Boletim Eletrônico em 27/07/2022

00094.001547/2022-44

PRESIDÊNCIA DA REPÚBLICA

COMITÊ DE GOVERNANÇA DIGITAL

RESOLUÇÃO Nº 29, DE 21 DE JULHO DE 2022

Institui a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República - POSITEC/PR.

O **COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO DA PRESIDÊNCIA DA REPÚBLICA - CGDSI/PR**, no uso das atribuições que lhe foram conferidas pelo Decreto nº 10.159, de 9 de dezembro de 2019, e com base no disposto no inciso I do art. 2º, **resolve**:

Art. 1º Fica instituída a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República - POSITEC/PR.

§ 1º A Política de Segurança da Informação em Meios Tecnológicos da Presidência da República e suas normas complementares aplicam-se aos ativos de tecnologia disponibilizados pela Diretoria de Tecnologia (DITEC) da Secretaria Especial de Administração da Secretaria-Geral da Presidência da República aos órgãos integrantes da Presidência da República - PR e Vice-Presidência da República - VPR.

§ 2º Os órgãos integrantes da PR que possuam recursos próprios de Tecnologia da Informação e Comunicação deverão elaborar, de forma alinhada a esta Política, suas políticas próprias de segurança da informação em meios tecnológicos.

CAPÍTULO I

DA FINALIDADE

Art. 2º A Política de Segurança da Informação em Meios Tecnológicos da Presidência da República tem por finalidade estabelecer diretrizes estratégicas que visam garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações armazenadas, transmitidas ou processadas nos meios tecnológicos da Presidência da República, assim como proteger a imagem institucional da Presidência da República e da Vice-Presidência da República.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos desta Política, entende-se por:

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade aos ativos de informação de um órgão ou entidade;

II - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado que possam resultar em dano para um sistema ou instituição;

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

IV - Ativo: qualquer componente humano, tecnológico, **software**, serviços ou outros que sustentem uma ou mais atividades, e que tenham valor para a organização;

V - Ativo de Informação: os documentos, os sistemas de informação, os processos, os meios de armazenamento, transmissão e processamento de dados e informações, incluindo os equipamentos necessários a isso, bem como os locais onde eles se encontram e as pessoas que os acessam;

VI - Ativo de Tecnologia: meio tecnológico utilizado para armazenamento, transmissão e processamento de dados e informações, bem como o corpo técnico que o administra;

VII - Computação em nuvem: modelo computacional que permite acesso por demanda e, independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

VIII - Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos meios de tecnologia oferecidos pela Presidência da República;

IX - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizado ou não credenciado;

X - Contramedidas eletrônicas: técnicas destinadas a anular, atenuar ou prevenir a quebra de segurança;

XI - Custódia: ato de zelar, provisória ou permanentemente, pelo armazenamento, acesso, utilização, administração e preservação de informação produzida por outrem;

XII - Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda de pessoa física ou determinado sistema, órgão ou entidade;

XIII - Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos a sua capacidade de prestar serviços essenciais ou críticos, por um período de tempo superior ao prazo de recuperação;

XIV - Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XV - Estimativa de Riscos: processo utilizado para atribuir valores à probabilidade e às consequências de determinado risco;

XVI - Evento de Segurança da Informação: ocorrência identificada de procedimento, sistema, serviço ou rede que possa ser relevante para a segurança da informação;

XVII - Gestão de Riscos: conjunto de processos que permite identificar, analisar, avaliar e implementar as medidas necessárias para o tratamento de riscos, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XVIII - 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, classificação e tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança de recursos humanos e segurança documental aos processos institucionais estratégicos, operacionais e táticos;

XIX - Gestor de Segurança da Informação em Meios Tecnológicos: agente público responsável pelas ações de segurança da informação em meios tecnológicos de determinado órgão ou instituição;

XX - Identificação de riscos: processo para localizar, listar e caracterizar os elementos do risco;

XXI - Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação;

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

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

XXIV - Meios Tecnológicos: os recursos de **hardware** e **software**, tais como: sistemas de informação, canais de comunicação de voz e dados, equipamentos de comunicação e interconexão, computadores, dentre outros, bem como as instalações técnicas necessárias ao seu funcionamento;

XXV - Meios tecnológicos da PR: meios tecnológicos disponibilizados pela Diretoria de Tecnologia aos órgãos integrantes da PR e VPR;

