa serão orientadas pelos seguintes princípios e diretrizes:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações;

II - continuidade dos processos e serviços essenciais ao funcionamento da Advocacia-Geral da União;

III - prevenção da ocorrência de incidentes;

IV - economicidade da proteção dos ativos de informação;

V - proporcionalidade em relação aos riscos existentes e à magnitude dos danos potenciais, considerando o ambiente, o valor e a criticidade da informação;

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

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

VIII - responsabilidade do usuário da informação pelos atos que comprometam a segurança dos ativos de informação;

IX - alinhamento estratégico da Política de Segurança da Informação com:

a) o Plano Estratégico da Advocacia-Geral da União;

b) as normas específicas de segurança da informação da administração pública federal; e

c) as melhores práticas de segurança da informação;

X - respeito às especificidades e à autonomia das unidades da Advocacia-Geral da União;

XI - conformidade das normas e das ações de segurança da informação com a legislação e regulamentação aplicáveis; e

XII - educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º Qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na Advocacia-Geral da União compõe o seu rol de ativos de informação e deverá ser protegida.

Parágrafo único. As informações mencionadas no caput que tramitem pelo ambiente computacional da Advocacia-Geral da União são passíveis de monitoramento e auditoria pela Secretaria de Controle Interno da Advocacia-Geral da União.

Art. 7º Os recursos tecnológicos, as instalações de infraestrutura, os sistemas de informação e as aplicações que sejam de propriedade ou posse da Advocacia-Geral da União deverão ser protegidos contra indisponibilidade, acessos indevidos, falhas, perdas, danos, furtos, roubos e interrupções não programadas.

Art. 8º As pessoas e os sistemas de informação deverão possuir o menor privilégio e o mínimo acesso aos recursos necessários para realizar as suas atividades.

Art. 9º É condição para o acesso aos recursos de tecnologia da informação da Advocacia-Geral da União:

I - a ciência aos termos desta política; e

II - a assinatura, preferencialmente eletrônica, de termo de responsabilidade que indique:

a) os compromissos assumidos em decorrência deste acesso; e

b) as responsabilidades pela inobservância dos compromissos assumidos.

Art. 10. A POSIN-AGU, suas atualizações e as normas complementares de segurança da informação deverão ser divulgadas amplamente a todos os usuários de informação, a fim de promover seu conhecimento, sua observância e a formação da cultura de segurança da informação no âmbito da Advocacia-Geral da União.

§ 1º Os usuários de informação deverão ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º deverão ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 11. O investimento necessário em medidas de segurança da informação deverá ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos.

Art. 12. Todos os contratos de prestação de serviços firmados pela Advocacia-Geral da União conterão cláusula específica sobre a obrigatoriedade de atendimento a esta POSIN-AGU e suas normas complementares.

CAPÍTULO II

DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Seção I

Dos processos de gestão de segurança da informação

Art. 13. A gestão da segurança da informação é constituída, no mínimo, pelos seguintes processos:

I - tratamento da informação;

II - segurança física e do ambiente;

III - gestão de incidentes em segurança da informação;

IV - gestão de ativos;

V - gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI - controles de acesso;

VII - gestão de riscos;

VIII - gestão de continuidade; e

IX - conformidade das práticas de segurança da informação

Seção II

Do tratamento da informação

Art. 14. As informações produzidas, recebidas, utilizadas, acessadas, reproduzidas, transportadas, transmitidas, distribuídas, arquivadas, armazenadas e descartadas no âmbito da Advocacia-Geral da União deverão ser avaliadas e, se for o caso, classificadas e protegidas adequadamente, de acordo com a Portaria AGU nº 529, de 23 de agosto de 2016.

Art. 15. A decisão de classificação, desclassificação, reclassificação ou redução do prazo de sigilo de informação observará os procedimentos previstos nos arts. 31 e 32 do Decreto nº 7.724, de 16 de maio de 2012.

Art. 16. O acesso, a divulgação e o tratamento de informação classificada em qualquer grau de sigilo ficarão restritos às pessoas com necessidade de conhecê-la, desde que credenciadas na forma estabelecida no Decreto nº 7.845, de 14 de novembro de 2012, e nas normas complementares do Gabinete de Segurança Institucional da Presidência da República.

Art. 17. O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme o Anexo I ao Decreto nº 7.845, de 14 de novembro de 2012.

Parágrafo único. O TCMS previsto no caput é o documento pelo qual a pessoa se obriga a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei, desde que atenda à necessidade de conhecer a informação solicitada.

