POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Sumário

Histórico das Revisões

Versão	Data	Responsável	Observações
00	30/10/2014	COA	DCA 01/119ª de 30/10/2014
01	01/10/2024	CSIC	Adequação da política à IN 01 de 27/05/2020, atualizada até 29/01/2022, à IN nº 3 de 28 de maio de 2021, à Portaria nº 93 de 18 de outubro de 2021 do GSI/PR Aprovada na RCA nº 03/280ª, de 08 de novembro de 2024

Informações Adicionais

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Seção I - Objeto

Art. 1º Esta política estabelece diretrizes para a gestão da Segurança da Informação e Comunicações na EPE.

§ 1º A Segurança da Informação e Comunicações (SIC) objetiva assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações da EPE.

§ 2º A gestão da SIC deve estar alinhada ao planejamento estratégico da EPE e às diretrizes emanadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI).

Art. 2º São diretrizes para a gestão da SIC:

I - planejar, implementar, avaliar e monitorar as medidas de segurança da informação e comunicações levando em consideração os objetivos institucionais e os riscos para as atividades da EPE;

II - utilizar metodologias e modelos de segurança de informação de acordo com o estabelecido pela legislação pertinente;

III - prover o controle e o monitoramento do acesso às informações produzidas ou custodiadas pela EPE;

IV - assegurar que o acesso às informações sigilosas seja concedido somente às pessoas devidamente autorizadas;

V - promover a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização;

VI - assegurar que os aspectos da segurança da informação e comunicações sejam considerados durante a obtenção e a aquisição de obras, bens e serviços, bem como no desenvolvimento de software; e

VII - assegurar que a informação sob a custódia da EPE receba um nível adequado de proteção de acordo com o seu valor, sensibilidade e criticidade.

Seção II - Âmbito de Aplicação

Art. 3º Esta política aplica-se a todas as áreas da EPE, englobando as informações custodiadas tanto em ambiente lógico quanto físico.

Seção III - Responsabilidades

Art. 4º Compete ao Conselho de Administração aprovar, acompanhar e supervisionar a implementação dessa política, assim como quaisquer revisões futuras.

Art. 5º Compete à Diretoria Executiva:

I - instituir a estrutura de gestão de SIC da EPE;

II - promover ações de capacitação dos recursos humanos em temas relacionados à SIC;

III - coordenar e executar as ações de SIC no âmbito de sua atuação;

IV - consolidar e analisar os resultados dos trabalhos de auditoria sobre gestão de SIC;

V - aplicar as ações corretivas e administrativas cabíveis, nos casos de violação da SIC;

VI - definir o nível de risco em que se baseiam todas as ações de SIC; e

VII - estabelecer o cronograma para implementação de normas previstas nesta política.

Art. 6º Compete ao Comitê de Segurança da Informação e Comunicações (CSIC):

I - assessorar a implementação das ações de SIC;

II - participar da elaboração da política de SIC e das normas internas de SIC; e

III - propor alterações à política de SIC e às normas internas de SIC;

Art. 7º Compete ao Gestor de Segurança da Informação e Comunicações (GSIC):

I - coordenar a elaboração da política de SIC e das normas internas de SIC da EPE, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

II - assessorar o Conselho de Administração e a Diretoria Executiva na implementação da política de SIC;

III - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SIC; e

IV - promover a divulgação da política e das normas internas de SIC da EPE a todos os empregados, usuários e prestadores de serviços que trabalham na empresa.

Art. 8º Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) realizar as ações de prevenção, tratamento e resposta a incidentes cibernéticos, de acordo com normas específicas da EPE, em consonância com os normativos, padrões e procedimentos técnicos exarados pelo CTIR-GOV, sem prejuízo das demais metodologias e padrões conhecidos.

Seção IV - Documentos de Referência

Art. 9º Este documento foi elaborado tendo como referência:

I - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e dá outras providências;

II - Decreto nº 10.748, de 16 de julho de 2021 da Presidência da República, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;

III - Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal; e

V - Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação.