XXVI - Plano de Continuidade de Tecnologia da Informação: documentação dos procedimentos e informações necessárias para que os órgãos e as entidades da Administração Pública Federal mantenham seus ativos de tecnologia críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em casos de incidentes;

XXVII - Política de Segurança da Informação: documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de estabelecer ações que visem a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações produzidas ou custodiadas pela Presidência da República, independentemente da forma e do meio físico em que estejam registradas;

XXVIII - Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento da segurança da informação;

XXIX - Segurança da Informação: consiste em assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação;

XXX - Tecnologia da Informação e Comunicação - TIC: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

XXXI - 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;

XXXII - Usuário: agentes públicos, colaboradores, consultores externos, estagiários, agentes honoríficos, prestadores de serviço, sistemas de informação e contemplados em relacionamentos formais de órgãos da Presidência da República com pessoas físicas, outros órgãos públicos ou entidades públicas ou privadas autorizados a utilizar os meios tecnológicos da PR; e

XXXIII - Visitante: pessoa sem vínculo com a Presidência da República que necessita do acesso aos meios tecnológicos especificados no inciso XXIV deste artigo.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º As ações desenvolvidas no âmbito da Política de Segurança da Informação em Meios Tecnológicos da Presidência da República serão norteadas pelos seguintes princípios:

I - Responsabilidade: os usuários e visitantes devem ter ciência das normas e procedimentos relativos à Segurança da Informação;

II - Ética: todos os direitos e interesses legítimos dos usuários e visitantes devem ser respeitados sem comprometimento da Segurança da Informação;

III - Auditabilidade: as soluções tecnológicas e os procedimentos implantados na Presidência da República devem dispor de funcionalidades suficientes para o registro dos acessos e ações dos usuários e visitantes;

IV - Celeridade: as ações de Segurança da Informação devem oferecer respostas a incidentes e correções de falhas de Segurança da Informação com brevidade;

V - Proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação devem ser apropriados e adequados ao valor e à necessidade de confiança nos ativos de informação da Presidência da República, considerando os impactos e a probabilidade de ocorrência dos riscos;

VI - Integração: as ações de Segurança da Informação devem ser integradas com as demais ações institucionais da Presidência da República; e

VII - Irretratabilidade (não repúdio): as ações de Segurança da Informação devem garantir que, num processo de envio e recebimento de informações, nenhum participante originador ou destinatário de informação possam, em momento posterior, negar a respectiva atuação.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5º As diretrizes de Segurança da Informação em meios tecnológicos estabelecidas nesta Política de Segurança da Informação em Meios Tecnológicos da Presidência da República deverão ser seguidas pelos usuários e visitantes, incumbindo-lhes a responsabilidade e o comprometimento com sua aplicação.

Art. 6º A informação deverá sempre ser protegida adequadamente, de acordo com esta Política, independentemente da forma ou do meio pelo qual seja apresentada ou compartilhada.

Art. 7º Os meios tecnológicos da PR serão fornecidos para uso institucional, para os fins a que se destinam e no interesse da administração.

Parágrafo único. O uso dos meios tecnológicos da PR para fins não institucionais será passível de punição, de acordo com a legislação.

Art. 8º Os casos omissos e as dúvidas decorrentes da aplicação do disposto nesta Resolução deverão ser direcionados ao Gestor de Segurança da Informação em Meios Tecnológicos da Presidência da República, para encaminhamento e deliberação do Comitê de Governança Digital e Segurança da Informação da Presidência da República.

CAPÍTULO V

DAS DIRETRIZES ESPECÍFICAS

Seção I

Da Gestão da Segurança da Informação em Meios Tecnológicos

Art. 9º Todos os mecanismos de proteção utilizados para a segurança da informação em meios tecnológicos deverão ser mantidos com o objetivo de garantir a continuidade da missão institucional da Presidência da República.

Art. 10 Os requisitos de segurança da informação em meios tecnológicos da PR deverão ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, devendo também ser exigido termo de confidencialidade, quando cabível.

Seção II

Da Gestão de Tratamento de Incidentes de Segurança em Rede

Art. 11 A Diretoria de Tecnologia deverá manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Art. 12 Os incidentes de segurança da informação em meios tecnológicos deverão ser comunicados, registrados e tratados de acordo com normativo específico.

Parágrafo único. Em caso de incidente, deverão ser seguidas as diretrizes previstas em normativo específico, para coleta e preservação de evidências.

