DIÁRIO OFICIAL DA UNIÃO

Publicado em: 27/09/2017 | Edição: 186 | Seção: 1 | Página: 64

Órgão: Ministério da Transparência, Fiscalização e Controladoria-Geral da União/SECRETARIA EXECUTIVA

PORTARIA Nº 2.042, DE 22 DE SETEMBRO DE 2017

Institui a Política de Segurança da Informaçãoe das Comunicações
Ministério da Transparênciae Controladoria-Geral da União.

O SECRETÁRIO-EXECUTIVO DO MINISTÉRIO DATRANSPARÊNCIA E CONTROLADORIA-G DA UNIÃO,Substituto, no uso da competência que lhe foi atribuída pelo art. 23do Anexo ao Decr 8.910, de 22 de novembro de 2016, e tendoem vista o disposto no Decreto nº 3.505, de 15 de jur 2000, noDecreto nº 7.845, de 14 de novembro de 2012, na Instrução NormativaGSI/PR nº 1, de 13 de de 2008, e na Instrução NormativaGSI/PR nº 2, de 5 de fevereiro de 2013, resolve:

Art. 1º Instituir a Política de Segurança da Informação e das Comunicações- POSI apresentar as diretrizes de segurança adotadaspelo Ministério da Transparência e Controladoria-Ge União - CGU.

Art. 2º Norteiam esta POSIC os princípios da disponibilidade,da integridad confidencialidade, da autenticidade, alémdos princípios que regem a Administração Pública.

CAPÍTULO I

CONSIDERAÇÕES INICIAIS

Seção I

Da Abrangência

Art. 3º As diretrizes da POSIC da CGU, constantes nesta Portariae em sua regulamer devem ser observadas por todos os agen tespúblicos, colaboradores e, no que couber, pelos visitant tenhamacesso às instalações da CGU, em todas as suas unidades, e aplicadas atodos os sistem informação e processos corporativos do órgão.

Seção II

Dos Princípios

Art. 4º A Segurança da Informação e das Comunicações daCGU deverá observar os seg princípios:

I - ser parte integrante dos processos organizacionais;

II - garantir a disponibilidade, integridade, confidencialidadee autenticidade das informaçõ

III - garantir a transparência das informações de acesso irrestrito,e a proteção ade daquelas com restrição de acesso;

IV - ser dinâmica e capaz de reagir a mudanças;

V - estar integrada às oportunidades e à inovação;

VI - ser adaptável à realidade orçamentária em vigor;

VII - prezar pelas conformidades legal e normativa dos procedimentosrelacionados à segu da informação e das comunicações;

VIII- orientar a tomada de decisões institucionais que visemà efetividade das açõ segurança da informação e das comunicações;e

IX - estar integrada aos processos de planejamento estratégico,tático e operacional, à ge à cultura organizacional daCGU.

Seção III

Dos Conceitos e Definições

Art. 5º Para os efeitos desta Portaria são estabelecidos osseguintes conceitos e definições

I - Agente Público: todo aquele que exerce, ainda que transitoriamente,com ou remuneração, por eleição, nomeação, designação,contratação ou qualquer outra forma de investid vínculo,mandato, cargo, emprego ou função na CGU;

II - Ativos de informação: os meios de armazenamento, transmissãoe processamer informação; os equipamentos necessáriosa isso; os sistemas utilizados para tal; os locais on encontramesses meios, e também os recursos humanos que a eles têm acesso;

III - Autenticidade: propriedade de que a informação foiproduzida, expedida, modifica destruída por uma determinadapessoa física, ou por um determinado sistema, órgão ou entidade;

IV - Colaboradores: fornecedores, estagiários e terceirizadosalocados no órgão;

V - Confidencialidade: propriedade de que a informação nãoesteja disponível ou reve pessoa física, sistema, órgão ou entidadenão autorizado e credenciado;

