



PRESIDÊNCIA DA REPÚBLICA  
COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO

RESOLUÇÃO Nº 49, DE 28 DE AGOSTO DE 2025

Institui a Política de Segurança da Informação da  
Presidência da República - Posin/PR

**O COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO DA PRESIDÊNCIA DA REPÚBLICA**, no uso das atribuições que lhe confere o inciso VIII, do art. 2º, do Decreto nº 10.433, de 21 de julho de 2020, e considerando o disposto no art. 10, inciso IV, do Decreto nº 12.572, de 4 de agosto de 2025,

**RESOLVE:**

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

**Objeto**

Art. 1º Fica instituída a Política de Segurança da Informação da Presidência da República - Posin/PR, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação nos órgãos integrantes da Presidência.

Art. 2º Para os efeitos desta Política, aplicam-se os termos do Glossário de Segurança da Informação, publicado pelo Gabinete de Segurança Institucional, acrescido dos seguintes termos:

I - órgãos integrantes da Presidência, aqueles definidos no art. 2º da Lei nº 14.600, de 19 de junho de 2023, incluindo-se a Vice-Presidência da República; e

II - segurança da informação, aquela proteção nos termos do art. 2º do Decreto nº 12.572, de 4 de agosto de 2025, relacionada à segurança:

- a) dos dados, dos ativos de informação e dos processos organizacionais;
- b) do ambiente físico e eletrônico que contenha ativos de informação; e
- c) do pessoal envolvido no ciclo de vida da informação.

## **Âmbito de aplicação**

Art. 3º Esta Política se aplica a todas as unidades organizacionais da Presidência da República, incluindo as unidades organizacionais colegiadas, abrangendo:

I - todos os ativos de informação de propriedade ou custodiados pelos órgãos integrantes da Presidência;

II - todos os usuários de informação dos órgãos integrantes da Presidência, incluindo agentes públicos, prestadores de serviços ou pessoas habilitadas pela administração para acessar os ativos de informação sob responsabilidade de quaisquer desses órgãos;

III - todas as instalações físicas e lógicas administradas ou utilizadas pelos órgãos integrantes da Presidência;

IV - todos os contratos, acordos e demais instrumentos congêneres firmados pelos órgãos integrantes da Presidência da República com outros órgãos ou entidades públicas, bem como com entidades privadas, que deverão conter cláusula que assegure a obrigatoriedade de observância às diretrizes estabelecidas nesta Política; e

V - as informações classificadas em grau de sigilo, no que couber, devendo ser observada a legislação específica para o tratamento dessas informações.

## **Objetivos**

Art. 4º São objetivos desta Política:

I - estabelecer as normas gerais dos órgãos integrantes da Presidência, a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II - instituir a estrutura de governança e gestão de segurança da informação;

III - estabelecer papéis e responsabilidades quanto à segurança da informação;

IV - fortalecer a proteção dos ativos de informação, de modo a preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

V - nortear a elaboração de planos de ação e procedimentos operacionais necessários à efetiva implementação da segurança da informação;

VI - fomentar uma cultura de segurança da informação no âmbito da Presidência da República; e

VII - promover a adequada gestão do tratamento de dados pessoais nos órgãos integrantes da Presidência.

## **CAPÍTULO II**

### **DOS PRINCÍPIOS E DIRETRIZES**

Art. 5º As ações de segurança da informação da Presidência da República devem ser baseadas nos princípios constantes da Política Nacional de Segurança da Informação, atendendo aos seguintes critérios:

I - considerar, prioritariamente, os objetivos estratégicos, os planos estratégicos institucionais, a estrutura e a finalidade dos órgãos integrantes da Presidência;

II - ser tratadas de forma integrada, respeitando as especificidades e a autonomia dos órgãos integrantes da Presidência;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

IV - ter investimento dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos aos órgãos integrantes da Presidência;

V - visar à prevenção da ocorrência de incidentes;

VI - estar continuamente alinhada com a evolução da tecnologia e de seus riscos;

VII - estar alinhadas às melhores práticas de gestão de segurança da informação e às diretrizes e recomendações governamentais vigentes; e

VIII - proporcionar capacitação contínua, em segurança da informação, dos usuários de informação da Presidência da República.

### CAPÍTULO III

#### DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 6º A estrutura de gestão de segurança da informação da Presidência da República abrange:

I - a alta administração, composta das autoridades de maior nível hierárquico nos órgãos integrantes da Presidência;

II - o Comitê de Governança Digital e Segurança da Informação da Presidência da República - CGD/PR, nos termos do Decreto nº 10.433, de 21 de julho de 2020;

III - o Gestor de Segurança da Informação da Presidência da República - Gestor de SI/PR;

IV - o Gestor de Tecnologia da Informação da Presidência da República - Gestor de TI/PR;

V - Equipe de Tratamento de Incidentes de Segurança da Rede Computacional da Presidência da República - ETIR/PR;

VI - a gestão de segurança e credenciamento, implementada pelos gestores de segurança e credenciamento dos órgãos de registro da Presidência da República, nos termos do Decreto nº 7.845, de 14 de novembro de 2012 e de suas normas complementares; e

VII - os usuários de informação dos órgãos integrantes da Presidência.

