

PORTARIA SEXEC/MCTI Nº 10.077, DE 21 DE MAIO DE 2026

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos no âmbito do Ministério da Ciência, Tecnologia e Inovação – ETIR/MCTI, e dispõe sobre sua organização e funcionamento.

O SECRETÁRIO-EXECUTIVO DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso das atribuições que lhe confere o parágrafo único do art. 20 da Portaria MCTI nº 9.609, de 14 de novembro de 2025, e considerando o disposto no inciso IV do art. 10 do Decreto nº 12.572, de 4 de agosto de 2025, bem como o art. 9º e § 1º do 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**

Art. 1º Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério da Ciência, Tecnologia e Inovação – ETIR/MCTI.

Art. 2º A atuação da ETIR/MCTI observará as diretrizes estabelecidas na Política Nacional de Segurança da Informação – PNSI, instituída pelo [Decreto nº 12.572, de 4 de agosto de 2025](#), e nas normas de segurança da informação aplicáveis à Administração Pública Federal.

Art. 3º A missão da ETIR/MCTI é facilitar, coordenar e executar as ações de prevenção, tratamento e resposta a incidentes cibernéticos no MCTI, tendo como objetivos:

I - Facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no MCTI;

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; e

VII - promover a cooperação com outras equipes e participar de fóruns e redes relativas à segurança da informação.

Art. 4º Para os fins desta Portaria, adotam-se, no que couber, os conceitos do Glossário de Segurança da Informação do GSI, instituído pela [Portaria GSI/PR nº 93, de 18 de outubro de 2021](#), e as seguintes definições:

I - incidente de segurança: evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou redes;

II - 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;

III - CTIR Gov: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, unidade responsável por receber e tratar notificações e atividades relacionadas a incidentes;

IV - CISC Gov.br: Centro Integrado de Segurança Cibernética do Governo Digital, unidade de coordenação operacional das ETIR dos órgãos e entidades integrantes do SISP; e

V - Agente Responsável: servidor público ocupante de cargo efetivo ou militar de carreira, integrante de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

CAPÍTULO II

DO PÚBLICO-ALVO E DO ESCOPO

Art. 5º A ETIR/MCTI atenderá a todos os usuários de serviços computacionais do MCTI, preferencialmente por meio de chamado registrado eletronicamente na Central de Serviços do Ministério ou mediante recebimento de mensagens eletrônicas em endereço institucional específico (etir@mcti.gov.br).

Art. 6º Os sistemas de informação mencionados nesta Portaria são aqueles sob a tutela da unidade responsável pela Tecnologia da Informação e Comunicação – TIC do MCTI.

Parágrafo único. O tratamento de incidentes de segurança da informação relacionados a equipamentos de terceiros não integra o escopo desta Portaria.

Art. 7º A ETIR/MCTI deverá comunicar a ocorrência de incidente de segurança da informação aos superiores imediatos, ao Gestor de Segurança da Informação, bem como ao proprietário e ao custodiante do ativo, além do Centro de Prevenção, Tratamento e Resposta a

Incidentes Cibernéticos de Governo – CTIR Gov, conforme procedimentos por ele estabelecidos, com vistas à adoção de soluções integradas no âmbito da Administração Pública Federal.

CAPÍTULO III

DA ORGANIZAÇÃO E COMPOSIÇÃO DA ETIR

Art. 8º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR funcionará como uma equipe institucional permanente, de caráter multidisciplinar e atuação predominantemente reativa, sem prejuízo da execução de atividades proativas de prevenção, monitoramento e detecção.

Parágrafo único. A ETIR será vinculada à Secretaria-Executiva.

Art. 9º A ETIR será composta por, no mínimo, 4 (quatro) integrantes, preferencialmente servidores ocupantes de cargo efetivo, vinculados à área de Tecnologia da Informação e Comunicação – TIC.

§ 1º Os integrantes da ETIR desempenharão, sem prejuízo de suas atribuições regulares, atividades relacionadas à prevenção, ao tratamento e à resposta a incidentes cibernéticos e em redes computacionais.

§ 2º Os membros da ETIR deverão pertencer à unidade responsável pela área de Tecnologia da Informação e Comunicação.

Art. 10. A composição da ETIR observará, no mínimo, a seguinte estrutura:

I – 1 (um) servidor da área de Segurança da Informação, designado como Agente Responsável, a quem competirá coordenar, supervisionar e orientar as atividades desenvolvidas pela equipe;

II – 1 (um) servidor da equipe de Sistemas de Informação;

III – 1 (um) servidor da equipe de Governança de Tecnologia da Informação e Comunicação; e

IV – 1 (um) servidor da equipe de Suporte ao Usuário.

Parágrafo único. Os integrantes da ETIR e seus respectivos substitutos serão indicados pelo Secretário-Executivo e designados em portaria específica.

