DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/01/2026 | Edição: 11 | Seção: 1 | Página: 43

Órgão: Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Serviços Compartilhados

PORTARIA SSC/MGI Nº 202, DE 15 DE JANEIRO DE 2026

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério da Gestão e da Inovação em Serviços Públicos - ETIR-MGI

A SECRETÁRIA DE SERVIÇOS COMPARTILHADOS SUBSTITUTA DO MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, , no uso das atribuições que lhe confere o art. 18, parágrafo único, da Portaria MGI nº 10.033, de 29 de dezembro de 2025, e tendo em vista o disposto no Decreto nº 12.572, de 4 de agosto de 2025, no Decreto nº 12.573, de 4 de agosto de 2025, no Decreto nº 11.837, de 21 de dezembro de 2023, no art. 22 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e na Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Objeto

Art. 1º Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério da Gestão e da Inovação em Serviços Públicos - ETIR-MGI.

Missão

Art. 2º A missão da ETIR-MGI é estruturar a prevenção, o tratamento e a resposta do Ministério da Gestão e da Inovação em Serviços Públicos contra ataques cibernéticos aos ativos de informação sob a sua gestão, de modo a maximizar a prevenção e minimizar o tempo de resolução de incidentes cibernéticos, de forma compartilhada e conjunta.

§1º A ETIR-MGI atuará na infraestrutura computacional e nos ativos de informação do Ministério da Gestão e da Inovação em Serviços Públicos e dos demais órgãos solicitantes do Centro de Serviços Compartilhados - ColaboraGov, de que trata o Decreto nº 11.837, de 21 de dezembro de 2023, gerenciados pela Diretoria de Tecnologia da Informação da Secretaria de Serviços Compartilhados.

§ 2º O gestor responsável por sistemas ou serviços de tecnologia da informação poderá atuar em conjunto com a ETIR-MGI sempre que o incidente cibernético envolver diretamente os ativos sob sua responsabilidade, para prestar apoio técnico e gerencial, fornecer informações relevantes, colaborar na definição de medidas corretivas e acompanhar a implementação das ações necessárias, de forma a assegurar a efetividade da resposta e a continuidade dos serviços afetados.

Definições

Art. 3º Para os fins do disposto nesta Portaria, consideram-se:

I - Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br - unidade de coordenação operacional das equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades integrantes do Sistema de Administração de Recursos de Tecnologia da Informação - SISP, de que trata o Decreto nº 7.579, de 11 de outubro de 2011;

II - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov - unidade do Departamento de Segurança Cibernética da Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional da Presidência da República com a atribuição de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

III - Agente Responsável pela ETIR-MGI - servidor público efetivo que coordenará a ETIR-MGI;

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

V - incidente cibernético - ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

VI - órgão correlato - unidades desconcentradas e formalmente constituídas de administração dos recursos de tecnologia da informação, integrante SISP; e

VII - usuário de informação - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO II

DA ORGANIZAÇÃO E FUNCIONAMENTO DA ETIR-MGI

Objetivos

Art. 4º São objetivos da ETIR-MGI:

I - manter um canal de compartilhamento de informações, ágil e de fácil acesso com as equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos solicitantes do ColaboraGov;

II - promover junto à área de comunicação da Secretaria de Serviços Compartilhados campanhas de prevenção a ataques cibernéticos e a divulgação de contatos para notificação de incidentes cibernéticos à ETIR-MGI;

III - definir um fluxo simplificado de resolução de incidentes cibernéticos, com identificação de responsáveis;

IV - divulgar um canal simplificado de comunicação de incidentes cibernéticos acessível aos usuários de informação;

V - realizar auditorias internas periódicas para identificar vulnerabilidades e ameaças que possam comprometer os negócios do Ministério da Gestão e da Inovação em Serviços Públicos; e

VI - acompanhar a implementação de controles de privacidade e segurança da informação e sensibilizar de forma contínua a Estrutura de Governança do Programa de Privacidade e Segurança da Informação - PPSI, de que trata a Portaria SGD/MGI nº 852, de 28 de março de 2023.