Parágrafo único. O CGD/PR é a estrutura da Presidência da República que corresponde ao comitê de segurança da informação previsto no inciso II do art. 10 do Decreto nº 12.572, de 4 de agosto de 2025.

Art. 7º Compete à Alta Administração da Presidência da República:

I - garantir o alinhamento da segurança da informação com as demais ações estratégicas em governança digital e privacidade e proteção de dados;

II - fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da gestão da segurança da informação da Presidência da República, bem como o tratamento e decisões de segurança da informação em um nível de relevância e prioridade adequados; e

III - fomentar ações de promoção da cultura de segurança da informação, por meio de campanhas e capacitação de segurança da informação.

Art. 8º Em razão das competências previstas no art. 2º, incisos I, II e III do Decreto nº 10.433, de 21 de julho de 2020, cabe ao Comitê Gestor de Segurança da Informação da Presidência da República:

I - designar um gestor de segurança da informação para a Presidência da República, conforme estabelece o Decreto nº 12.572, de 4 de agosto de 2025, para atuar em nome de todos os órgãos integrantes da Presidência;

II - instituir a ETIR/PR;

III - aprovar esta Política e suas atualizações;

IV - coordenar e monitorar a implementação desta Política, promovendo a adoção de boas práticas de governança de segurança da informação;

V - avaliar propostas recebidas do Gestor de SI/PR;

VI - instituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

VII - acompanhar os trabalhos de tratamento e resposta a incidentes de segurança da informação; e

VIII - analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação.

Art. 9º Nos termos da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, compete ao Gestor de SI/PR:

I - coordenar a revisão e atualização desta Política e dos normativos dela decorrentes;

II - assessorar a Alta Administração na implementação desta Política;

III - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV - promover a divulgação desta Política, bem como dos planos de ação e procedimentos operacionais de segurança, a todos os usuários de informação na Presidência da República;

V - incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VI - acompanhar os trabalhos da ETIR/PR e dar ciência ao CGD/PR das estatísticas de incidentes cibernéticos;

VII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; e

VIII - manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Parágrafo único. Ao gestor de SI/PR cabe ainda a coordenação do Subcomitê de Segurança da Informação, vinculado ao CGD/PR, conforme disposto no Decreto nº 10.433, de 21 de julho de 2020.

Art. 10. Compete ao Gestor de TI/PR, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada.

Art. 11. Compete à ETIR/PR:

I - facilitar, coordenar e executar atividades de prevenção, tratamento e resposta a incidentes cibernéticos na Presidência da República;

II - monitorar sistemas, aplicativos, dispositivos e as redes computacionais, no âmbito de sua atuação;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação, em conjunto com as respectivas áreas;

V - elaborar relatórios de incidentes e comunicar ao Gestor de SI;

VI - identificar vulnerabilidades e artefatos maliciosos;

VII - apoiar a recuperação de sistemas computacionais;

VIII - promover a cooperação com outras equipes; e

IX - participar de fóruns e redes relativas à segurança da informação.

Parágrafo único. A composição, estrutura, recursos e funcionamento da ETIR/PR serão definidos em ato administrativo específico, de acordo com a legislação sobre o tema.

Art. 12. Os usuários de informação devem conhecer, cumprir e fazer cumprir esta Política, os planos de ação e os procedimentos operacionais de segurança da informação da Presidência da República.

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

Art. 13. A gestão da segurança da informação na Presidência da República deve ser constituída, no mínimo, pelos seguintes processos, nos termos da Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021:

I - gestão de recursos humanos;

II - tratamento e classificação da informação;

III - segurança física e do ambiente;

IV - gestão de incidentes em segurança da informação;

V - gestão de ativos;

VI - gestão do uso dos recursos operacionais e de comunicações, tais como correio eletrônico, acesso à internet, mídias sociais, dispositivos móveis, computação em nuvem e outras soluções computacionais;

VIII - controles de acesso lógico e físico;

IX - gestão de riscos;

X - gestão de continuidade de negócios; e

XI - auditoria e conformidade.

Parágrafo único. Podem ser propostos outros processos de gestão de segurança da informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

Art. 14. Para cada um dos processos que compõem a gestão de segurança da informação, devem ser elaborados planos de ação ou procedimentos operacionais, podendo ser ambos, que auxiliem na sua disciplina e compreensão.

§1º Os planos de ação devem definir as ações estratégicas a serem adotadas, estabelecendo objetivos, responsabilidades, prazos e métricas para sua implementação e acompanhamento.

§2º Os procedimentos operacionais podem ser formalizados por meio de instruções normativas e devem fornecer, de maneira clara e objetiva, diretrizes sobre a execução de cada atividade, incluindo os responsáveis por sua realização.

§3º A escolha entre a elaboração de um plano de ação, um procedimento operacional ou ambos dependerá da complexidade, do impacto e da necessidade de detalhamento do processo a ser regulamentado.

## CAPÍTULO IV

### DAS DIRETRIZES ESPECÍFICAS

#### **Gestão de recursos humanos**

Art. 15. É responsabilidade de todos os usuários de informação dos órgãos integrantes da Presidência:

I - procurar conhecer as principais ameaças e preocupações relativas ao tema de segurança da informação;

II - ter ciência de suas responsabilidades e obrigações no âmbito desta Política;

III - difundir e exigir o cumprimento desta Política, dos planos de ação e dos procedimentos

operacionais para implementação da segurança da informação e da legislação vigente sobre o tema;

IV - tratar os dados pessoais de modo ético e responsável, ao longo de todo o ciclo de vida;

e

V - buscar manter-se atualizado sobre segurança da informação.