Seção III

Da segurança física e do ambiente

Art. 18. As instalações físicas que armazenam e processam as informações classificadas deverão ser mantidas em áreas seguras, protegidas por perímetros e barreiras de segurança, visando à integridade dos bancos de dados e à prevenção de danos e interferências que possam causar perda, subtração ou

comprometimento de dados ou informações.

Art. 19. A Secretaria de Governança e Gestão Estratégica deverá implementar mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências, em resposta aos riscos identificados.

Seção IV

Da gestão de incidentes de segurança da informação

Art. 20. A gestão de incidentes de segurança da informação envolve os procedimentos para o tratamento e a resposta aos incidentes de segurança da informação.

Art. 21. Os incidentes de segurança de informação serão classificados como:

I - cibernéticos; e

II - não cibernéticos.

§ 1º Os incidentes cibernéticos que apresentarem indícios de prática criminosa deverão ser:

I - registrados, analisados e tratados por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas; e

II - comunicados às autoridades competentes, nos termos do que dispuser o Plano de Resposta a Incidentes de Segurança da informação da Advocacia-Geral da União.

§ 2º O plano de que trata o inciso II do § 1º deverá ser instituído por ato do Secretário de Governança e Gestão Estratégica.

§ 3º Os indícios a que se refere o § 1º do caput deverão ser preservados.

Seção V

Da gestão de ativos

Art. 22. A gestão de ativos deverá contemplar, no mínimo, a identificação, o mapeamento, o inventário e a classificação de informações consideradas relevantes para a concretização dos objetivos estratégicos e a execução dos processos de trabalho da Advocacia-Geral da União.

Art. 23. O mapeamento de ativos de informação deverá considerar, preliminarmente:

I - os objetivos estratégicos;

II - os processos de trabalho internos;

III - os requisitos legais; e

IV - a estrutura da Advocacia-Geral da União.

Art. 24. O inventário será feito pelo registro de ativos de informação resultante do processo de mapeamento que deverá conter:

I - os responsáveis, proprietários e custodiantes, de cada ativo de informação;

II - as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;

III - os contêineres de cada ativo de informação; e

IV - as interfaces de cada ativo de informação e as interdependências entre eles.

Art. 25. Os ativos de informação deverão ser classificados segundo critérios que orientem a implantação de mecanismos para assegurar a privacidade e a proteção dos dados conforme o seu valor, sensibilidade e criticidade.

Art. 26. Cabe ao agente responsável pela gestão dos ativos de informação:

I - identificar e classificar os ativos de informação por nível de criticidade;

II - identificar:

a) potenciais ameaças aos ativos de informação; e

b) vulnerabilidades dos ativos de informação;

III - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

IV - autorizar a atualização do relatório mencionado no inciso III do caput; e

V - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

Seção VI

Da gestão de operações e comunicações

Art. 27. A Secretaria de Governança e Gestão Estratégica deverá:

I - implementar medidas adequadas relacionadas à segurança da informação, para a disponibilização dos serviços, sistemas e da infraestrutura que apoiam, de forma a atender aos requisitos de qualidade e às necessidades da Advocacia-Geral da União; e

II - garantir a segregação lógica dos ambientes computacionais de desenvolvimento, homologação e produção, a fim de manter a segurança da informação e a privacidade de dados da Advocacia-Geral da União.

Art. 28. O uso da internet pela rede da Advocacia-Geral da União deverá ser empregado para fins institucionais.

Parágrafo único. Os usuários de informação terão seus acessos autorizados conforme o disposto nesta POSIN-AGU e suas normas complementares.

Art. 29. O correio eletrônico da Advocacia-Geral da União é de uso institucional e deverá ser empregado por seus usuários para fins institucionais, de acordo com esta POSIN-AGU.

Seção VII

Do controle de acesso

Art. 30. O acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações deverão ser limitados ao cumprimento das atividades institucionais de cada usuário.

Art. 31. A identificação do usuário, qualquer que seja o meio e a forma, deverá ser pessoal e intransferível, permitindo o seu reconhecimento de forma clara e irrefutável.

Art. 32. O usuário é responsável pela segurança dos ativos, dos processos que estejam sob sua responsabilidade e por todos os atos executados com sua identificação, salvo se comprovado que o fato ocorreu sem o seu conhecimento ou consentimento.