Público-alvo

Art. 5º O público-alvo das atividades pertinentes à ETIR-MGI são os usuários de informação do Ministério da Gestão e da Inovação em Serviços Públicos e dos órgãos solicitantes do ColaboraGov enquanto usuários dos ativos de informação geridos pela Diretoria de Tecnologia da Informação.

Parágrafo único. Os incidentes de segurança que envolvam sistemas não atendidos pela ETIR-MGI, serão comunicados aos órgãos gestores para providências

Art. 6º Os usuários de informação do Ministério da Gestão e da Inovação em Serviços Públicos poderão enviar notificações acerca de incidentes de segurança à ETIR-MGI, através dos canais disponibilizados na página de segurança da informação na intranet.

Parágrafo único. Serão automaticamente rejeitadas as notificações recebidas pela ETIR-MGI que não configurem incidentes de segurança, de que trata o caput.

Modelo de atuação

Art. 7º As atividades da ETIR-MGI enquadram-se no modelo de atuação singular, uma vez que presta serviço apenas ao seu público-alvo, no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos e do ColaboraGov.

Modelo de implementação

Art. 8º A ETIR-MGI adotará o modelo de implementação de que trata o item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, e será composta pelas pessoas representantes dos órgãos a que se refere o art. 9º.

§ 1º As pessoas representantes da ETIR-MGI desempenharão as atividades relacionadas à prevenção, ao tratamento e à resposta a incidentes cibernéticos, sem prejuízo das atribuições legais.

§ 2º As funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por especialistas em segurança da informação.

Estrutura Organizacional

Art. 9º A ETIR-MGI tem a seguinte composição:

I - autoridade titular da Coordenação de Segurança em Tecnologia da Informação da Coordenação-Geral de Segurança, Recursos e Infraestrutura Tecnológica da Diretoria de Tecnologia da Informação da Secretaria de Serviços Compartilhados do Ministério da Gestão e da Inovação em Serviços Públicos, que atuará como Agente Responsável pela ETIR-MGI;

II - pessoas representantes da Coordenação de Segurança em Tecnologia da Informação; e

III - pessoas representantes dos órgãos correlatos do SISP no Ministério da Gestão e da Inovação em Serviços Públicos, de que trata a Resolução CGDSI /MGI nº 4, de 2 de maio de 2024:

a) uma da Diretoria de Inovação e Inteligência em Gestão de Estatais da Secretaria de Coordenação e Governança das Empresas Estatais;

b) uma da Coordenação-Geral de Tecnologia da Informação da Diretoria de Gestão Interna do Arquivo Nacional;

c) um da Diretoria de Modernização e Inovação da Secretaria do Patrimônio da União;

d) um da Diretoria de Soluções Digitais da Secretaria de Gestão de Pessoas; e

e) uma da Secretaria de Gestão e Inovação.

§ 1º Cada pessoa representante da ETIR-MGI terá uma suplência, que a substituirá em suas ausências e seus impedimentos.

§ 2º As pessoas representantes da ETIR-MGI de que tratam os incisos II e III do caput serão escolhidas, preferencialmente, dentre servidores públicos efetivos com capacitação técnica compatível com as atividades da equipe.

§ 3º As pessoas representantes da ETIR-MGI de que tratam os incisos II e III do caput serão indicadas pelas autoridades titulares dos órgãos que representam e designadas em ato da autoridade titular da Diretoria de Tecnologia da Informação da Secretaria de Serviços Compartilhados.