VI - Continuidade de Negócios: capacidade que uma organizaçãotem de continuar a entre produtos ou serviços emníveis aceitáveis pré-definidos após um incidente de interrupção;

VII - Disponibilidade: propriedade de que a informação estejaacessível e utilizável sob der por uma pessoa física oudeterminado sistema, órgão ou entidade;

VIII - Dispositivos móveis: consiste em equipamentos portáteisdotados de capac computacional, e dispositivos removíveisde memória para armazenamento;

IX - Gestão de Riscos de Segurança da Informação e dasComunicações: conjunto de proc que permitem identificar e implementaras medidas de proteção necessárias para minimizar ouelimi riscos a que estão sujeitos os seus ativos de informação,e equilibrá-los com os custos operacio financeiros envolvidos;

X - Incidente de segurança: qualquer evento adverso, confirmadoou sob suspeita, relacior segurança dos ativos de informação;

XI- Informação: dados, processados ou não, que podem serutilizados para produ transmissão de conhecimento, contidos emqualquer meio, suporte ou formato;

XII - Integridade: propriedade de que a informação não foimodificada ou destruída de m não autorizada ou acidental; e

XIII - Tratamento da informação: recepção, produção, reprodução,utilização, acesso, trans transmissão, distribuição, armaze namento,eliminação e controle da informação, inclusive as sigilosas

CAPÍTULO II

GESTÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃOE DAS COMUNICAÇÕES

Seção I

Do Sistema de Gestão

Art. 6º O Sistema de Gestão de Segurança Corporativa daCGU - SISEG -, instituído Instrução Normativa nº 04, de 03 dejunho de 2014, é composto por:

I - Gestores de Segurança da Informação e das Comunicações,nomeados e com compet definidas na Instrução Normativanº 04, de 2014;

II - Comitê Permanente de Segurança Corporativa - COPESEG-, instituído pela Portaria r de 18 de abril de 2017, comcaráter permanente, para o qual devem convergir as informaçõesrelat implementação e ao cumprimento da POSIC;

III - Núcleo Técnico de Segurança Corporativa - NUTESEG-, instituído pela Portaria nº 9 2017, composto por servidoresdesignados pelo COPESEG;

IV - Equipe de Tratamento e Resposta a Incidentes de Rede- ETIR-CGU -, instituída NC04/IN04/SE/CGU/PR, de 20 deabril de 2016; e

V - Ocupantes de cargos em comissão do Grupo-Direção eAssessoramento Superiores - ou de Funções Comissionadas doPoder Executivo - FCPE -, de nível 4 ou superior, e equival eSuperintendentes das Controladorias Regionais da União nos Estados.

Art.7º Compete ao Gestor de Segurança da Informação edas Comunicações implemer ações desta POSIC no âmbito daCGU, observando-se o disposto no art. 18 da Instrução Normativa nº 2014.

Parágrafo único. A Diretoria de Pesquisas e InformaçõesEstratégicas (DIE) absorv responsabilidade de coordenar e acompanhara execução das ações de implementação desta POS quesejam designados servidores e estrutura própria.

Art. 8º Compete ao COPESEG centralizar as decisões normativasda POSIC.

Parágrafo único. Aplicam-se à Segurança da Informação edas Comunicações as compet do COPESEG estabelecidas paraa Política de Segurança Corporativa pela Portaria nº 948, de 2017,q cabíveis.

Art. 9º No âmbito desta Política, compete ao NUTESEGauxiliar o COPESEG na execução d competências e, notadamente:

I- averiguar o cumprimento da POSIC, das normas e dosprocedimentos, por meio de pes auditorias ou outros métodosque julgar adequados;

II - avaliar a eficácia dos procedimentos de segurança;

III - verificar periodicamente, observado o disposto no art.44 desta norma, a conformida POSIC com os requisitos legais,com as normas e diretrizes internas e com os requisitos té deSegurança da Informação e das Comunicações;

IV - avaliar a eficácia dos procedimentos de segurança e suaconformidade com os req legais, com as normas e diretrizesinternas e com os requisitos técnicos de segurança corporativa; e

V - assessorar o COPESEG e viabilizar a implementação desuas decisões.

