MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
Comitê de Governança Digital e Segurança da Informação

RESOLUÇÃO CONJUNTA CGDSI/CITARC/MGI Nº 1, DE 26 de junho de 2026

Dispõe sobre os processos relacionados à gestão de segurança da informação, no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos.

O **COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO DO MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS** , no uso das atribuições que lhe confere o art. 2º, *caput*, inciso I, da Portaria MGI nº 3.844, de 28 de julho de 2023, e o **COMITÊ DE INTEGRIDADE, TRANSPARÊNCIA, ACESSO À INFORMAÇÃO, RISCOS E CONTROLE**, no uso das atribuições que lhe confere o art. 2º, *caput,* inciso I, da Portaria GM/MGI nº 5.897, de 5 de outubro de 2023, e considerando o disposto na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, e na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025,

RESOLVEM:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução Conjunta dispõe sobre os processos relacionados à gestão de segurança da informação, no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos.

§ 1º O disposto nesta Resolução Conjunta aplica-se a órgãos específicos singulares e, no âmbito dos órgãos de assistência direta e imediata à Ministra, ao Gabinete e Secretaria-Executiva da estrutura do Ministério da Gestão e da Inovação em Serviços Públicos.

§ 2º Constituem os processos de que tratam esta Resolução:

I - processo de mapeamento de ativos de informação;

II - processo de gestão de riscos de segurança da informação;

III - processo de gestão de continuidade de negócios em segurança da informação;

IV - processo de gestão de mudanças nos aspectos de segurança da informação; e

V - processo de avaliação de conformidade de segurança da informação.

Art. 2º Esta resolução tem como objetivo estabelecer:

I - diretrizes complementares à Política de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos – POSI-MGI, à Política de Gestão de Riscos e Controles Internos, ao Sistema de Gestão de Riscos e Controles Internos do Ministério da Gestão e da Inovação em Serviços Públicos – PGRCI-MGI e à Política de Gestão de Continuidade de Negócios do Ministério da Gestão e da Inovação em Serviços Públicos – PGCN-MGI; e

II - diretrizes para a sistematização dos processos relacionados à gestão de segurança da informação nas unidades do Ministério da Gestão e da Inovação em Serviços Públicos, conforme disposto na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

Parágrafo único. Os processos de que trata esta Resolução devem ser executados em

conformidade com:

I - a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

II - o Programa de Privacidade e Segurança da Informação (PPSI 2.0), instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025;

III - a Política de Gestão de Continuidade de Negócios do Ministério da Gestão e da Inovação em Serviços Públicos, instituída pela Resolução CITARC/MGI nº 6, de 10 de abril de 2025;

IV - a Política de Gestão de Riscos e Controles Internos do Ministério da Gestão e da Inovação em Serviços Públicos, instituída pela Resolução CITARC/MGI nº 7, de 10 de abril de 2025; e

V - o Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação.

Art. 3º Os conceitos relacionados à temática desta Resolução poderão ser consultados no Glossário de Segurança da Informação, aprovado e atualizado por Portaria do Gabinete de Segurança Institucional da Presidência da República, e, adicionalmente:

I - unidade(s): unidade(s) administrativa(s) cujo titular seja ocupante de Cargo Comissionado Executivo de nível igual ou superior à CCE-17, ou equivalente, e no âmbito dos órgãos de assistência direta e imediata à Ministra, Secretaria-Executiva e Gabinete da Ministra, o qual representará as assessorias especiais a ele vinculadas.

CAPÍTULO II

DAS DIRETRIZES GERAIS

Art. 4º As unidades do Ministério da Gestão e da Inovação em Serviços Públicos que gerenciem ativos de informação deverão manter e implementar a gestão de segurança da informação de forma contínua, conforme preconiza a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

Art. 5º A gestão de segurança da informação no Ministério da Gestão e da Inovação em Serviços Públicos dar-se-á pela atuação direta:

I - da alta administração do Ministério da Gestão e da Inovação em Serviços Públicos;

II - do Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos, servidor designado pela alta administração do Órgão;

III - dos Gestores Setoriais de Segurança da Informação em cada unidade;

IV - dos agentes responsáveis pela gestão dos ativos de informação em cada unidade;

V - dos agentes responsáveis pela gestão de riscos de segurança da informação em cada unidade;

VI - dos agentes responsáveis pela gestão de mudança em cada unidade; e

VII - dos agentes responsáveis pela avaliação de conformidade de segurança da informação.