§ 4º As pessoas representantes da ETIR-MGI de que tratam os incisos II e III do caput atuarão na ETIR, conforme perfil técnico, atuarão, preferencialmente, nas seguintes áreas:

I - suporte operacional de tecnologia da informação;

II - monitoramento e produção de tecnologia da informação;

III - desenvolvimento de sistemas;

IV - infraestrutura de tecnologia da informação;

V - estratégia de Segurança de tecnologia da informação;

VI - resposta a incidentes cibernéticos; e

VII - gestão de riscos cibernéticos.

Art. 10. A participação na ETIR-MGI será considerada serviço público relevante, não remunerada.

Art. 11. O processo de gestão de incidentes a ser definido pela ETIR-MGI será apoiado com prioridade pelas unidades da Diretoria de Tecnologia da Informação.

Parágrafo único. A autoridade titular da Diretoria de Tecnologia da Informação poderá designar servidores públicos da Diretoria para atuar em demandas específicas de tratamento e resposta a incidentes cibernéticos, sem prejuízo das atribuições legais, em conjunto com as pessoas representantes da ETIR-MGI.

Art. 12. O Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos, designado nos termos da Portaria MGI nº 3.844, de 28 de julho de 2023, poderá solicitar a designação de servidores públicos lotados ou em exercício em órgãos de assistência direta e imediata e órgãos específicos singulares da estrutura regimental do Ministério da Gestão e da Inovação em Serviços Públicos para atuar em incidente cibernético, sem prejuízo das atribuições legais, em conjunto com as pessoas representantes da ETIR-MGI.

Art. 13. As atividades de prevenção, tratamento e resposta a incidentes cibernéticos, no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos, poderão ser exercidas parcialmente por empresas contratadas que prestam serviço de tecnologia da informação, desde que justificado em parecer técnico pelo Agente Responsável pela ETIR-MGI.

Art. 14. ETIR-MGI observará os normativos, padrões e procedimentos técnicos exarados pelo CTIR Gov.

Parágrafo único. A ETIR-MGI poderá adotar as melhores práticas de mercado para a execução de suas atividades, desde que não conflitem com a legislação em vigor, em especial, os atos normativos de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos, do Gabinete de Segurança da Informação da Presidência da República e os padrões e orientações do órgão central do SISP, do CTIR Gov e do CISC Gov.br.

Atribuições e competências

Art. 15. São atribuições do Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos:

I - acompanhar os trabalhos da ETIR-MGI;

II - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação realizados pela ETIR-MGI;

III - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

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

Art. 16. São atribuições do Agente Responsável pela ETIR-MGI:

I - coordenar as atividades da ETIR-MGI;

II - estabelecer os procedimentos internos da ETIR-MGI;

III - realizar a comunicação com o CTIR Gov, o CISC gov.br e o Encarregado pelo Tratamento de Dados Pessoais do Ministério da Gestão e da Inovação em Serviços Públicos, quando necessário;

IV - apresentar os resultados das atividades da ETIR-MGI ao Gestor de Segurança da Informação do Ministério; e

V - apresentar estudos e parecer técnico sobre as necessidades da ETIR-MGI para o cumprimento da missão e dos objetivos definidos.

Art. 17. À ETIR-MGI compete:

I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no Ministério da Gestão e da Inovação em Serviços Públicos;

II - monitorar as redes computacionais;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação;

V - identificar vulnerabilidades e artefatos maliciosos;

VI - recuperar sistemas de informação;

VII - promover a cooperação com outras equipes, bem como participar de fóruns e redes relativas à segurança da informação;

VIII - apoiar a condução de políticas de segurança cibernética e da informação;

IX - realizar ações voltadas para o fortalecimento da resiliência cibernética do Ministério da Gestão e da Inovação em Serviços Públicos;

X - comunicar ao CTIR Gov e ao CISC Gov.br a ocorrência de incidentes cibernéticos com a maior brevidade possível; e

XI - manter registro histórico de incidentes cibernéticos e vulnerabilidades que permitam a geração de dados estatísticos.

Autonomia

Art. 18. A ETIR-MGI possui autonomia operacional.