Art. 11. Para cada membro da ETIR deverá ser designado um substituto, que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.

Art. 12. Os integrantes da ETIR exercerão suas funções regulares, não havendo necessidade de dedicação exclusiva.

Art. 13. As atividades proativas poderão ser atribuídas pelo Agente Responsável, conforme planejamento e necessidade operacional.

Art. 14. O Agente Responsável deverá ser servidor público ocupante de cargo efetivo ou militar de carreira, pertencente a órgão ou entidade da Administração Pública Federal, direta ou indireta.

CAPÍTULO IV

DOS PRINCÍPIOS, PAPÉIS E RESPONSABILIDADES DA ETIR

Art. 15. As atividades da ETIR/MCTI observarão os princípios e diretrizes estabelecidos na Política Nacional de Segurança da Informação – PNSI, especialmente:

I - a garantia dos direitos fundamentais, em especial a proteção de dados pessoais, a privacidade e o acesso à informação;

II - a educação como instrumento para o desenvolvimento da cultura de segurança da informação; e

III - o foco na gestão de riscos, com abordagem preventiva e orientada à proteção dos ativos de informação e dos dados pessoais.

Art. 16. São papéis no âmbito da ETIR:

I - o Gestor de Segurança da Informação;

II - o Agente Responsável pela ETIR; e

III - os integrantes da ETIR.

Art. 17. Compete ao Gestor de Segurança da Informação, nos termos da [Instrução Normativa GSI/PR nº 9, de 8 de janeiro de 2026](#):

I - Coordenar as iniciativas de segurança da informação no âmbito do Ministério, assegurando o cumprimento da legislação vigente e das normas internas;

II - Estimular iniciativas de capacitação e promover ações de conscientização em segurança da informação;

III - divulgar as normas internas de segurança da informação aos agentes públicos;

IV - Realizar avaliações de riscos e análises de impacto previamente à adoção de tecnologias emergentes;

V - Planejar e propor os recursos orçamentários necessários à implementação, atualização e manutenção das ações de segurança da informação;

VI - Acompanhar os trabalhos da ETIR;

VII - atuar como segunda linha de defesa no âmbito do Sistema de Controle Interno;

VIII - realizar avaliações de conformidade quanto à implementação da Política Nacional de Segurança da Informação e normas correlatas, bem como apoiar auditorias internas e externas;

IX - Acompanhar a aplicação de ações corretivas e administrativas decorrentes de violações à segurança da informação;

X - Cooperar com o Encarregado pelo Tratamento de Dados Pessoais nas ações que envolvam dados pessoais;

XI - elaborar e revisar o planejamento tático de segurança da informação e acompanhar sua execução;

XII - participar de fóruns especializados relacionados à segurança da informação; e

XIII - avaliar a capacidade operacional do MCTI, com vistas a subsidiar as decisões da alta administração.

Art. 18. O Gestor de Tecnologia da Informação e Comunicação deverá colaborar e fornecer os subsídios necessários ao Gestor de Segurança da Informação para o exercício de suas competências.

Art. 19. Compete ao Agente Responsável pela ETIR:

I - Estabelecer procedimentos operacionais, gerenciar as atividades e distribuir tarefas no âmbito da ETIR;

II - Assistir o CTIR Gov com informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal;

III - fazer interface com o Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br, no intuito de identificar e disseminar informações sobre vulnerabilidades e apoiar na prevenção, tratamento e resposta a incidentes cibernéticos;

IV - Promover, sempre que possível, a adoção de atividades proativas de segurança, mediante a atribuição de responsabilidades aos membros da ETIR, sem prejuízo do caráter reativo predominante do modelo adotado; e

V - comunicar ao Encarregado pelo Tratamento de Dados Pessoais sempre que houver indícios ou ocorrência de incidentes que resultem em vazamento ou comprometimento de dados pessoais, especialmente dados sensíveis, nos termos da [Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais – LGPD), bem como em conformidade com o Processo de Resposta a Incidentes de Segurança com Dados Pessoais do MCTI.

Art. 20. Compete aos integrantes da ETIR:

I - Receber, analisar, classificar e responder a notificações e atividades relacionadas a incidentes cibernéticos e em redes computacionais;

II - Manter registros e histórico de incidentes para fins estatísticos e de melhoria contínua;

III - realizar exercícios simulados de ataques cibernéticos e de tratamento de incidentes, como mecanismo de validação da capacidade institucional de resposta;

IV - atuar em conformidade com as normas internas de segurança da informação e com as diretrizes estabelecidas pelo Gestor de Segurança da Informação; e

V - Exercer outras atividades compatíveis com sua área de atuação.

Art. 21. Os integrantes da ETIR deverão ser estimulados a realizar capacitações vinculadas à temática de segurança da informação, com promoção da inclusão e da diversidade.