Art. 16. Em razão das competências previstas no art. 16, inciso I, do Decreto nº 11.329, de 1 de janeiro de 2023, cabe à unidade responsável pela gestão de pessoas da Presidência da República, orientar planos de ação, procedimentos operacionais ou ambos, para implementar e manter processos permanentes voltados à:

I - conscientização permanente para o desenvolvimento de uma cultura de segurança da informação, com atualizações periódicas para refletir alterações nos normativos e padrões aplicáveis; e

II - capacitação dos usuários de informação da Presidência da República, abordando:

a) a Política de Segurança da Informação e seus normativos complementares;

b) as responsabilidades dos usuários para garantir a eficácia do sistema de gestão da segurança da informação e de seus controles;

c) os benefícios decorrentes da melhoria da segurança da informação; e

d) as consequências do não cumprimento dos requisitos do sistema de gestão da segurança da informação.

Parágrafo único. Os processos de que trata o *caput* devem alcançar todos os usuários de informação da Presidência da República, de acordo com suas competências funcionais.

### **Tratamento da informação classificada**

Art. 17. Toda informação produzida ou custodiada pelos órgãos integrantes da Presidência deverá receber adequado tratamento durante todo seu ciclo de vida, conforme sua classificação quanto ao grau de sigilo, nos termos do Decreto nº 7.845, de 14 de novembro de 2012.

Art. 18. O acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas, nos termos do Decreto nº 7.845, de 2012.

Art. 19. As informações classificadas armazenadas ou processadas em equipamentos e sistemas de informação deverão ser protegidas por meio de criptografia, conforme estabelecido na Portaria GSI/PR nº 23, de 15 de julho de 2014, e somente poderão ser tratadas por recursos tecnológicos consonantes com os requisitos previstos do Decreto nº 7.845, de 2012.

Parágrafo único. O Gestor de TI/PR adotará medidas para implantação de rede para tratamento de informações classificadas, em articulação com o Núcleo de Segurança e Credenciamento, de que trata a Lei nº 12.527, de 18 de novembro de 2011.

Art. 20. Cabe à gestão de segurança e credenciamento dos órgãos integrantes da Presidência da República elaborar planos de ação, procedimentos operacionais ou ambos, destinados ao credenciamento de segurança e ao tratamento de informação classificada, contemplando, no mínimo, os seguintes aspectos:

I - controle da informação classificada;

II - produção, marcação, tramitação, expedição e reprodução de informação classificada;

III - recebimento e destinação da informação classificada;

IV - preservação e guarda da informação classificada;

V - definição, demarcação, sinalização e segurança das áreas de acesso restrito; e

VI - transporte de documentos com informação classificadas.

Parágrafo único. O documento preparatório que possa originar informação classificada deverá receber tratamento correspondente ao grau de sigilo estimado.

## **Controle de acesso aos ativos de informação**

Art. 21. A segurança física e lógica dos ativos de informação de propriedade dos órgãos integrantes da Presidência, ou por eles custodiados:

I - será realizada por intermédio da implementação de controles de acesso físico e lógico; e

II - terá o acesso controlado e limitado ao estritamente necessário ao desempenho das funções de cada usuário da informação.

Parágrafo único. Os controles de acesso físico e lógico abrangem todas as instalações físicas onde sejam desenvolvidas atividades permanentes ou temporárias dos órgãos integrantes da Presidência.

Art. 22. A concessão do acesso de que trata o inciso II do art. 21 deverá:

I - ser estritamente funcional, pessoal e intransferível;

II - ser autorizada por autoridade competente, conforme os procedimentos formais estabelecidos; e

III - ser periodicamente revisada e revogada quando não houver mais justificativa para sua manutenção.

Parágrafo único. Os usuários de informação devem responder perante a autoridade responsável, por acessos, tentativas de acessos ou uso indevido da informação, realizados com suas credenciais de acesso.

Art. 23. Os acessos devem ser registrados para viabilizar procedimentos de auditoria.

Art. 24. A implementação de controle de acesso físico às áreas e instalações dos órgãos integrantes da Presidência, onde se encontram mantidos os ativos de informação, é de competência da unidade responsável pela segurança física na Presidência da República.

Art. 25. Cabe à unidade responsável pela segurança física na Presidência da República, criar planos de ação, procedimentos operacionais ou ambos, para:

I - definir perímetros de segurança física para proteção dos ativos de informação de propriedade dos órgãos integrantes da Presidência, ou por eles custodiados;

II - definir regras para concessão, revogação e restrição de acesso físico às áreas e instalações onde serão tratadas informações de acesso restrito de propriedade dos órgãos integrantes da Presidência, ou por eles custodiadas;

III - estabelecer responsabilidades dos usuários dos serviços de controle de acesso físico; e

IV - promover a capacitação dos usuários de informação dos serviços de controle de acesso físico, em articulação com a unidade responsável pela gestão de pessoas da Presidência da República.

§1º A localização e a capacidade dos perímetros de segurança física devem ser adequadas e proporcionais aos requisitos de segurança dos ativos da informação tratados nessas áreas, observadas a análise de riscos dos ativos e a classificação do nível de segurança física do local.