§ 1º Ao Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos compete a tomada de decisão sobre quais medidas devem ser adotadas referentes às atividades de prevenção, tratamento e resposta a incidentes cibernéticos relacionados aos ativos de informação gerenciados pela Diretoria de Tecnologia da Informação da Secretaria de Serviços Compartilhados.

§ 2º A ETIR-MGI participará do processo de decisão recomendando os procedimentos, medidas e ações a serem executados para o tratamento e a recuperação durante um incidente cibernético, bem como indicando as repercussões se as recomendações não forem seguidas.

§ 3º O Gestor de Segurança da Informação poderá compartilhar o processo de tomada de decisão de que trata o § 1º com a ETIR-MGI.

§ 4º Nas ausências ou impedimentos do Gestor de Segurança da Informação, compete ao substituto legal a tomada de decisão de que trata o § 1º.

§ 5º Durante um incidente cibernético, se justificado tecnicamente, a ETIR-MGI poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

Art. 19. O acionamento da ETIR-MGI e o processo de gestão de incidentes cibernéticos serão definidos em ato do Gestor de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos.

Serviços Prestados pela ETIR-MGI

Art. 20. A ETIR-MGI prestará os seguintes serviços:

I - Serviço de Monitoramento e Detecção, com o objetivo de realizar o monitoramento contínuo de eventos e indicadores de segurança, a fim de identificar potenciais incidentes cibernéticos em tempo hábil;

II - Serviço de Análise de incidentes, com o objetivo de conduzir a análise técnica e a classificação dos incidentes reportados, identificando sua origem, impacto, abrangência e criticidade;

III - Serviço de Resposta e Contenção, com o objetivo de atuar na coordenação e execução das medidas necessárias para contenção, erradicação e mitigação dos efeitos dos incidentes de segurança; e

IV - Serviço de Gestão do Conhecimento, com o objetivo de manter uma base de dados atualizada com informações sobre incidentes, vulnerabilidades e lições aprendidas, de forma a apoiar a tomada de decisão estratégica.

CAPÍTULO III

DISPOSIÇÕES FINAIS

Revogação

Art. 21. Fica revogada a Portaria SGC/ME nº 8.554, de 26 de setembro de 2022.

Vigência

Art. 22. Esta Portaria entra em vigor na data de sua publicação.

LUCÍOLA MAURÍCIO DE ARRUDA

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/01/2026 | Edição: 11 | Seção: 1 | Página: 40

Órgão: Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital

INSTRUÇÃO NORMATIVA SGD/MGI Nº 4, DE 14 DE JANEIRO DE 2026

Dispõe sobre o ciclo de implementação de 2026 do framework do Programa de Privacidade e Segurança da Informação - PPSI no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional que possuem unidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal.

A SECRETÁRIA DE GOVERNO DIGITAL SUBSTITUTA DO MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, no uso da competência que lhe foi subdelegada pelo art. 11 da Portaria MGI nº 572, de 8 de março de 2023, publicada no Diário Oficial da União de 9 de março de 2023, e nas atribuições que lhe conferem o art. 23, caput, inciso VI, do Anexo I ao Decreto nº 12.102, de 8 de julho de 2024, o art. 3º, caput, inciso VI, do Decreto nº 12.198, de 24 de setembro de 2024, e o art. 4º, caput, incisos I, IV e V do Decreto nº 7.579, de 11 de outubro de 2011, e tendo em vista o disposto na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, resolve:

Objeto e âmbito de aplicação

Art. 1º Esta Instrução Normativa dispõe sobre o ciclo de implementação de 2026 do framework do Programa de Privacidade e Segurança da Informação - PPSI no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional que possuem unidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal.