Art. 10 Competem à ETIR-CGU o recebimento, a análise ea resposta às notificações atividades relacionadas a incidentes desegurança em redes de computadores.

Art. 11. No âmbito desta Política, compete aos dirigentes deque trata o art. 6º, V:

I - garantir o cumprimento da POSIC em sua unidade organizacional;

II- receber comunicação de incidente ou ameaça à Segurançada Informação Comunicações e levá-la ao conhecimentodas unidades competentes;

III - verificar continuamente a necessidade de melhoriasquanto à Segurança da Informa das Comunicações; e

IV - propor atividades de capacitação, de conscientização, dedivulgação e de disseminaç orientações previstas nesta POSIC.

CAPÍTULO III

DIRETRIZES

Seção I

Do Tratamento da Informação

Art. 12. Toda informação institucional no âmbito da CGU épatrimônio do Estado brasileiro ser gerida adequadamente como objetivo de garantir a sua disponibilidade, integr confidencialidadee autenticidade, independente do meio de armazenamento,processament transmissão que esteja sendo utilizado.

Parágrafo único. As salvaguardas de informação serão proporcionaisà sensibilidad criticidade.

Art. 13. O tratamento das informações pessoais deve ser feitocom respeito a intimidad privada, honra e imagem das pessoas,bem como às liberdades e garantias individuais.

Art. 14. Cabe ao COPESEG propor diretrizes de Segurançada Informação e das Comunic para a instituição do processo detratamento da informação em todo o seu ciclo de vida, conformeir do art. 4º da Lei nº 12.527, de 18 de novembro de 2011.

Art. 15. A eliminação de documentos produzidos pela CGUserá realizada mediante autor do Arquivo Nacional.

Seção II

Da Classificação da Informação

Art. 16. As informações da CGU são passíveis de classificaçãose consideradas imprescind segurança da sociedade edo Estado e se enquadrem no rol taxativo de hipótese classificaçãoapresentado no art. 23 da Lei nº 12.527, de 2011.

Parágrafo único. Na classificação da informação, deverá serutilizado o critério menos re possível.

Art. 17. A decisão de classificação, desclassificação, reclassificaçãoou redução do prazo de de informação classificada emqualquer grau de sigilo observará os procedimentos previstos nos ar 32 do Decreto nº 7.724, de 16 de maio de 2012, e deverá serformalizada em decisão consubstancia Termo de Classificaçãode Informação.

Art. 18. O acesso, a divulgação e o tratamento de informaçãoclassificada ficarão rest pessoas com necessidade de conhecê-lae que sejam credenciadas na forma estabelecida no Decr 7.845,de 14 de novembro de 2012, e nas normas complementares do Gabinetede Segurança Institu da Presidência da República, semprejuízo das atribuições dos agentes públicos autorizados na legisl

SeçãoIII

Do Controle dos Ativos de Informação

Art. 19. A gestão dos ativos de informação deve assegurarque esses ativos:

I - sejam inventariados e protegidos;

II - tenham entrada e saída nas dependências da CGU autorizadase registradas por auto competente;

III - sejam passíveis de monitoramento, garantindo a rastreabilidadedo seu uso;

IV - tenham identificados os seus custodiantes responsáveis;

V- sejam utilizados estritamente dentro do seu propósito,sendo vedado seu uso pa particulares ou de terceiros, entretenimento,veiculação de opiniões político-parti religiosas,discriminatórias e afins, observando a legislação em vigor; e

VI - quando se tratarem de dispositivos portáteis, tenhamregistrada sua cessão.

Parágrafo único. Ocorrências como extravio ou roubo devemser imediatamente comunic um membro do SISEG, para quesejam registradas como incidente de segurança da inform semprejuízo das demais providências necessárias.