Parágrafo único. Os dirigentes máximos das unidades do Ministério da Gestão e da Inovação em Serviços Públicos que gerenciem ativos de informação deverão:

I - designar, no âmbito da unidade, Gestor Setorial de Segurança da Informação; e

II - encaminhar para ciência do Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos, por meio de ofício, nome e dados de contato do Gestor Setorial de Segurança da Informação e dos agentes responsáveis de seus respectivos processos relacionados à gestão de segurança da informação.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 6º Cabe ao Gestor Setorial de Segurança da Informação, no âmbito de sua unidade:

I - coordenar:

a) o processo de mapeamento de ativos de informação;

b) o processo de gestão de riscos de segurança da informação;

c) o processo de gestão de continuidade de negócios em segurança da informação; e

d) o processo de gestão de mudanças nos aspectos de segurança da informação;

II - designar:

a) o agente responsável pela gestão dos ativos de informação;

b) o agente responsável pela gestão de riscos de segurança da informação;

c) o agente responsável pela gestão de continuidade de negócios em segurança da informação; e

d) o agente responsável pela gestão de mudança nos aspectos de segurança da informação.

III - aprovar e encaminhar ao Gestor de Segurança da Informação:

a) o plano de gestão de riscos de segurança da informação;

b) o relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

c) o relatório de tratamento de riscos de segurança da informação.

IV - analisar e encaminhar ao Gestor de Segurança da Informação:

a) o plano de gestão de continuidade de negócios em segurança da informação de sua unidade; e

b) o documento de avaliação e aprovação de mudança de sua unidade, nos aspectos de segurança da informação;

V - proporcionar a interação constante entre o agente responsável pela gestão de ativos de informação, o agente responsável pela gestão de riscos de segurança da informação, o agente responsável pela gestão de continuidade de negócios em segurança da informação e o agente responsável pela gestão de mudanças em aspectos de segurança da informação;

VI - fornecer ao(s) agente(s) responsável(is) pela avaliação de conformidade de segurança da informação, todas as informações necessárias ao processo de gestão de conformidade no que diz respeito aos aspectos de segurança da informação;

VII - apoiar o Gestor de Segurança da Informação na elaboração do parecer técnico sobre o relatório de avaliação de conformidade de segurança da informação; e

VIII - adotar, no âmbito de sua unidade, as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade de segurança da informação aprovado pela alta administração.

Parágrafo único. A designação de que trata o inciso II do *caput* será de titulares e suplentes, dentre os agentes públicos em exercício na unidade.

Art. 7º Cabe ao Gestor de Segurança da Informação, no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos:

I - acompanhar:

a) o processo de mapeamento de ativos de informação;

b) o processo de gestão de riscos de segurança da informação;

c) o processo de gestão de continuidade de negócios em segurança da informação; e

d) o processo de gestão de mudanças nos aspectos de segurança da informação;

II - aprovar, consolidar e encaminhar para a alta administração:

a) o plano de gestão de riscos de segurança da informação;

b) o relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

c) o relatório de tratamento de riscos de segurança da informação;

III - analisar, consolidar e encaminhar para a alta administração:

a) o documento de avaliação e aprovação de mudança nos aspectos de segurança da informação; e

b) o relatório de avaliação de conformidade de segurança da informação;

IV - propor medidas preventivas à alta administração relacionadas aos riscos de segurança da informação;

V - emitir parecer técnico sobre o relatório de avaliação de conformidade de segurança da informação e apresentá-lo ao Comitê de Governança Digital e Segurança da Informação;