Art. 33. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais deverão ser adequados imediatamente pelo Departamento de Tecnologia da Informação, devendo ser cancelados em caso de desligamento da Advocacia-Geral da União.

Art. 34. É vedada a utilização de acesso remoto, salvo se for realizado com a utilização de recursos próprios da Advocacia-Geral da União, homologados pelo Departamento de Tecnologia da Informação.

Art. 35. Todos os acessos aos sistemas de informação deverão ser registrados para garantir a segurança das informações.

Seção VIII

Da gestão de riscos de segurança da informação

Art. 36. O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis.

Art. 37. As vulnerabilidades deverão ser gerenciadas para proteger a rede corporativa, por meio da aplicação sistemática de ações de identificação, classificação, tratamento e monitoramento de vulnerabilidades, compreendendo:

I - a obtenção de informações para identificar vulnerabilidades em tempo hábil;

II - a avaliação de exposição às vulnerabilidades identificadas;

III - a adoção de medidas apropriadas para lidar com os riscos; e

IV - o monitoramento contínuo dos ativos de informação.

Art. 38. Deverão ser estabelecidos critérios de identificação, avaliação e implementação das medidas de proteção necessárias à mitigação ou à eliminação das vulnerabilidades e riscos à segurança da informação.

Art. 39. A gestão de riscos de segurança da informação deverá ser operacionalizada por meio de plano e metodologia específicos, de forma sistemática e contínua, incluindo todos os ativos de informação da Advocacia-Geral da União.

§ 1º A gestão de riscos de segurança da informação deverá manter alinhamento com a Política de Gestão de Riscos da Advocacia-Geral da União, conforme dispuser portaria normativa específica do Advogado-Geral da União.

§ 2º O plano e a metodologia mencionados no caput serão instituídos por ato do Secretário de Governança e Gestão Estratégica.

Seção IX

Da gestão de continuidade do negócio

Art. 40. A implementação do processo de gestão de continuidade de negócios em segurança da informação tem por objetivo:

I - minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da Advocacia-Geral da União nessa área; e

II - recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art. 41. O processo de gestão de continuidade de negócios em segurança da informação deverá ser baseado:

I - nas estratégias de continuidade para as atividades críticas;

II - na avaliação dos riscos levantados no processo de gestão de riscos; e

III - em diretrizes institucionais sobre gestão de continuidade de negócio.

Parágrafo único. As diretrizes institucionais de que trata o inciso III do caput serão editadas pelo CSI-AGU, nos termos do que dispõe o art. 48, caput, inciso III, alínea "a", e contemplarão, no mínimo, os seguintes aspectos:

I - consonância com a missão da Advocacia-Geral da União, considerando sua estrutura, natureza e complexidade, a fim de que a política reflita a cultura e o ambiente institucional;

II - compromissos claros com relação às obrigações legais e regulamentares e à melhoria contínua do processo de gestão de continuidade de negócios em segurança da informação;

III - definição da abrangência e dos limites do processo de gestão de continuidade de negócios em segurança da informação;

IV - identificação de quaisquer autoridades da Advocacia-Geral da União e delegações necessárias, incluindo os responsáveis por continuidade de negócios na Instituição;

V - critérios para o tipo e a escala dos incidentes a serem tratados;

VI - referências às normas, aos regulamentos ou às políticas que o processo considere ou cumpra; e

VII - compromisso de realizar e manter a continuidade do negócio da Advocacia-Geral da União.

Art. 42. O processo de gestão de continuidade de negócios em segurança da informação deverá ser composto por Planos de Continuidade de Negócios em Segurança da Informação, cuja finalidade é definir como:

I - serão realizadas a gestão dos incidentes em caso de desastres ou de outras interrupções das operações de negócios; e

II - deverão ser recuperadas as atividades nos prazos estabelecidos.

Parágrafo único. Os planos a que se refere o caput serão editados pelo Secretário de Governança e Gestão Estratégica.

Seção X

Da conformidade das práticas de segurança da informação

Art. 43. A Secretaria de Governança e Gestão Estratégica implementará um programa de verificação de conformidade das práticas de segurança da informação na Advocacia-Geral da União com o disposto nesta POSIN-AGU.

Art. 44. A verificação de conformidade das práticas de segurança da informação deverá ser realizada sempre que necessária, não excedendo o período máximo de dois anos.

Parágrafo único. A verificação da conformidade de que trata o caput será realizada:

I - de forma planejada, mediante calendário de ações aprovado pelo CSI-AGU, a partir de proposta elaborada pela Secretaria de Governança e Gestão Estratégica; e

II - nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a Advocacia-Geral da União.