Definições

Art. 2º Para os fins do disposto nesta Instrução Normativa, consideram-se:

I - diagnóstico: avaliação conduzida pelo órgão ou entidade, destinada a aferir o nível de implementação das medidas do framework do PPSI;

II - plano de trabalho: instrumento tático de planejamento da implementação das medidas de privacidade e de segurança da informação;

III - ciclos de implementação: ciclos anuais de priorização incremental de medidas, estruturados para promover a maturidade em privacidade e segurança da informação, por meio da execução das etapas do framework do PPSI, de que trata o art. 15 da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025;

IV - gestão contínua: processo continuado destinado a monitorar, revisar e adequar o nível de implementação das medidas priorizadas, assegurando sua efetividade frente a necessidades tecnológicas, organizacionais ou normativas;

V - maturidade em privacidade e segurança da informação: estágio em que o órgão ou entidade encontra-se quanto ao nível de implementação de um conjunto específico de medidas estabelecidas no framework do PPSI;

VI - Nível de Adoção do Controle - NAC: grau de adoção de um controle em escala nominal, determinado a partir da média da pontuação do nível de implementação das medidas contidas no controle, na forma do Anexo III; e

VII - Nível de Implementação da Medida - NIM: grau de implementação de uma medida em escala nominal, com respectiva pontuação, considerando o seu propósito e escopo de aplicação no framework do PPSI, na forma do Anexo II.

Informações sobre serviços prestados por órgãos ou entidades provedores

Art. 3º Caso haja prestação de serviços a órgãos ou entidades por integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, os órgãos ou entidades provedores deverão prestar as informações essenciais à execução das etapas do framework do PPSI aos respectivos órgãos ou entidades providos.

Das medidas a serem adotadas pelos órgãos e entidades

Art. 4º Os órgãos e entidades de que trata o art. 1º deverão adotar as medidas prioritárias e as medidas de gestão contínua de que trata o Anexo I.

Parágrafo único. O órgão ou entidade de que trata o art. 1º poderá implementar outras medidas não priorizadas no ciclo de implementação de 2026 do framework do PPSI.

Art. 5º A Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos disponibilizará ferramenta para preenchimento, pelos órgãos e entidades, de informações relativas:

I - à estrutura de governança do PPSI, de que trata o art. 7º da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025; e

II - ao ciclo de implementação de 2026 do framework do PPSI.

Parágrafo único. Os órgãos e entidades deverão manter atualizadas as informações dispostas nos incisos I e II do caput.

Do diagnóstico e do plano de trabalho

Art. 6º O diagnóstico e o plano de trabalho resultante da etapa de planejamento do PPSI deverão ser encaminhados à Secretaria de Governo Digital, exclusivamente por meio da ferramenta de que trata o art. 5º, até 27 de fevereiro de 2026.

§ 1º Para registro do diagnóstico na ferramenta de que trata o caput, deverá ser indicado o nível de implementação de cada medida constante do framework do PPSI, observado o disposto no Anexo II.

§ 2º Na hipótese de a medida possibilitar a indicação de "Não se aplica", o órgão ou entidade que consignar tal opção para a medida deverá registrar na ferramenta a justificativa para a não aplicabilidade.

§ 3º Após o preenchimento dos níveis de implementação de que trata o § 1º, a ferramenta apresentará, automaticamente, o NAC.

§ 4º Os órgãos e entidades de que trata o art. 1º deverão indicar, no plano de trabalho a que se refere o caput, as datas inicial e final planejadas para o atingimento do nível de implementação aprimorado das medidas de que tratam os Anexos I e II.

§ 5º A data final indicada pelo órgão ou entidade para algumas das ações decorrentes do plano de trabalho a que se refere o § 3º poderá ultrapassar o ano de 2026, devendo ser registrada a respectiva justificativa na ferramenta.

Dos indicadores de maturidade

Art. 7º Ficam instituídos os seguintes indicadores:

I - iBase: indicador usado para aferir a maturidade relacionada às medidas de estruturação básica para governança e de instrumentos fundamentais de privacidade e segurança da informação do órgão ou entidade;

II - iSeg: indicador usado para aferir a maturidade relacionada às medidas de segurança da informação do órgão ou entidade; e

III - iPriv: indicador usado para aferir a maturidade relacionada às medidas de privacidade do órgão ou entidade.