Seção V - Definições

Art.10. Adotam-se as seguintes siglas e definições no âmbito deste documento:

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

II - **ativo:** tudo que tenha valor para a organização, material ou não;

III - **ativos de informação:** meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

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

VI - **continuidade de negócios:** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido;

VII - **credencial de acesso:** permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como por exemplo um crachá), ou lógica (como por exemplo a identificação de usuário e senha);

VIII - **credenciamento:** processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso, em função de autorização prévia e da necessidade de conhecer;

IX - **CSIC:** Comitê de Segurança da Informação e Comunicações;

X - **CSIRT:** *Computer Security Incident Response Team*;

XI - **CTIR-GOV:** Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XII - **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;

XIII - **ETIR:** Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

XIV - **FIRST:** *Forum of Incident Response and Security Teams*;

XV - **GCN:** Gestão de Continuidade de Negócios;

XVI - **GSI** ou **GSI/PR:** sigla de Gabinete de Segurança Institucional da Presidência da República;

XVII - **GSIC:** Gestor de Segurança da Informação e Comunicações;

XVIII - **incidente:** interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, 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;

XIX - **incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

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

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

XXII - **ISO***: International Organization for Standardization*;

XXIII - **ReGIC:** Rede Federal de Gestão de Incidentes Cibernéticos; e

XXIV - **SIC:** Segurança da Informação e Comunicações.

CAPÍTULO II - DISPOSIÇÕES GERAIS

Seção I - Da Estrutura de Gestão da Segurança da Informação e Comunicações

Art.11. A gestão da Segurança da Informação e Comunicações (SIC) na EPE será exercida por uma estrutura composta por um Comitê de Segurança da Informação e Comunicações (CSIC), um Gestor de Segurança da Informação e Comunicações (GSIC) e uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

§ 1º O CSIC será regido por regimento próprio, aprovado pela Diretoria Executiva.

§ 2º O CSIC será vinculado administrativamente à Presidência da EPE.

§ 3º O GSIC titular e o GSIC suplente serão designados dentre os empregados da EPE, e deverão possuir formação técnica compatível com suas responsabilidades.

§ 4º O funcionamento da ETIR será regido por norma específica.

§ 5º A estrutura de gestão de SIC deve estar de acordo com o Decreto nº 9.637, de 26 de dezembro de 2018, a Instrução Normativa GSI nº 01, de 27 de maio de 2020 e demais instruções exaradas pelo GSI.

Seção II - Abrangência

Subseção I - Introdução

Art.12. A gestão da SIC visa a integrar os diversos temas relacionados à SIC aos processos institucionais estratégicos, operacionais e táticos, não se limitando à rede cibernética da empresa.

Parágrafo único. Os temas relacionados à SIC e cobertos pela gestão são:

I - tratamento da informação;

II - segurança física e do ambiente;

III - gestão de incidentes de SIC;

IV - mapeamento de ativos de informação;

V - gestão do uso dos recursos computacionais e de comunicações;

VI - gestão de identidade e acesso;

VII - gestão de riscos de SIC;

VIII - gestão de continuidade do negócio;

IX - avaliação de conformidade nos aspectos de SIC;

X - gestão de mudança nos aspectos de SIC; e

XI - segurança cibernética.

Subseção II - Tratamento da Informação

Art.13. O tratamento da informação é o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação e controle da informação.

Art.14. Toda informação institucional da EPE é patrimônio do Estado brasileiro e seu tratamento, ao longo do ciclo de vida, deve ser realizado de modo ético e responsável por todos os envolvidos.

Art.15. O tratamento da informação visa assegurar sua disponibilidade, integridade, confidencialidade e autenticidade.

Art.16. É dever de todo empregado da EPE salvaguardar a informação sigilosa e pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as exclusivamente para o exercício das atribuições de sua função.

Art.17. As medidas e os procedimentos relacionados ao tratamento da informação realizado por terceiros devem ser estabelecidos contratualmente, de forma a assegurar o cumprimento do normativo da EPE.

Art.18. O tratamento da informação será regulado por norma emitida pela EPE.

Subseção III - Segurança Física e do Ambiente

Art.19. A segurança física e do ambiente consiste nas ações de prevenção contra o acesso físico não autorizado, que pode causar danos e interferências com as instalações e informações da EPE.

Parágrafo único. A segurança física será regulada por norma específica.

Subseção IV - Gestão de Incidentes de SIC

Art.20. A gestão de incidentes de SIC engloba as atividades para prevenção, tratamento e resposta a incidentes de SIC.

Art.21. A gestão de incidentes será feita pela ETIR, de acordo com norma específica.

Parágrafo único. A EPE deverá designar um agente responsável pela ETIR.

Subseção V - Mapeamento de Ativos de Informação

Art.22. Será mantido registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade, de gestão da segurança cibernética e de gestão de mudanças nos aspectos relativos à SIC.