Art. 45. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 46. Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade e, com base neste, o Gestor de Segurança da Informação tomará medidas cabíveis.

CAPÍTULO III

DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

Seção I

Disposições gerais

Art. 47. A POSIN-AGU contará com a seguinte estrutura de governança:

I - Comitê de Segurança da Informação da Advocacia-geral da União - CSI-AGU;

II - Comissão Técnica de Governança Digital - CT-DIGITAL;

III - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-AGU;

IV - Gestor de Segurança da Informação; e

V - usuários de informação.

Seção II

Do Comitê de Segurança da Informação da Advocacia-Geral da União

Art. 48. Fica instituído, nos termos do que determina o art. 15, caput, inciso IV, do Decreto nº 9.637, de 26 de dezembro de 2018, o Comitê de Segurança da Informação da Advocacia-Geral da União - CSI-AGU, com as seguintes competências:

I - assessorar o Advogado-Geral da União nos temas de segurança da informação;

II - propor:

a) estratégias para as ações relacionadas à segurança da informação; e

b) alterações à POSIN-AGU e a outras políticas a ela correlatas;

III - editar, nos termos do que dispõe o art. 7º da Portaria Normativa AGU nº 141, de 19 de junho de 2024, atos normativos que disponham sobre:

a) normas complementares de segurança da informação; e

b) suas regras de organização e funcionamento;

IV - apreciar os processos relacionados ao descumprimento do termo de responsabilidade previsto no art. 9º e encaminhá-los às autoridades competentes, conforme o caso;

V - constituir grupos de trabalho para tratar de temas relacionados à segurança da informação;

VI - recepcionar os resultados dos trabalhos de auditoria interna ou externa sobre a gestão da segurança da informação, propondo ajustes aos processos internos quando necessário;

VII - coordenar as ações necessárias para o tratamento de crises cibernéticas e outras crises que afetem a segurança da informação;

VIII - avaliar as ações propostas pelo gestor de segurança da informação; e

IX - acompanhar, no âmbito da Advocacia-Geral da União, a execução do Programa de Privacidade e Segurança da Informação, de que trata a Portaria SGD/MGI nº 852, de 28 de março de 2023, e suas atualizações;

§ 1º As competências do CSI-AGU serão exercidas pelo Comitê de Governança da Advocacia-Geral da União - CG-AGU, conforme disposto no art. 6º, caput, inciso X, alínea "b", da Portaria Normativa AGU nº 165, de 12 de março de 2025.

§ 2º Para o exercício das competências previstas neste artigo, o Departamento de Tecnologia da Informação e a Ouvidoria integrarão o CG-AGU, com direito a voto.

§ 3º O titular da Secretaria de Controle Interno poderá participar das reuniões do CG-AGU, sem direito a voto.

Seção III

Da Comissão Técnica de Governança Digital

Art. 49. Aplica-se à Comissão Técnica de Governança Digital - CT-DIGITAL o disposto na Portaria Normativa AGU nº 165, de 12 de março de 2025.

Seção IV

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Art. 50. Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, com as seguintes competências:

I - implementar medidas e manter um processo de gestão de riscos de segurança da informação com vistas a minimizar possíveis impactos associados aos ativos de informação, reduzir as vulnerabilidades e evitar ameaças;

II - analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação;

III - recolher de forma ágil as provas após um incidente cibernético;

IV - executar uma análise crítica sobre os registros de falha para assegurar que elas foram satisfatoriamente resolvidas;

V - investigar as causas dos incidentes de segurança da informação;

VI - facilitar e coordenar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos;

VII - implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento dos ativos de tecnologia da informação;

VIII - indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes de segurança da informação;

IX - estabelecer, manter, revisar, no mínimo anualmente, e aperfeiçoar, quando necessário, o processo de gerenciamento de incidentes de segurança da informação;

X - monitorar as redes computacionais;

XI - detectar e analisar ataques e intrusões;

XII - tratar incidentes de segurança da informação;

XIII - identificar vulnerabilidades e artefatos maliciosos;

XIV - atuar na recuperação de sistemas de informação; e

XV - promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação e Comunicações.