§ 1º A aferição dos indicadores de maturidade iBase, iSeg e iPriv será realizada conforme disposto no Anexo IV.

§ 2º O cálculo dos indicadores de que tratam os incisos I, II, e III do caput será realizado automaticamente pela ferramenta após o preenchimento dos níveis de implementação de todas as medidas do respectivo indicador.

Disposições finais

Art. 8º A Secretaria de Governo Digital realizará o monitoramento contínuo do ciclo de implementação de 2026 do framework do PPSI.

§ 1º As informações do diagnóstico e do plano de trabalho decorrentes da etapa de planejamento do PPSI poderão ser atualizadas na ferramenta a qualquer tempo pelos órgãos e entidades de que trata o art. 1º, sendo obrigatória a atualização nos meses de julho e dezembro de 2026.

§ 2º Na hipótese de a Secretaria de Governo Digital identificar necessidade de atualização das informações, o órgão ou entidade de que trata o art. 1º será comunicado para proceder à atualização na ferramenta.

Art. 9º Esta Instrução Normativa entra em vigor na data de sua publicação.

LUANNA SANT'ANNA RONCARATTI

ANEXO I

MEDIDAS DO CICLO DE 2026

a) MEDIDAS PRIORIZADAS PARA O CICLO DE IMPLEMENTAÇÃO DE 2026

Tabela 1 - Medidas priorizadas para o ciclo de implementação de 2026

Segmento	Controle	Medidas
BASE	0 - ESTRUTURAÇÃO BÁSICA PARA GOVERNANÇA	0.1 0.5 0.7
	0 - INSTRUMENTOS FUNDAMENTAIS	0.9 0.13 0.14 0.15 0.16 0.17
SEGURANÇA DA INFORMAÇÃO	3 - PROTEÇÃO DE DADOS	3.7 3.8 3.9 3.11 3.12
	5 - GESTÃO DE CONTAS	5.5 5.6
	6 - GESTÃO DE ACESSO	6.7 6.8
	8 - GESTÃO DE REGISTROS DE AUDITORIA	8.5 8.9 8.12
	12 - GESTÃO DA INFRAESTRUTURA DE REDE	12.2
	13 - MONITORAMENTO E DEFESA DA REDE	13.1
	14 - CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS	14.9
	15 - GESTÃO DE PROVEDOR DE SERVIÇOS	15.2 15.3 15.4 15.5 15.6 15.7
	16 - SEGURANÇA DE APLICAÇÕES	16.4 16.9 16.13
	17 - GESTÃO DE INCIDENTES	17.5 17.6
	18 - TESTES DE INTRUSÃO	18.1

PRIVACIDADE	19 - REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS	19.1 19.2 19.3 19.4
	20 - AÇÕES DE PREVENÇÃO	20.1 20.2 20.3 20.4
	21 - ENCARREGADO E DIREITOS DOS TITULARES	21.1 21.2 21.3 21.4 21.5 21.6
	22 - CONTRATOS, ACORDOS E INSTRUMENTOS CONGÊNERES	22.1 22.2 22.3 22.4
	23 - ANÁLISE DAS OPERAÇÕES DE TRATAMENTO	23.1 23.2 23.3 23.4 23.5 23.6 23.7
	24 - COMPARTILHAMENTO E TRANSFERÊNCIA INTERNACIONAL	24.1 24.2 24.3 24.4 24.5
	25 - PRINCÍPIOS DA LGPD	25.1
		25.2
		25.3
		25.4
		25.5
		25.6
		25.7
		25.8
		25.9
		25.10

b) MEDIDAS DE GESTÃO CONTÍNUA

Tabela 2 - Medidas de gestão contínua

Segmento	Controle	Medidas
BASE	0 - ESTRUTURAÇÃO BÁSICA PARA GOVERNANÇA	0.2 0.3 0.4 0.6 0.8
	0 - INSTRUMENTOS FUNDAMENTAIS	0.10 0.11 0.12
SEGURANÇA DA INFORMAÇÃO	1 - INVENTÁRIO DE ATIVOS INSTITUCIONAIS	1.1 1.2
	2 - INVENTÁRIO DE SOLUÇÕES DE SOFTWARE	2.1 2.2 2.3 2.4