Seção IV

Do Tratamento de Incidentes de Segurança

Art. 20. A gestão de incidentes em segurança da informaçãoe das comunicações te objetivo assegurar que fragilidades eincidentes sejam identificados tempestivamente, para per tomadade ação corretiva em tempo hábil.

§ 1º Os procedimentos para gestão de incidentes em segurançada informação são dispost normativo específico.

§ 2º Os incidentes de segurança devem ser registrados eanalisados periodicamente, se de subsídio para melhorias nosprocedimentos de segurança e para verificar falhas dos cor desegurança vigentes.

§ 3º O COPESEG deve ser informado sobre incidentes desegurança por meio de rel gerenciais.

Seção V

Da Gestão de Riscos

Art. 21. A Gestão de Riscos de Segurança da Informação edas Comunicações deve ser rea de forma sistemática e contínuae englobar todos os ativos de informação da CGU, visando a trata relacionados a disponibilidade, integridade, confidencialidade eautenticidade.

Art. 22. Aplicam-se à Segurança da Informação e das Comunicações,no que coub princípios e diretrizes de Gestão deRiscos definidos pela Política de Gestão de Riscos da CGU.

Art. 23. A Gestão de Riscos de Segurança da Informação e das Comunicaçõesdeve operacionalizada por meio de Metodologia específica.

Art. 24. Compete ao COPESEG a definição da periodicidademáxima para a execuçã processos de Gestão de Riscos deSegurança da Informação e das Comunicações.

Art. 25. Compete a todos os servidores da CGU o monitoramentoda evolução dos nív riscos e da efetividade dasmedidas de tratamento de riscos de Segurança da Informação e Comunic

Parágrafoúnico. No monitoramento de que trata o caputdeste artigo, caso sejam identif mudanças ou fragilidades emativos de informação, o servidor deverá reportar imediatamente o fat membro do SISEG.

Seção VI

Do Sistema de Gestão de Continuidade de Negócios

Art. 26. A Segurança da Informação e das Comunicaçõesdeve auxiliar a manutenção do Si de Gestão de Continuidade deNegócios da CGU, por meio da proteção, da redução da probabilid eventos negativos e da definição de medidas de controlee de recuperação dos seus ativos e proc críticos em situações deincidentes de interrupção.

Art. 27. Cabe ao COPESEG aprovar as diretrizes e responsabilidadesdo Sistema de Gest Continuidade de Negócio noque tange à Segurança da Informação e das Comunicações.

Seção VII

Da Auditoria e Conformidade

Art. 28. O uso dos ativos de informação da CGU deve serpassível de monitoramento e au devendo ser implementados emantidos mecanismos que permitam sua rastreabil acompanhamento,controle e verificação de acessos aos sistemas corporativos erede interna da CGU

Art. 29. O COPESEG deve promover, periodicamente, avaliaçãode conformidade a esta Por a suas normas e procedimentoscomplementares, bem como às regulamentações e legislaçõesem relativas à Segurança da Informação e das Comunicações,considerando os requisitos mínimo assegurem adisponibilidade, integridade, confidencialidade e autenticidade das informações.

SeçãoVIII

Da Segurança em Gestão de Pessoas

Art. 30. O COPESEG deverá propor ações de divulgação econscientização de agentes pú colaboradores e visitantes comacesso à CGU ou aos seus ativos de informação, que abordem osprin diretrizes, procedimentos e responsabilidades relacionadosà Segurança da Informação e Comunicações.

Parágrafo único. Qualquer agente público ou colaboradorpoderá propor ações de divulga conscientização, as quais serãoapreciadas pelo COPESEG.

Art. 31. O COPESEG proporá atividades de capacitação, dedivulgação e de disseminaçã orientações previstas nesta POSICaos agentes públicos e colaboradores.