Seção III

Da Gestão de Riscos de Tecnologia da Informação

Art. 13 A unidade responsável pelos ativos de tecnologia deverá implementar processo de Gestão de Riscos de Tecnologia da Informação baseado na legislação própria, do qual deverá resultar a confecção de documento específico.

Art. 14 A Gestão de Riscos de Tecnologia da Informação será implementada com vistas a identificar os ativos de tecnologia relevantes e determinar ações de gestão apropriadas.

Art. 15 O Plano de Continuidade de Tecnologia da Informação deverá complementar a Gestão de Riscos de Tecnologia da Informação, visando limitar os impactos de incidentes e garantir que as informações requeridas para os processos de interesse institucional estejam prontamente disponíveis.

Art. 16 A Norma de Gerenciamento de Incidentes de Segurança em Rede Computacional definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas perante incidentes de segurança em tecnologia.

Seção IV

Da Gestão de Ativos de Tecnologia da Informação e Comunicação

Art. 17 A unidade responsável pelos ativos de tecnologia deverá implementar normas operacionais e procedimentos específicos para sua gestão, que observem os requisitos de segurança e garantam sua adequada proteção e operação contínua.

Art. 18 Os ativos de tecnologia da Presidência da República deverão ser inventariados e atribuídos aos respectivos responsáveis.

Art. 19 É vedado comprometer a segurança da informação tratada ou custodiada pela PR.

Seção V

Do Tratamento e da Classificação da Informação

Art. 20 A informação deverá ser adequadamente manuseada e protegida.

Art. 21 Os dados, as informações e os sistemas de informação da Presidência da República deverão ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir-lhes a disponibilidade, a integridade, a confidencialidade e a autenticidade.

Art. 22 O Tratamento da Informação será feito conforme a legislação específica, assegurando-se os requisitos da disponibilidade, da integridade, da confidencialidade e da autenticidade da informação em todo o seu ciclo de vida.

Seção VI

Do Monitoramento, da Auditoria e da Conformidade

Art. 23 Todo evento de segurança da informação em meios tecnológicos deverá ser registrado, a fim de permitir a auditoria e a detecção de incidentes de segurança.

Art. 24 Os controles de segurança de tecnologia implementados deverão ser testados para verificar sua efetividade e conformidade com esta Política.

Art. 25 Toda interação do usuário e do visitante com os recursos tecnológicos da Presidência da República deverá ser registrada, a fim de permitir a auditoria.

Seção VII

Do Correio Eletrônico

Art. 26 O serviço de correio eletrônico será oferecido como um recurso institucional para apoiar os usuários da Presidência da República no cumprimento de suas atividades.

Art. 27 É vedado o uso para fins institucionais de serviço de correio eletrônico que não seja o disponibilizado pela PR.

Seção VIII

Do Acesso à Internet

Art. 28 A unidade responsável pelos ativos de tecnologia deverá instituir normas e procedimentos específicos para o acesso à internet disponibilizado pela PR, atendendo às determinações desta Política e da Lei nº 12.965, de 23 de abril de 2014.

Seção IX

Da Restrição, Controle de Acesso e Uso de Senhas

Art. 29 Os usuários terão identificação única, pessoal e intransferível.

Art. 30 O usuário terá acesso apenas aos ativos necessários e indispensáveis ao exercício das suas funções, respeitado o disposto em normas e na legislação específica.

Art. 31 A unidade responsável pelos ativos de tecnologia deverá instituir regras de controle de acesso aos meios tecnológicos da PR, atendendo às determinações desta Política.

Seção X

Do Uso Institucional das Redes Sociais

Art. 32 A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações da PR, será regida por normas internas especificas e deverá estar em consonância com esta Política e com os objetivos estratégicos da instituição.

Seção XI

Da Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Art. 33 As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação deverão observar os padrões, critérios e controles de segurança dispostos em normas e na legislação específica.

Seção XII

Da Conscientização, Sensibilização e Capacitação em Segurança da Informação de Tecnologia

Art. 34 Os órgãos integrantes do Comitê de Governança Digital e Segurança da Informação da Presidência da República deverão promover, continuamente, capacitação, reciclagem e aperfeiçoamento em segurança de tecnologia da informação a todos os usuários, com o propósito de criar uma cultura de segurança dentro da instituição.

Seção XIII

Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 35 Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta Política.

Parágrafo único. Os instrumentos do **caput** também deverão prever a obrigação de que a contra parte divulgue esta Política e suas normas complementares aos empregados, prepostos e a todos os envolvidos em atividades vinculadas à PR.