§2º As regras para entrada, permanência, circulação e saída das áreas e instalações podem abranger a identificação e o registro de informações de dispositivos móveis de propriedade particular ou corporativos, bem como de seus portadores.

§3º Os procedimentos de que trata os incisos I e II devem considerar os públicos autorizados, os locais específicos, os meios de acesso e os requisitos de segurança dos ativos, além de estabelecer regras para a solicitação e o registro de perda, extravio ou furto de credenciais físicas.

Art. 26. As áreas e instalações utilizadas para o tratamento da informação de propriedade ou custodiada pelos órgãos integrantes da Presidência devem estar localizadas em edificações sólidas, que contenham barreiras físicas, recursos de prevenção e resposta a incêndios e a outros tipos de falhas, sistemas adequados de detecção de intrusos e meios para controlar o acesso físico ao local.

Art. 27. Os órgãos integrantes da Presidência devem comunicar formalmente à unidade responsável pela segurança física na Presidência da República:

I - as áreas e instalações onde são tratadas informações classificadas ou informações de acesso restrito;

II - as áreas ou instalações que contêm ativos de informação de sua propriedade, ou por eles custodiados, a serem protegidos por controles de acesso físico; e

III - os veículos de serviço a serem credenciados, observadas a necessidade de acesso, as atividades a serem executadas e a avaliação de riscos correspondente.

Parágrafo único. Quando o controle de acesso for realizado por meio de um serviço de vigilância contratado, a indicação de que trata o inciso II também deverá ser comunicada aos responsáveis pelo serviço contratado.

Art. 28. A implementação de controle de acesso lógico aos ativos de informação dos órgãos integrantes da Presidência é de competência unidade responsável pela tecnologia da informação da Presidência da República.

§1º São considerados ativos de informação aqueles, conectados ou não à rede computacional da Presidência da República, que são gerenciados pelos seus órgãos integrantes.

§2º A definição de controle de acesso lógico considerará, se necessário, os requisitos de segurança específicos de um órgão integrante, de ocupantes de uma função ou de um recurso computacional, observando, quando possível, os resultados da análise de riscos realizada e do plano de continuidade de negócio vigente.

§3º O controle de acesso lógico que tem como resultado a concessão ou negação de acesso físico será considerado controle de acesso físico, cabendo o regramento estabelecido nos arts. 24 a 27 desta Resolução.

Art. 29. O controle de acesso lógico deverá utilizar, preferencialmente, autenticação de multifatores, com o objetivo de possibilitar a autenticação da identidade do usuário e a sua vinculação a uma conta de acesso a ativos de informação.

Parágrafo único. Quando utilizada biometria como fator de autenticação, os dados biométricos devem ser tratados como dados pessoais sensíveis, conforme disposto no inciso II do art. 5º da Lei nº 13.709, de 14 de agosto de 2018.

Art. 30. Os órgãos integrantes da Presidência devem comunicar formalmente à unidade responsável pela tecnologia de informação da Presidência da República:

I - os direitos e as restrições de acesso lógico às informações sob sua propriedade ou custódia, quando se tratarem de ativos de informação gerenciados por aquela diretoria;

II - a necessidade de concessão, alteração e revogação de permissões de acesso lógico a informações de sua propriedade ou por eles custodiadas, armazenadas em ativos de informação gerenciados por aquela diretoria;

III - a necessidade de revisão dos direitos de acesso quando houver mudanças nos ativos de informação utilizados, para atualização das regras de acesso correspondentes; e

IV - a necessidade de acesso remoto de seus usuários de informação.

Parágrafo único. A unidade responsável pela tecnologia de informação da Presidência da República também poderá indicar aos órgãos integrantes da Presidência, a necessidade de revisão dos direitos e das restrições de acesso lógico, em decorrência de atualizações tecnológicas nos ativos de informação que gerencia.

Art. 31. Cabe à unidade responsável pela tecnologia da informação da Presidência da República, criar planos de ação, procedimentos operacionais ou ambos, para:

I - a concessão, revogação e restrição de acesso lógico aos ativos de informação;

II - a utilização de autenticação multifator;

III - o controle de acesso de usuários desligados ou afastados;

IV - as responsabilidades dos usuários em relação aos serviços de controle de acesso lógico;

V - o acesso remoto à rede computacional da Presidência da República, por meio de rede virtual privada institucional, criptografada e autenticação multifator;

VI - a capacitação dos usuários nos serviços de controle de acesso lógico, em articulação com a unidade responsável pela gestão de pessoas da Presidência da República; e

VII - o uso de dispositivos móveis institucionais e particulares - para acesso às informações de propriedade ou custodiadas pelos órgãos integrantes da Presidência - incluindo o registro, o monitoramento do uso e a identificação do portador.

### **Gestão de incidentes em segurança da informação**

Art. 32. É dever dos usuários de informação da Presidência da República reportar imediatamente à ETIR/PR, os eventos ou incidentes de segurança da informação por eles identificados.

Art. 33. Qualquer incidente de segurança que represente risco ou cause dano relevante aos dados pessoais dos titulares deve ser comunicado ao EDP/PR, que realizará a análise e, se necessário, encaminhará a ocorrência à ANPD.