	3 - PROTEÇÃO DE DADOS	3.1 3.2 3.3 3.4
		3.5 3.6 3.10 3.14
	4 - CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOLUÇÕES DE SOFTWARE	4.1 4.2 4.3 4.4 4.5 4.6 4.7
	5 - GESTÃO DE CONTAS	5.1 5.2 5.3 5.4
	6 - GESTÃO DE ACESSO	6.1 6.2 6.3 6.4 6.5 6.6
	7 - GESTÃO CONTÍNUA DE VULNERABILIDADES	7.1 7.2 7.3 7.4 7.7
	8 - GESTÃO DE REGISTROS DE AUDITORIA	8.1 8.2 8.3 8.4 8.6 8.10
	9 - PROTEÇÕES DE E-MAIL E NAVEGADOR WEB	9.1 9.2
	10 - DEFESAS CONTRA*MALWARE*	10.1 10.2 10.3
	11 - RECUPERAÇÃO DE DADOS	11.1 11.2 11.3 11.4 11.5
	12 - GESTÃO DA INFRAESTRUTURA DE REDE	12.1 12.4
	14 - CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS	14.1 14.2 14.3 14.4
		14.5 14.6 14.7 14.8
	15 - GESTÃO DE PROVEDOR DE SERVIÇOS	15.1
	16 - SEGURANÇA DE APLICAÇÕES	16.8
	17 - GESTÃO DE INCIDENTES	17.1 17.2 17.3 17.4

ANEXO II

NÍVEIS DE IMPLEMENTAÇÃO DAS MEDIDAS

a) NÍVEIS DE IMPLEMENTAÇÃO DAS MEDIDAS AVALIADAS DE FORMA GRADUAL

Tabela 3 - Níveis de implementação das medidas avaliadas de forma gradual e respectivas pontuações

Nível	Descrição	Pontuação
0 - Não se aplica	A medida não se aplica.	-
1 - Não adota ou há decisão formal	A medida é aplicável, mas não é implementada ou existe apenas um planejamento ou decisão formal para implementá-la.	0,00
2 - Inicial	A implementação da medida atende menos de 40% do seu propósito.	0,25
3 - Intermediário	A implementação da medida atende entre 40% e 80% do seu propósito.	0,50
4 - Completo	A implementação da medida atende mais de 80% do seu propósito.	0,75
5 - Aprimorado	A implementação da medida atende mais de 80% do seu propósito e é monitorada e revisada continuamente de forma sistemática, com base em métricas quantitativas, possuindo mecanismos que garantem uma implementação consistente ao longo do tempo.	1,00

b) NÍVEIS DE IMPLEMENTAÇÃO DAS MEDIDAS AVALIADAS DE FORMA BINÁRIA

Tabela 4 - Níveis de implementação das medidas avaliadas de forma binária e respectivas pontuações

Nível	Descrição	Pontuação
0 - Não se aplica	A medida não se aplica.	-
1 - Não	A medida é aplicável, mas não é implementada ou existe apenas um planejamento ou decisão formal para implementá-la.	0,00
2 - Sim	Medida integralmente implementada.	1,00 ANEXO III AFERIÇÃO DOS NÍVEIS DE ADOÇÃO DOS CONTROLES (NAC) a) FÓRMULA DE CÁLCULO DO NÍVEL DE ADOÇÃO DO CONTROLE (NAC): $NAC_c = \frac{\sum_{med=1}^{n_{m,c}} NIM_{med}}{n_{m,c}}$ Onde: NAC_c = pontuação do Nível de Adoção do Controle c ; NIM_{med} = pontuação do Nível de Implementação da Medida med , quando aplicável, contida no controle c ; $n_{m,c}$ = número total de medidas aplicáveis contidas no controle c .