Art. 51. A ETIR será composta:

I - pelo Gestor de Segurança da Informação, que a coordenará; e

II - por servidores, titulares e suplentes, dos seguintes órgãos:

a) Departamento de Tecnologia da Informação:

1. Coordenação de Segurança e Soluções;

2. Coordenação de Suporte e Infraestrutura; e

3. Coordenação de Desenvolvimento e Arquitetura de Dados; e

b) Coordenação de Tratamento de Dados Pessoais e Gestão do Conhecimento, do Departamento de Inteligência Jurídica e Inovação.

§ 1º Os servidores de que trata o inciso II, alíneas "a" e "b", do caput serão indicados pelos Diretores do Departamento de Tecnologia da Informação e do Departamento de Inteligência Jurídica e Inovação, respectivamente, e designados pelo Secretário de Governança e Gestão Estratégica.

§ 2º Os membros de outras áreas ou unidades poderão ser chamados pelo coordenador da ETIR para auxiliar no tratamento dos incidentes.

Seção V

Do Gestor de Segurança da Informação

Art. 52. Ato do Secretário-Geral de Consultoria designará o Gestor de Segurança da Informação da Advocacia-Geral da União.

§ 1º O Gestor de Segurança da Informação deverá ser servidor público efetivo ou empregado público com formação ou capacitação técnica compatível às suas atribuições estabelecidas por esta Portaria Normativa.

§ 2º O Gestor de Segurança da Informação exercerá suas atribuições sem prejuízo daquelas que já exerce.

Art. 53. São atribuições do Gestor de Segurança da Informação:

I - coordenar:

a) os processos de gestão de segurança da informação; e

b) a elaboração da POSIN-AGU e das normas complementares de segurança da informação, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República e as melhores práticas sobre o assunto;

II - incentivar a cultura de segurança da informação;

III - articular:

a) com a Assessoria Especial de Comunicação Social, a divulgação desta POSIN-AGU e das normas complementares de segurança da informação a todos os servidores, usuários e prestadores de serviços; e

b) com a Escola Superior da Advocacia-Geral da União Ministro Victor Nunes Leal, a realização de ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

V - propor ao CSI-AGU recursos necessários às ações de segurança da informação;

VI - coordenar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

VII - coordenar os trabalhos da ETIR;

VIII - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

IX - coordenar o processo de mapeamento de ativos de informação;

X - coordenar o planejamento e a implementação dos processos de segurança da informação e a melhoria contínua dos controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução;

XI - propor medidas preventivas à CT-DIGITAL; e

XII - manter contato com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação.

Seção VI

Dos usuários de informação

Art. 54. Para os fins desta Portaria Normativa, consideram-se usuários de informação os membros, servidores, prestadores de serviço, colaboradores, fornecedores, estagiários, consultores externos e quem, de alguma forma, execute atividades oficialmente para a Advocacia-Geral da União.

Art. 55. Os usuários de informação deverão conhecer, cumprir e fazer cumprir o disposto nesta Portaria Normativa e nas normas complementares de segurança da informação da Advocacia-Geral da União.

Parágrafo único. Os usuários de informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 56. Ficam vedados:

I - a utilização dos recursos de tecnologia da informação disponibilizados pela Advocacia-Geral da União para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente;

II - o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela Advocacia-Geral da União;

III - a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, fornecidos aos usuários; e

IV - a exploração de eventuais vulnerabilidades, as quais deverão ser comunicadas às instâncias superiores assim que identificadas.

Art. 57. A Escola Superior da Advocacia-Geral da União e o Departamento de Tecnologia da Informação deverão promover ações de treinamento e conscientização voltadas à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação deverão ser adequadas aos papéis e responsabilidades dos integrantes da Advocacia-Geral da União.

Art. 58. As denúncias de violação a esta POSIN-AGU deverão ser comunicadas ao Gestor de Segurança da Informação por meio do endereço de correio eletrônico abuse@agu.gov.br.

Art. 59. Os processos e os recursos de segurança da informação serão passíveis de auditoria pela Secretaria de Controle Interno da Advocacia-Geral da União, que avaliará se as implementações que assegurem a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação

estão em conformidade com a legislação em vigor.

Art. 60. A POSIN-AGU será revisada periodicamente, pelo menos a cada três anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 61. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação da Advocacia-Geral da União deverão ser submetidos ao CSI-AGU.

Art. 62. Fica revogada a Portaria nº 24, de 22 de janeiro de 2013.

Art. 63. Esta Portaria Normativa entra em vigor na data de sua publicação.

JORGE RODRIGO ARAÚJO MESSIAS