Art. 34. Os incidentes de segurança, de que trata o art. 32, devem:

I - ser identificados, registrados, monitorados, comunicados e devidamente tratados, em tempo hábil, de forma a garantir a continuidade das atividades e o não comprometimento do alcance dos objetivos estratégicos; e

II - ser tratados pela ETIR/PR.

Parágrafo único. Na gestão dos incidentes de que trata o *caput*, conforme a necessidade, podem ser coletadas e armazenadas evidências para assegurar conformidades legais.

Art. 35. Cabe à ETIR/PR estabelecer planos de ação, procedimentos operacionais ou ambos, para a gestão de incidentes de segurança da informação, abrangendo, no mínimo, as etapas de identificação, contenção, erradicação e recuperação de atividades após a ocorrência de incidentes.

### **Gestão de ativos**

Art. 36. Os ativos de informação dos órgãos integrantes da Presidência devem:

I - possuir controles de segurança implementados, independentemente do meio em que se encontram; e

II - ser protegidos contra divulgação não autorizada, modificações, remoção e destruição, a fim de evitar incidentes de segurança da informação que possam danificar a imagem institucional e interromper suas operações;

Parágrafo único. Devem ser implementados, mecanismos que mitiguem o risco de acesso indevido, tais como revisão periódica dos acessos ou inativação automatizada dos acessos quando do desligamento ou de mudanças funcionais de usuários de informação.

Art. 37. São diretrizes para o controle de acesso privilegiado:

I - as contas com privilégios administrativos devem empregar mecanismos de autenticação forte, preferencialmente múltiplos fatores de autenticação - MFA e senhas exclusivas;

II - as credenciais utilizadas por contas privilegiadas não devem ser reutilizadas entre sistemas computacionais distintos, sendo exigida a adoção de senhas únicas e complexas;

III - sempre que tecnicamente viável, os dispositivos de rede devem adotar múltiplos fatores de autenticação e contar com senhas de administração exclusivas para cada dispositivo;

IV - é obrigatório o uso de MFA para todos os acessos remotos a sistemas computacionais críticos, inclusive via rede virtual privada - VPN, conexões administrativas e interfaces de gerenciamento em nuvem; e

V - auditoria periódica das contas privilegiadas.

Art. 38. Cabe à unidade responsável pela tecnologia informação da Presidência da República estabelecer planos de ação, procedimentos operacionais ou ambos, para a gestão de ativos de segurança da informação, contemplando, no mínimo:

- I - o mapeamento e a classificação dos ativos conforme sua criticidade para a organização;
- II - entrada e saída de ativos de informação das instalações dos órgãos integrantes da Presidência;
- III - a manutenção de um inventário atualizado, incluindo tipo de ativo, localização, proprietário ou custodiante e status de segurança;
- IV - a definição de uso aceitável dos ativos, vedada sua utilização para fins particulares pelo responsável;
- V - a identificação de vulnerabilidades, ameaças e suas interdependências;
- VI - o monitoramento contínuo dos ativos, em conformidade com os princípios legais de segurança da informação e privacidade;
- VII - a investigação de sua operação e uso sempre que houver indícios de falha de segurança ou privacidade.

### **Gestão de cópias de segurança e recuperação de dados**

Art. 39. A gestão de cópias de segurança poderá ser realizada para os seguintes tipos de ativos de informação:

- I - arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;
- II - arquivos de *log* de aplicativos, inclusive *log* da ferramenta de cópia e restauração de dados;
- III - informações e configurações de banco de dados;
- IV - conteúdo de repositórios de dados institucionais; e
- V - arquivos institucionais diversos.

Parágrafo único. As cópias de segurança devem ser utilizadas exclusivamente para a recuperação em casos de desastre, perda de dados por apagamento acidental ou corrupção, não sendo destinadas ao armazenamento ou à preservação de longo prazo.

Art. 40. Os órgãos integrantes da Presidência devem comunicar formalmente, à unidade responsável pela tecnologia da informação da Presidência da República, a necessidade de realizar cópias de segurança das informações sob sua propriedade ou custódia.

§1º A realização de cópias de segurança e a restauração de dados serão permitidas apenas para dispositivos administrados pela unidade responsável pela tecnologia da informação da Presidência da República.

§2º Os órgãos integrantes da Presidência devem comunicar a necessidade de garantir a confidencialidade do ativo de informação, para que as cópias de segurança possam ser protegidas por criptografia pela unidade responsável pela tecnologia da informação da Presidência da República.

§3º A gestão das cópias de segurança dos dados armazenados nas estações de trabalho é de responsabilidade exclusiva do usuário, que deve garantir a realização e a preservação dessas cópias.

§4º É dever do usuário armazenar todas as informações corporativas que produzir em área de rede mantida pela unidade responsável pela tecnologia da informação da Presidência da República, viabilizando a realização da devida cópia de segurança.

§5º O usuário poderá, a seu critério, realizar cópia pessoal de material que não seja objeto dos procedimentos de cópia de segurança, uma vez que procedimentos de recuperação de incidentes podem implicar na formatação completa da estação de trabalho.

Art. 41. A infraestrutura de cópias de segurança deve ser apartada, lógica e fisicamente, dos sistemas computacionais críticos dos órgãos integrantes da Presidência.

Art. 42. As cópias de segurança dos dados devem ser testadas periodicamente, com o objetivo de garantir a confiabilidade e a integridade dos dados resguardados, bem como verificar o atendimento dos níveis de serviços pactuados.