Art. 32. Agentes públicos e colaboradores devem:

I - ter ciência das ameaças e preocupações relativas à segurançadas informações comunicações;

II - ter ciência de suas responsabilidades e obrigações noâmbito dessa política; e

III - difundir e exigir o cumprimento desta POSIC e demaisnormativos sobre o tema.

Art. 33. O ingresso, a movimentação e o desligamento dosagentes públicos e colabora bem como o encerramento de contratos,devem ser realizados de modo controlado, garantindo:

I - a devolução de todos os ativos de informação;

II - o cancelamento de autorizações de acesso às informaçõesclassificadas; e

III - a entrega de compromisso assinado de não divulgaçãode informações sigilosas.

Seção IX

Da Segurança Física

Art. 34. A segurança física e patrimonial, disposta em normativoespecífico tem por objeti
relação à segurança da informação,prevenir danos e interferências nas instalações da CGU quep
causar perda, roubo ou comprometimento das informações,em consonância com a Política de Ges
Riscos da CGU.

Art. 35. Será assegurada a salvaguarda das instalações e dosdemais ativos de informaç
que são elaborados, tratados, custodiados,manuseados ou guardados dados e informações c
ousensíveis, independentemente do meio em que estão armazenados.

Art. 36. O ingresso de visitantes deve ser controlado deforma a impedir o acesso destes às
de armazenamento ouprocessamento de informações sensíveis, salvo acompanhados, comautorizaç
responsável.

Art. 37. Todas as pessoas que tiverem acesso às instalaçõesfísicas devem portar identif
visível e, quando couber, nível deautorização de acesso.

Seção X

Da Segurança Lógica

Art. 38. A sistematização do controle de acesso à informação,detalhada em
complementar, tem por objetivo garantirque o acesso à informação e aos ativos que a armazenar
franqueadoexclusivamente a pessoas autorizadas, com base nos requisitosde negócio e de segurar
informação.

Parágrafo único. O acesso aos computadores, à rede corporativae aos serviços ofer
depende de prévia autenticação.

Art. 39. O acesso a qualquer informação veiculada eletronicamenteé passível de monitora
com vistas a garantir a rastreabilidadee a auditoria das ações realizadas.

Art. 40. A utilização dos meios de comunicação, inclusive ouso de dispositivos móveis, c
eletrônico e acesso à internet,bem como as responsabilidades dos usuários no tocante às informaçõ
trânsito devem ser tratados em norma específica.

Seção XI

Das Responsabilidades

Art. 41. É responsabilidade dos agentes públicos, colaboradorese visitantes com acesso
ou aos seus ativos de informaçãozelar pela estrita observância do disposto nesta Portaria,bem
comunicar formalmente a um membro do SISEG qualquerincidente ou ameaça à Seguran
Informação e das Comunicaçõesde que tiver ciência.

Art. 42. A violação da POSIC ou a quebra de segurança serácomunicada pelo COPES
autoridades competentes para a apuração.

CAPÍTULO IV

DISPOSIÇÕES GERAIS

Art. 43. Os contratos, convênios, acordos de cooperação eoutros instrumentos congê
celebrados pela CGU devem observaro contido nesta Política e nos seus dispositivos complementare

Art. 44. O COPESEG promoverá a edição ou a atualizaçãode normas complementares,
objetivo de estabelecer os procedimentosoperacionais necessários para a execução
determinaçõesdesta POSIC.

Art. 45. A POSIC da CGU será revisada, no mínimo, a cada5 (cinco) anos, ou sempre que h
alteração das diretrizes vigentes.

Art.46. Os casos omissos e as dúvidas surgidas na aplicaçãodesta Política serão dirimido
COPESEG.

Art. 47. Ficam revogadas a Portaria nº 1.213, de 03 de junhode 2014, e a Portaria nº 1.219,
de maio de 2015.

Art. 48. Esta Portaria entra em vigor na data de sua publicação.