CAPÍTULO V

DO MODELO DE IMPLEMENTAÇÃO E FUNCIONAMENTO DA ETIR

Art. 22. A ETIR, estabelecida com referência à [NC05/IN01/DSIC/GSIPR/2009](#), seguirá o Modelo 1, “Utilizando a equipe de Tecnologia da Informação – TI”, e possuirá autonomia completa, segundo o item 9 da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

Art. 23. As funções e serviços de tratamento de incidentes deverão ser realizados, preferencialmente, por servidores públicos com capacitação técnica compatível em administração de redes, sistemas ou bancos de dados, bem como por quaisquer outras pessoas com conhecimento técnico comprovado na área de segurança da informação, observada a necessidade de garantir a multidisciplinaridade da equipe.

Art. 24. Respeitadas as atribuições estabelecidas nesta Portaria, a ETIR disporá de autonomia gerencial para orientar seu público-alvo na adoção das ações e medidas necessárias ao fortalecimento da resposta e da postura organizacional na recuperação de incidentes de segurança.

Art. 25. Durante a ocorrência de incidentes de rede computacional ou cibernéticos, a ETIR poderá executar medidas imediatas de contenção e recuperação, sem prévia aprovação de níveis superiores de gestão, visando minimizar danos e garantir a continuidade dos serviços.

Art. 26. Extraordinariamente, o Agente Responsável poderá convocar representantes de outras unidades da área de TIC para atuarem no tratamento e na resposta de determinado incidente de segurança.

Art. 27. A ETIR poderá contar com suporte operacional de terceiros para execução de suas atribuições, desde que haja previsão legal.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 28. Fica revogada a Portaria GSIC/MCTIC nº 5.357, de 12 de setembro de 2017.

Art. 29. Esta Portaria entra em vigor na data de sua publicação.

LUIS MANUEL REBELO FERNANDES



Documento assinado eletronicamente por Luis Manuel Rebelo Fernandes, Secretário-Executivo, em 26/05/2026, às 14:45 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

ANEXO I - CATÁLOGO DE SERVIÇOS DA ETIR

1. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR prestará, de forma coordenada, os seguintes serviços:

1.1 Serviço de Monitoramento e Detecção, que compreende:

- a) o acompanhamento contínuo de eventos e indicadores de segurança da informação;
- b) a identificação, em tempo hábil, de potenciais incidentes de segurança e tentativas de intrusão; e
- c) o monitoramento proativo das redes computacionais gerenciadas sob responsabilidade da área de Tecnologia da Informação e Comunicação.

1.2 Serviço de Análise de Incidentes, que compreende:

- a) a análise técnica, a filtragem e a classificação de alertas e notificações recebidas;
- b) a identificação da origem, do impacto, da abrangência e da criticidade dos incidentes de segurança;
- c) o tratamento de artefatos maliciosos, incluindo a análise de sua natureza, mecanismo, versão e objetivo; e
- d) a análise das vulnerabilidades técnicas que possibilitaram a ocorrência do incidente.

1.3 Serviço de Resposta e Contenção, que compreende:

- a) a execução de medidas destinadas à contenção da propagação, à erradicação de ameaças e à mitigação dos efeitos decorrentes de incidentes de segurança;
- b) a recuperação e a restauração dos ativos de informação e dos serviços afetados; e
- c) o desenvolvimento de estratégias de detecção, remoção e defesa contra códigos maliciosos.

1.4 Serviço de Gestão do Conhecimento, que compreende:

- a) a manutenção de base de dados atualizada com o histórico de incidentes de segurança e vulnerabilidades, de modo a preservar o conhecimento institucional, observadas as disposições da [Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais – LGPD), especialmente quanto às hipóteses legais de tratamento de dados pessoais previstas em seu art. 7º;

- b) a elaboração de relatórios relativos a exercícios simulados de incidentes e reuniões de ponto de controle;
- c) o compartilhamento de informações e procedimentos padronizados para o apoio à tomada de decisão estratégica e ao fortalecimento da resiliência cibernética; e
- d) a extração de informações para identificação de tendências e o registro de lições aprendidas.

ANEXO II - REFERÊNCIA NORMATIVA

[Decreto nº 12.572, de 4 de agosto de 2025](#), que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da Administração Pública Federal.

[Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 \(IN GSI/PR nº 1/2020\)](#): dispõe sobre a estrutura de gestão de segurança da informação nos órgãos e entidades da Administração Pública Federal, com as alterações introduzidas pela [Instrução Normativa GSI/PR nº 9, de 8 de janeiro de 2026](#).

[Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 \(NC nº 05/2009\)](#): trata da criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito da Administração Pública Federal.

[Portaria MCTI nº 9.609, de 14 de novembro de 2025 \(PSI/MCTI\)](#): institui a Política de Segurança da Informação do Ministério da Ciência, Tecnologia e Inovação.