Art. 43. As unidades de armazenamento utilizadas na cópia de segurança dos dados devem considerar as seguintes características:

- I - a criticidade do dado resguardado;
- II - o tempo de retenção do dado resguardado;
- III - a probabilidade de necessidade de restauração;
- IV - o tempo esperado para restauração;
- V - o custo de aquisição da unidade de armazenamento de backup; e
- VI - a vida útil da unidade de armazenamento de backup.

Art. 44. Cabe à unidade responsável pela tecnologia informação da Presidência da República estabelecer planos de ação, procedimentos operacionais ou ambos, para a gestão de cópias de segurança e recuperação de dados, complementares a esta Política, observando as seguintes diretrizes:

- I - ser periódicos e orientados para a restauração dos dados no menor tempo possível;
- II - utilizar soluções especializadas para este fim, preferencialmente de forma automatizada;
- III - realizar verificação periódica de integridade dos dados armazenados;
- IV - possuir requisitos mínimos diferenciados de acordo com o tipo do ativo de informação e sua criticidade quanto ao nível de disponibilidade requerido;
- V - observar os requisitos de controle de acesso; e
- VI - buscar a melhoria contínua de acordo com as melhores práticas vigentes.

### **Uso do correio eletrônico**

Art. 45. É vedado o uso:

- I - de serviço de correio eletrônico, para fins institucionais, alheio aquele disponibilizado pela Presidência da República; e
- II - de endereços de e-mail e de outras credenciais corporativas, para criar contas em plataformas externas que não sejam por necessidade de serviço ou determinação expressa de superior hierárquico.

Art. 46. O acesso às caixas de correio eletrônico institucionais e às listas de transmissão de e-mails observará as seguintes regras:

- I - o acesso a caixas individuais, de uso exclusivo de um único usuário de informação, é proibido a terceiros, salvo quando houver interesse público, nos termos da legislação vigente;
- II - o acesso a caixas setoriais, compartilhadas por múltiplos usuários de informação, será permitido apenas aos usuários designados e autorizados pelo titular da unidade organizacional solicitante; e
- III - cabe ao titular da unidade organizacional solicitante a gestão dos membros das listas de transmissão de e-mails, bem como dos permissionários das caixas compartilhadas.

Art. 47. Cabe à unidade responsável pela tecnologia informação da Presidência da República estabelecer planos de ação, procedimentos operacionais ou ambos, para o uso do correio eletrônico institucional, incluindo diretrizes para a abertura de anexos de e-mail.

### **Uso de mídias sociais**

Art. 48. O uso seguro de mídias sociais pelos órgãos integrantes da Presidência deverá observar as diretrizes estabelecidas nos arts. 14 a 18 da Instrução Normativa GSI/PR nº 6, de 23 de dezembro de 2021, especialmente quanto à segurança da informação e preservação da imagem institucional.

Art. 49. Cabe aos órgãos integrantes da Presidência, estabelecer planos de ação, procedimentos operacionais ou ambos, para o uso seguro de mídias sociais, em conformidade com os arts. 9º a 13 da Instrução Normativa GSI/PR nº 6, de 2021.

### **Uso de dispositivos móveis**

Art. 50. O uso de dispositivos móveis, corporativos ou particulares, para acesso a informações institucionais está sujeito às seguintes regras:

I - dispositivos móveis corporativos devem ser utilizados exclusivamente para fins institucionais, sendo vedado o uso para atividades pessoais ou instalação de aplicativos não autorizados;

II - o armazenamento de informações sensíveis ou sigilosas em dispositivos móveis deve seguir as diretrizes de segurança definidas pela unidade responsável pela tecnologia da informação da Presidência da República, incluindo criptografia e controle de acesso;

III - o acesso a sistemas computacionais institucionais a partir de dispositivos particulares deve ser realizado apenas por meio de canais seguros e autorizados, com autenticação adequada e exclusivamente por meio de redes seguras;

IV - em caso de perda, furto ou extravio de dispositivo móvel corporativo ou pessoal com acesso a informações do órgão, o usuário deve comunicar imediatamente ao Gestor de SI/PR; e

V - É proibido conectar dispositivos móveis pessoais a redes internas ou sistemas computacionais críticos do órgão sem autorização expressa da unidade responsável pela tecnologia da informação da Presidência da República.

Art. 51. Cabe à unidade responsável pela tecnologia da informação da Presidência da República estabelecer planos de ação, procedimentos operacionais ou ambos, para o uso de dispositivos móveis, corporativos ou particulares.

### **Computação em nuvem**

Art. 52. O tratamento de informações em computação em nuvem deverá atender aos requisitos mínimos de segurança da informação estabelecidos na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, garantindo, no mínimo, que:

I - sejam utilizados exclusivamente serviços que integrem o catálogo de soluções de computação em nuvem em uso na Presidência da República;

II - seja obrigatório o uso de controle de acesso sob a gestão da Presidência da República, em conformidade com os riscos de segurança da informação e a legislação vigente, para o tratamento de:

- a) informações sigilosas protegidas por legislação específica;
- b) materiais de acesso restrito, conforme regulamentação do próprio órgão; e
- c) informações pessoais relacionadas à intimidade, vida privada, honra e imagem.