§ 1º A EPE designará um agente responsável para o mapeamento de ativos de informação.

§ 2º O mapeamento de ativos de informação será regulado por norma específica.

Subseção VI - Gestão do Uso dos Recursos Computacionais e de Comunicações

Art.23. O uso dos recursos computacionais da empresa será regulado por norma específica.

Subseção VII - Gestão de Identidade e Acesso

Art.24. O acesso a informações custodiadas pela EPE em ambiente computacional será controlado com o uso de credenciais de acesso.

Parágrafo único. As credenciais serão pessoais e intransferíveis e sua emissão será regulada por normativo específico.

Art.25. A concessão de permissões de acesso aos titulares das credenciais deverá levar em consideração a necessidade de conhecer e o princípio de mínimos privilégios, de forma a que os usuários consigam acesso ao conjunto mínimo de informações necessários à execução de seu trabalho.

Subseção VIII - Gestão de Riscos de SIC

Art.26. A gestão de riscos de SIC tem por objetivo direcionar e controlar os riscos de SIC, a fim de adequá-los aos níveis aceitáveis para a EPE.

§ 1º A gestão de riscos de SIC deverá seguir a metodologia adotada pela EPE, de acordo com as normas existentes.

§ 2º O planejamento da gestão de riscos de SIC deve ser revisado anualmente ou sempre que necessário.

§ 3º A gestão de riscos de SIC deverá ter caráter qualitativo.

§ 4º Nas revisões desta política deverá ser considerada a necessidade de adotar uma gestão quantitativa, incluindo cálculo de riscos, relação custo-benefício e eficácia das ações de segurança, de acordo com a maturidade da EPE no tema.

Art.27. O GSIC será o responsável pela Gestão de Riscos de SIC e terá a responsabilidade de realizar as tarefas de identificação, análise e avaliação dos riscos, bem como a proposição dos planos de tratamento dos riscos, em acordo com os demais envolvidos.

Subseção IX - Gestão de Continuidade de Negócio

Art.28. A implementação do processo de gestão de continuidade de negócio em aspectos de SIC tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da EPE, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art.29. É produto da GCN um conjunto de planos associados ao negócio da EPE e à infraestrutura, que devem ser periodicamente atualizados por todas as áreas envolvidas.

Art.30. A gestão de continuidade de negócio deverá seguir norma emitida pela EPE.

Art.31. A EPE deverá designar um agente responsável pela gestão de continuidade de Negócio, com as responsabilidades definidas pela norma.

Subseção X - Avaliação de Conformidade nos Aspectos de SIC

Art.32. A avaliação de conformidade nos aspectos de SIC consiste em proporcionar adequado grau de confiança aos processos de SIC, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

Art.33. O processo de avaliação de conformidade consiste na emissão do plano de verificação de conformidade e na emissão dos relatórios periódicos de avaliação de conformidade.

Art.34. A EPE designará um responsável pelo processo de avaliação de conformidade nos aspectos de SIC, que não deverá ser nenhum dos membros da equipe de gestão da SIC.

Subseção XI - Gestão de Mudança nos Aspectos de SIC

Art.35. Será implementado o processo de gestão de mudanças nos aspectos de SIC, com a finalidade de adaptar a empresa a mudanças decorrentes da evolução dos processos de tecnologia da informação.

§ 1º A gestão de mudança deverá levar em consideração as informações levantadas no âmbito da gestão de riscos de SIC.

§ 2º A gestão de mudança será regida por norma específica.

Subseção XII - Segurança Cibernética

Art.36. A segurança cibernética engloba as ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético ou locais, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Parágrafo único. A segurança cibernética será regulada por norma específica.

Seção III - Participação na ReGIC

Art.37. A EPE deverá fazer parte da ReGIC – Rede Federal de Gestão de Incidentes Cibernéticos, com o objetivo de aumentar o nível de resiliência em segurança cibernética de seus ativos de informação.

CAPÍTULO III - DISPOSIÇÕES FINAIS

Art.38. Esta política deverá ser revista no prazo máximo de 3 anos a partir da data de aprovação deste instrumento normativo.

Art.39. Casos omissos serão decididos pelo Conselho de Administração.

Art.40. Esta política entra em vigor na data de sua aprovação pelo Conselho de Administração.

Art.41. Fica revogada a política PDG-COA-006.