VI - adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade de segurança da informação aprovado pela alta administração;

VII - proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação; e

VIII - elaborar e publicar, anualmente, relatório consolidado de gestão de segurança da informação contendo, no mínimo:

a) percentual de unidades com os processos de segurança da informação implementados e em operação;

b) evolução do nível de maturidade em segurança da informação, conforme critérios do PPSI;

c) principais riscos de segurança da informação tratados, com descrição das ações de mitigação adotadas;

d) incidentes de segurança da informação registrados, classificados por gravidade e tipo; e

e) lições aprendidas e recomendações para melhoria contínua.

§ 1º O Gestor de Segurança da Informação apoiará as unidades do Ministério da Gestão e da Inovação em Serviços Públicos na elaboração dos planos, relatórios e demais documentos previstos nesta Resolução.

§ 2º O relatório de que trata o inciso VIII do *caput* será encaminhado ao Comitê de Governança Digital e Segurança da Informação e ao Comitê de Integridade, Transparência, Acesso à Informação, Riscos e Controle para ciência e adoção de providências, quando cabível.

§ 3º As unidades do Ministério da Gestão e da Inovação em Serviços Públicos deverão fornecer, tempestivamente, as informações necessárias à consolidação do relatório previsto no inciso VIII do *caput*.

Art. 8º Cabe ao ao(s) agente(s) responsável(is) pela avaliação de conformidade elaborar o relatório de avaliação de conformidade e remetê-lo ao gestor de segurança da informação.

Parágrafo único. Para fins desta Resolução Conjunta, a Assessoria Especial de Controle Interno – AECI atuará como agente responsável pela avaliação de conformidade nos termos do art. 12 da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.

Art. 9º Cabem aos agentes responsáveis citados no art. 6º, inciso II, respectivamente aos

processos em que atuam, as responsabilidades constantes na Instrução Normativa GSI/PR nº 3, de 2021.

Art. 10. Cabe ao Gestor de Tecnologia da Informação colaborar e fornecer os subsídios necessários ao Gestor de Segurança da Informação para a execução de suas competências.

Art. 11. Cabe à alta administração do órgão, representada pelo Comitê de Governança Digital e Segurança da Informação:

I - aprovar o relatório de avaliação de conformidade, bem como todo o processo de avaliação de conformidade de segurança da informação, e devolvê-lo ao Gestor de Segurança da Informação para adoção das providências cabíveis;

II - analisar o relatório de identificação, análise e avaliação dos riscos de segurança da informação, e deliberar sobre as medidas preventivas propostas pelo Gestor de Segurança da Informação;

III - apreciar o documento de avaliação e aprovação de mudança, à quem cabe a decisão de aprovar ou indeferir a mudança; e

IV - promover ações de capacitação continuada relacionada aos processos da gestão de segurança da informação, para:

a) gestores de Tecnologia da Informação;

b) gestores setoriais de Segurança da Informação;

c) agentes responsáveis pela gestão de ativos, riscos, mudança e continuidade;

d) servidores com acesso a ativos críticos de informação;

e) agentes responsáveis pela avaliação de conformidade, visando ao aperfeiçoamento de seus conhecimentos sobre a legislação vigente relativa à segurança da informação; e

f) demais servidores e colaboradores, na temática de boas práticas de segurança da informação.

Parágrafo único. A designação a que se refere o inciso I do *caput* não poderá recair sobre membros da equipe de gestão de segurança da informação do órgão ou das unidades.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 12. A gestão de segurança da informação, regida por esta Resolução, deverá observar as boas práticas relacionadas ao tema e seguir as diretrizes e normas de segurança da informação emanadas pelo Gabinete de Segurança da Informação da Presidência da República, bem como observar as orientações expedidas pelo Órgão Central do SISP.

§ 1º Para a implementação do processo de gestão de risco de segurança da informação – PGRSI recomenda-se a utilização do Processo de Gestão de Riscos de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos aprovado no âmbito do Comitê de Governança Digital e Segurança da Informação e do Comitê de Integridade, Transparência, Acesso à Informação, Riscos e Controle.