Art. 53. O uso institucional de serviços de computação em nuvem no âmbito dos órgãos integrantes da Presidência é restrito aos usuários de informação com cadastro no sistema de pessoal da Presidência da República.

Parágrafo único. Excepcionalmente, e por interesse da administração, poderá ser autorizada a utilização por usuários não contemplados no *caput*, de forma temporária ou contínua, mediante análise prévia de riscos.

Art. 54. Nas contratações de serviço de computação em nuvem devem constar como requisitos as cláusulas de que trata o art. 19 da Instrução Normativa GSI/PR nº 5, de 2021.

Art. 55. Cabe à unidade responsável pela tecnologia da informação da Presidência da República estabelecer planos de ação, procedimentos operacionais ou ambos, para o uso de computação em nuvem.

Parágrafo único. Os instrumentos tratados no *caput* devem incluir diretrizes para a atualização do catálogo de soluções de computação em nuvem em uso, especificando o modelo de implementação, os tipos de informação autorizados para tratamento nesse ambiente e outros dados considerados relevantes.

## **Inteligência artificial**

Art. 56. O desenvolvimento e a implementação de plataformas corporativas de inteligência artificial no âmbito da Presidência da República, inclusive protótipos para avaliação de funcionalidades ainda não disponíveis em plataformas já aprovadas pelo CGD/PR, devem ser supervisionados pela unidade responsável pela tecnologia da informação da Presidência da República.

Art. 57. Qualquer usuário de informação da Presidência da República que utilizar soluções de inteligência artificial é responsável por revisar e validar os resultados obtidos, assegurando que o conteúdo gerado seja adequado, preciso e alinhado aos princípios institucionais, evitando informações discriminatórias, incorretas ou prejudiciais aos ativos de informação e à sociedade.

Art. 58. Cabe à unidade responsável pela tecnologia da informação da Presidência da República estabelecer planos de ação, procedimentos operacionais ou ambos, para o uso de tecnologia da inteligência artificial no âmbito da Presidência da República.

## **Uso de recursos computacionais diversos**

Art. 59. O acesso à internet deverá ser utilizado exclusivamente para fins institucionais.

§ 1º O tráfego de dados poderá ser monitorado e registrado para garantir a segurança e o uso adequado dos recursos.

§ 2º É vedado o acesso a *sites* que possam comprometer a segurança da informação ou que sejam incompatíveis com a missão da Presidência da República.

§ 3º A navegação deve passar por filtros de segurança, incluindo sistemas de proteção contra ameaças cibernéticas, como bloqueio de *phishing* e *malware*.

Art. 60. O *download* de arquivos deve ser realizado apenas de fontes confiáveis e previamente analisado por soluções de segurança, como antivírus e sistemas de proteção contra ameaças.

Parágrafo único. É proibido o *download* de *softwares* ou arquivos que possam comprometer a segurança dos sistemas computacionais institucionais ou violar normas de conformidade.

Art. 61. Apenas *softwares* autorizados pela unidade responsável pela tecnologia da informação na Presidência da República podem ser instalados nos computadores institucionais.

§ 1º As atualizações dos *softwares* instalados devem ocorrer periodicamente, preferencialmente de forma automatizada, de modo a garantir a conformidade com as melhores práticas de segurança e a proteção contra vulnerabilidades.

§ 2º Qualquer necessidade de *software* adicional deve ser formalmente justificada e submetida à análise da unidade responsável pela tecnologia da informação da Presidência da República.

## **Aquisição, desenvolvimento e manutenção de sistemas computacionais**

Art. 62. A segurança da informação deve ser projetada e implementada em todo o ciclo de desenvolvimento e manutenção de sistemas computacionais.

Art. 63. Os ambientes de desenvolvimento, teste e produção de sistemas computacionais devem ser desagregados para reduzir riscos de acesso ou modificações indevidas ou não autorizadas.

Art. 64. Cabe à unidade responsável pela tecnologia da informação da Presidência da

República estabelecer planos de ação, procedimentos operacionais ou ambos, para a aquisição, o desenvolvimento e a manutenção de sistemas computacionais no âmbito da Presidência da República.

### **Gestão de riscos em segurança da informação**

Art. 65. Em conformidade com o art. 12, inciso IV, da Resolução CGD/PR nº 42, de 23 de maio de 2024, compete ao Subcomitê de Segurança da Informação, vinculado ao CGD/PR, definir planos de ação, procedimentos operacionais ou ambos, voltados à gestão de riscos em segurança da informação, que:

I - sejam permanentes, direcionados e monitorados, bem como partes integrantes de todos os processos organizacionais e atividades da instituição;

II - observem o histórico dos eventos e suas consequências, bem como a imprevisibilidade de ocorrências para o tratamento dos riscos, de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade dos processos, serviços e informações institucionais;

III - considerem os fatores humanos e culturais da instituição para tratamento adequado dos riscos;

IV - considerem a interconectividade entre as pessoas, os processos e as informações; e

V - sejam alinhado à Instrução Normativa GSI/PR nº 3, de 2021.

### **Gestão de continuidade de negócios em segurança da informação**

Art. 66. Os órgãos integrantes da Presidência devem elaborar planos ou procedimentos de gestão de continuidade de negócios em segurança da informação, cumprindo os padrões e requisitos mínimos estabelecidos na Instrução Normativa GSI/PR nº 3, de 2021.