b) NÍVEIS DE ADOÇÃO DOS CONTROLES

Tabela 5 - Níveis de adoção dos controles e respectivos intervalos

Nível	Descrição	Intervalo do NAC
0 - Não se aplica	O controle não se aplica.	-
1 - Não adota ou há decisão formal	O controle é aplicável, mas não é implementado ou existe apenas um planejamento ou decisão formal para implementá-lo.	NAC = 0,00
2 - Inicial	A média da implementação das medidas contidas no controle atinge menos de 40% do seu propósito.	0,00 < NAC < 0,25
3 - Intermediário	A média da implementação das medidas contidas no controle atinge entre 40% e 80% do seu propósito.	0,25 <= NAC < 0,50
4 - Completo	A média da implementação das medidas contidas no controle atinge mais de 80% do seu propósito.	0,50 <= NAC < 0,75
5 - Aprimorado	A média da implementação das medidas contidas no controle atinge mais de 80% do seu propósito, e as medidas são monitoradas e revisadas continuamente de forma sistemática, com base em métricas quantitativas, possuindo mecanismos que garantem uma implementação consistente ao longo do tempo.	0,75 <= NAC <= 1,00

ANEXO IV

AFERIÇÃO DOS INDICADORES DE MATURIDADE EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

a) FÓRMULA DE CÁLCULO DO INDICADOR iBase:

$$iBase = NAC_{c=0}$$

Onde:

$NAC_{c=0}$ = pontuação do Nível de Adoção dos Controles Zero.

b) FÓRMULA DE CÁLCULO DO INDICADOR iSeg:

$$iSeg = \frac{\sum_{c=1}^{18} NAC_c}{n_c}$$

Onde:

NAC_c = pontuação do Nível de Adoção do Controle c, de 1 a 18, quando aplicável;

n_c = número total de controles aplicáveis contidos no indicador iSeg.

c) FÓRMULA DE CÁLCULO DO INDICADOR iPriv:

$$iPriv = \frac{\sum_{c=19}^{25} NAC_c}{n_c}$$

Onde:

NAC_c = pontuação do Nível de Adoção do Controle c, de 19 a 25, quando aplicável;

n_c = número total de controles aplicáveis contidos no indicador iPriv.

d) NÍVEIS DE MATURIDADE DOS INDICADORES iBase, iSeg e iPriv

Tabela 6 - Níveis de maturidade dos indicadores iBase, iSeg e iPriv e respectivos intervalos

Nível	Descrição	Intervalo do indicador
1 - Inicial	O órgão atua de forma reativa, com ações pontuais e baseadas em demandas circunstanciais. Dispõe de nenhuma ou poucas políticas, normas e procedimentos.	0,00 <= iBase/iSeg/iPriv < 0,30
2 - Intermediário	O órgão apresenta iniciativas de estruturação que dependem de esforços individuais. Dispõe de algumas políticas, normas e procedimentos definidos, mas ainda enfrenta desafios de implementação prática destes instrumentos.	0,30 <= iBase/iSeg/iPriv < 0,60
3 - Em aprimoramento	O órgão possui políticas, normas e procedimentos definidos e aplicados de forma consistente na maioria das áreas. Resultados são monitorados de forma parcial.	0,60 <= iBase/iSeg/iPriv < 0,90
4 - Aprimorado	O órgão demonstra capacidade de governança institucional consolidada. Resultados são monitorados, avaliados e aprimorados continuamente.	0,90 <= iBase/iSeg/iPriv <= 1,00