§ 2º Quando o contexto da análise e avaliação de riscos de segurança da informação envolver ativos relacionados a processos que realizem tratamento de dados pessoais, deve ser realizada a análise de alto risco disponibilizada na ferramenta ColaboraDap.

§ 3º O resultado da análise de alto risco indicará a eventual necessidade de elaboração do Relatório de Impacto à Proteção de Dados Pessoais – RIPD, conforme previsto na Política de Proteção de Dados Pessoais do Ministério.

Art. 13. O sistema de Tecnologia da Informação estabelecido para a gestão de riscos e integridade do Ministério da Gestão e da Inovação em Serviços Públicos, disponibilizado aos órgãos e

entidades do Ministério como apoio às atividades de gerenciamento dos riscos, será preferencialmente utilizado na gestão de riscos de segurança da informação.

§ 1º A ferramenta de que trata o *caput* observará, preferencialmente:

I - interoperabilidade com o Sistema Eletrônico de Informações – SEI e com plataformas do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP;

II - acessibilidade conforme os padrões do Modelo de Acessibilidade em Governo Eletrônico – e-MAG;

III - registro de trilha de auditoria (log) para fins de conformidade e apuração de responsabilidades; e

IV - possibilidade de extração de relatórios gerenciais em formatos abertos.

§ 2º Os colaboradores que atuam no processo de gestão de riscos de segurança da informação deverão ser continuamente capacitados, visando ao aperfeiçoamento de seus conhecimentos sobre gestão de riscos relativa à segurança da informação e à consolidação da sua cultura.

Art. 14. O Plano de continuidade de negócios das unidades do Ministério da Gestão e da Inovação em Serviços Públicos deverão contemplar o processo de gestão de continuidade de negócios em segurança da informação, como previsto na Instrução Normativa GSI/PR nº 3, de 2021.

Art. 15. Esta Resolução será revisada a cada dois anos pelo Comitê de Governança Digital e Segurança da Informação e pelo Comitê de Integridade, Transparência, Acesso à Informação, Riscos e Controle, ouvidas as unidades executoras, para avaliação de sua eficácia, pertinência frente ao cenário de ameaças cibernéticas e adequação à evolução normativa federal e interna.

Parágrafo único. A revisão de que trata o *caput* poderá resultar em proposta de alteração, consolidação ou revogação desta Resolução.

Art. 16. As unidades do Ministério da Gestão e da Inovação em Serviços Públicos terão seis meses, a contar do início da vigência desta Resolução, para se adaptar às diretrizes nela estabelecidas.

Parágrafo único. As unidades que já possuam processos de segurança da informação implementados poderão aproveitar integralmente ou parcialmente os trabalhos já realizados, desde que demonstrada a conformidade com as diretrizes estabelecidas nesta Resolução, mediante parecer técnico do Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos.

Art. 17. O Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos poderá especificar os aspectos operacionais desta Resolução, especialmente no que concerne aos modelos de documentos, fluxos de aprovação e integração com ferramentas institucionais.

Art. 18. Esta Resolução entra em vigor na data de sua publicação.

Documento assinado eletronicamente

ROGÉRIO GABRIEL NOGALHA DE LIMA

Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos

Coordenador do Comitê de Governança Digital e Segurança da Informação

Documento assinado eletronicamente

FRANCISCO EDUARDO DE HOLANDA BESSA

Presidente do Comitê de Integridade, Transparência, Acesso à Informação, Riscos e Controle

Documento assinado eletronicamente por **Francisco Eduardo de Holanda Bessa**, **Presidente(a) de Comitê**, em 26/06/2026, às 17:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Rogério Gabriel Nogalha de Lima**, **Diretor(a)**, em 29/06/2026, às 11:07, 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 deste documento pode ser conferida no site https://colaboragov.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **62383683** e o código CRC **A7F22963**.