Art. 67. Os planos de que trata o art. 70 devem ser elaborados para:

I - identificar as potenciais ameaças à Presidência da República conforme o registro histórico, o contexto atual e a imprevisibilidade dos eventos;

II - preservar a continuidade das atividades críticas;

III - prever os impactos decorrentes de falhas desastres ou indisponibilidades nas atividades institucionais; e

IV - fornecer orientações e apoio nas ações de resposta e recuperação.

### **Monitoramento, auditoria e conformidade**

Art. 68. Os acessos aos ativos de informação e os eventos de segurança da informação devem ser adequadamente registrados e monitorados, por meio de mecanismos que assegurem o rastreamento, acompanhamento, controle e verificação, de forma a prevenir e detectar atividades não autorizadas, comportamentos anômalos e incidentes de segurança da informação, bem como permitir auditoria.

§1º Os registros serão armazenados e protegidos contra perda, destruição, falsificação e acesso não autorizado de acordo com legislação específica.

§2º Durante o monitoramento ou auditoria, caso sejam identificados comportamentos anômalos, vulnerabilidades ou suspeitas de incidentes de segurança da informação, estes devem ser reportados imediatamente ao Gestor de SI/PR.

Art. 69. Cabe à unidade responsável pela auditoria interna estabelecer planos de ação, procedimentos operacionais ou ambos, relacionados ao monitoramento de conformidade de segurança da informação, contemplando minimamente:

I - as unidades organizacionais abrangidas;

II - os aspectos para a verificação de conformidade;

III - os documentos necessários para a fundamentação de verificação de conformidade;

IV - as responsabilidades;

V - o parecer de conformidade e as recomendações.

Parágrafo único. A verificação da conformidade deverá ser realizada em intervalos regulares e de forma planejada.

Art. 70. Os resultados de ações de auditoria e conformidade devem ser documentados e encaminhados ao Gestor de SI/PR e ao CGD/PR, para ciência e tomada de decisão.

## CAPÍTULO V

### DAS PENALIDADES

Art. 71. As ações que violem esta Política ou quaisquer de suas diretrizes, planos ou procedimentos, ou que infrinjam controles de segurança da informação devem ser devidamente apuradas, sendo cabíveis as sanções administrativas, civis e penais aos responsáveis, nos termos da lei.

Art. 72. Em caso de caracterizada infração funcional por descumprimento desta Política, podem ser suspensas as permissões de acessos aos ativos de informação e aos recursos envolvidos até que o fato seja apurado ou solucionado.

Art. 73. As denúncias de violação a esta Política devem ser comunicadas ao Gestor de SI/PR.

Art. 74. A apuração de responsabilidade, dúvidas e casos omissos sobre responsabilização e penalidades serão tratados no âmbito da Corregedoria-Geral da Presidência da República.

## CAPÍTULO VI

### DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

#### **Vedações**

Art. 75. É vedada a disponibilização a pessoas não autorizadas de informações de identificação, autenticação e autorização baseadas em conta e senha ou em mecanismos de certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 76. Os usuários da informação no âmbito da Presidência da República são responsáveis por preservar a confidencialidade das informações acessadas no exercício de suas funções, sendo expressamente proibido o compartilhamento, divulgação ou repasse de qualquer dado sigiloso, restrito ou interno sem autorização formal.

Art. 77. Vulnerabilidades identificadas nos sistemas, equipamentos ou processos de informação devem ser comunicadas imediatamente às instâncias competentes, sendo expressamente proibida sua exploração, manipulação ou divulgação não autorizada.

#### **Revisão desta Política e normativos derivados**

Art. 78. Esta Política e os normativos dela decorrentes:

I - devem ser revisados sempre que houver mudanças significativas na estrutura da Presidência da República ou nos normativos e padrões nos quais ela se fundamenta, ou surgirem riscos relevantes à segurança da informação, não excedendo o período máximo de quatro anos; e

II - devem ser amplamente divulgados para todos usuários de informação dos órgãos integrantes da Presidência.

Art. 79. Os normativos relacionados à segurança da informação dos órgãos integrantes da

Presidência da República deverão, no prazo máximo de doze meses a contar da publicação desta Política, ser elaborados, quando inexistentes, ou ajustados, quando já existentes, de modo a garantir sua conformidade com as diretrizes estabelecidas nesta Política.

Art. 80. As dúvidas e os casos omissos em relação a esta Política serão dirimidos pelo Comitê de Governança Digital da Presidência da República.

### Revogação

Art. 81. Ficam revogadas as seguintes resoluções do CGD/PR:

I - Resolução nº 24, de 10 de junho de 2022;

II - Resolução nº 29, de 21 de julho de 2022;

III - Resolução nº 36, de 7 de novembro de 2022; e

IV - Resolução nº 37, de 7 de novembro de 2022.

### Vigência

Art. 82. Esta Resolução entra em vigor na data de sua publicação.

**MIRIAM BELCHIOR**

Presidenta do Comitê de Governança Digital e Segurança da Informação  
da Presidência da República



Documento assinado eletronicamente por **Miriam Belchior, Secretário(a)-Executivo(a)**, em 28/08/2025, às 21:14, 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 **6941454** e o código CRC **C17C9033** no site:

[https://protocolo.presidencia.gov.br/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://protocolo.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)