Seção XIV

Do Uso de Computação em Nuvem

Art. 36 O uso de recursos de computação em nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, será regido por normas e procedimentos específicos, que deverão ser instituídos pela unidade responsável pelos ativos de tecnologia, atendendo às determinações desta Política.

Art. 37 É vedado o uso de recurso de computação em nuvem não disponibilizado institucionalmente pela PR, para o armazenamento de informação institucional ou custodiada.

Seção XV

Do Uso de Dispositivos Móveis

Art. 38 A unidade responsável pelos ativos de tecnologia deverá instituir normas e procedimentos específicos para o uso de dispositivos móveis que acessarem os ativos de tecnologia da PR, atendendo às determinações desta Política.

Seção XVI

Da Propriedade Intelectual

Art. 39 Os códigos, técnicas, procedimentos e demais informações produzidas por servidores ou colaboradores, no exercício de suas funções, serão propriedade intelectual da PR, nos termos da Lei nº 9.279, de 14 de maio de 1996, e do art. 4º da Lei nº 9.609, de 19 de fevereiro de 1998, resguardado o direito de autoria nos casos de obras simplesmente subvencionadas pela PR, conforme disposto no art. 6º da Lei nº 9.610, de 19 de fevereiro de 1998.

Art. 40 É vedada a utilização de propriedade intelectual da PR em quaisquer projetos ou atividades de finalidade diversa da estabelecida pela Instituição, salvo mediante autorização específica.

Seção XVII

Das Penalidades

Art. 41 As ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de Segurança da Informação serão devidamente apuradas, sendo cabíveis, aos responsáveis, sanções administrativas, civis e penais.

CAPÍTULO VI

DAS ATRIBUIÇÕES E RESPONSABILIDADE

Art. 42 A gestão da segurança da informação em meios tecnológicos será realizada pelo Gestor de Segurança da Informação em Meios Tecnológicos da Presidência da República.

Art. 43 Compete à Diretoria de Tecnologia, como responsável técnica e custodiante dos ativos de tecnologia da informação e comunicação da Presidência da República:

I - elaborar e implementar normas de segurança da informação em meios tecnológicos, em cumprimento a esta Política;

II - proteger os dados, as informações, os sistemas de informação da PR sob sua guarda, bem como os meios utilizados para o armazenamento, processamento e transmissão, contra ameaças e ações não autorizadas;

III - manter registros dos eventos de segurança da informação relacionados aos recursos tecnológicos providos institucionalmente, devendo preservá-los, sob sigilo, em ambiente controlado e de segurança, de acordo com legislação específica;

IV - implementar processo para a gestão da continuidade dos serviços de tecnologia, contemplando a criação de planos de contingência e recuperação de desastres, periodicamente testados;

V - manter atuante a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da Presidência da República;

VI - implementar processo de gestão de riscos dos serviços e ativos de tecnologia da informação e comunicação;

VII - implementar processo para a avaliação da conformidade com as normas e procedimentos de segurança relativos à utilização dos meios tecnológicos da Presidência da República;

VIII - estabelecer parcerias e convênios para a implementação de ações em segurança da informação em meios tecnológicos;

IX - manter a Equipe de Contramedidas Eletrônicas atuando nas atividades de segurança eletrônica e de comunicações nos ambientes de uso do Presidente da República;

X - executar ações para o cumprimento das diretrizes definidas nesta Política e das metas definidas no Plano de Ação de Segurança da Informação; e

XI - designar servidor com notórios conhecimentos em segurança da informação para atuar como Gestor de Segurança da Informação em Meios Tecnológicos.

Art. 44 Os usuários dos meios tecnológicos da Presidência da República deverão conhecer, observar e adotar as ações de segurança da informação em meios tecnológicos estabelecidas por esta Política, bem como por suas normas específicas.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 45 Fica revogada a Resolução Nº 4, de 05 de junho de 2020, publicada em Boletim Eletrônico de 18 de junho de 2020.

Art. 46 Esta Resolução entra em vigor na data de sua publicação.

MARIO FERNANDES

Documento assinado eletronicamente por **Mario Fernandes**, **Coordenador do Comitê de Governança Digital/PR**, em 22/07/2022, às 19:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida informando o código verificador **3513833** e o código CRC **D5C1F93B** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00094.001547/2022-44 SEI nº 3513833