



MINISTÉRIO PÚBLICO FEDERAL SECRETARIA GERAL

INSTRUÇÃO NORMATIVA SG/MPF Nº 33, DE 23 DE SETEMBRO DE 2025.

Institui o Plano de Gerenciamento de Crises de Tecnologia da Informação e Comunicação do Ministério Público Federal.

O SECRETÁRIO-GERAL ADJUNTO DO MINISTÉRIO PÚBLICO FEDERAL, no uso das atribuições que lhe são conferidas no art. 6º, incisos II e V c/c art. 7º, incisos I e III, do Regimento Interno Administrativo do Ministério Público Federal, aprovado pela [Portaria PGR/MPF nº 382, de 5 de maio de 2015](#), tendo em vista o disposto no PGEA nº 1.00.000.000051/2024-61, e:

Considerando a [Portaria PGR/MPU nº 78, de 8 de agosto de 2017](#), que institui a Política de Gestão de Riscos do Ministério Público da União;

Considerando a [Portaria PGR/MPF nº 155, de 24 de março de 2022](#), que dispõe sobre a Gestão de Riscos no Ministério Público Federal e aprova o Plano de Gestão de Riscos do Ministério Público Federal;

Considerando a [Instrução Normativa SG/MPF Nº 39, de 7 de novembro de 2023](#), que dispõe sobre a institucionalização da Política de Gestão de Continuidade de Serviços de Tecnologia da Informação e Comunicação - PGCSTIC - do Ministério Público Federal;

Considerando a Cartilha de Gestão de Riscos do Ministério Público Federal, de 2023, que institui um guia de acesso rápido para todos os colaboradores da Instituição, suportando o processo de Gestão de Riscos da instituição;

Considerando a Resolução CNMP nº 294, de 28 de maio de 2024, que institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP);

Considerando a [Instrução de Serviço STIC nº 1, de 5 de fevereiro de 2025](#), que dispõe sobre a definição do critério de seleção e do processo de gestão da lista de serviços de tecnologia da informação e comunicação críticos do MPF, resolve:

CAPÍTULO I

DISPOSIÇÕES INICIAIS

Art. 1º Fica instituído o Plano de Gerenciamento de Crises de Tecnologia da Informação e Comunicação - PGC do Ministério Público Federal - MPF.

Art. 2º O PGC tem o objetivo de minimizar o impacto em situação de crise ou de ameaça de crise, no contexto da tecnologia da informação e comunicação - TIC, de forma rápida, organizada e proporcionar o retorno à normalidade no menor tempo possível.

Art. 3º O PGC define os cenários de crise ou ameaça de crise e formaliza os procedimentos, os protocolos e os demais elementos a serem implementados na ocorrência de algum desses cenários.

Art. 4º O PGC atua em conjunto com o Plano de Comunicação de Tecnologia da Informação e Comunicação - PCOM e com os Planos de Continuidade de Serviços de Tecnologia da Informação e Comunicação - PCSTICs dos serviços de TIC.

Art. 5º Adota-se a abordagem objetiva como princípio norteador do gerenciamento de crises, quando aplicável, fundamentando o protocolo de atuação, em seus graus de criticidade, em boas práticas reconhecidas e legitimadas pela área e em indicadores e gatilhos pré-definidos.

CAPÍTULO II

DOS CONCEITOS

Art. 6º Para os fins desta Instrução Normativa, considera-se:

I - serviço de TIC: sistema de informação ou qualquer solução de TIC que armazene informações em formato digital, incluindo bases de dados e repositórios de arquivos institucionais;

II - serviço de TIC crítico: serviço de TIC que suporta os processos ou atividades críticas, tendo obtido classificação de criticidade alta após a aplicação dos critérios definidos de avaliação, segundo a [Instrução de Serviço STIC nº 1, de 5 de fevereiro de 2025](#);

III - risco em TIC: uma ameaça de um evento relacionado a um serviço de TIC com determinado impacto para instituição, em caso de sua manifestação, juntamente com a probabilidade de seu acontecimento;

IV - impacto de um risco de TIC: descreve a consequência para a organização de eventual manifestação de um risco em TIC, sendo classificado qualitativamente em cinco níveis crescentes de gravidade, quais sejam, insignificante, mínimo, mediano, significativo e máximo;

V - gestão de riscos em TIC: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos referentes à TIC;

VI - crise de TIC: manifestação de risco em um serviço de TIC crítico com impacto de nível significativo ou máximo;

VII - plano de comunicação de TIC: documento que estabelece as diretrizes e os padrões de comunicação às partes interessadas (pessoas chaves), internas ou externas, em situações de crises ou desastres de TIC;

VIII - plano de continuidade de serviço de TIC: conjunto de procedimentos documentados que objetiva responder a uma interrupção e retomar, recuperar e restaurar os serviços

de TIC após a ocorrência de um cenário de crise ou ameaça de crise que afete a entrega de produtos ou serviços a um nível abaixo do previamente definido;

IX - plano de recuperação de desastre - PRDTIC: plano definido e documentado, compondo o PCSTIC, que recupera as capacidades dos serviços de TIC quando uma interrupção ocorre;

X - recuperação de desastre online: tipo de recuperação de desastre em TIC que envolve recuperação de dados em mídia disponível em rede, como, por exemplo, imagens de máquinas virtuais em storages; e

XI - recuperação de desastre offline: tipo de recuperação de desastre em TIC que envolve recuperação de dados em mídia não disponível em rede, como, por exemplo, fitas de cópias de segurança armazenadas em cofre.

XII - Inventário de Sistemas do MPF: sistema de informação que cataloga todos os serviços de TIC do Ministério Público Federal e suas características básicas;

XIII - unidade gestora de serviço de TIC: unidade registrada no Inventário de Sistemas como responsável pela gestão do serviço de TIC;

XIV - unidade técnica de serviço de TIC: unidade registrada no Inventário de Sistemas como responsável pelo aspecto técnico do serviço de TIC;

CAPÍTULO III

DAS CRISES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 7º As crises de TIC no MPF serão reconhecidas quando da manifestação, ou de indício de manifestação, de risco em serviço de TIC crítico, definido em PCSTIC respectivo, com impacto de nível significativo ou máximo.

Parágrafo único. Embora possam ser estabelecidos PCSTICs para serviços de TIC não críticos, em casos especiais definidos na PGSTIC, as crises de TIC só serão reconhecidas considerando riscos em serviços de TIC críticos.

Art. 8º A manifestação, ou indício de manifestação, de um risco em TIC definido em PCSTIC com impacto de nível significativo dará origem ao reconhecimento de uma crise de TIC de nível grave.

§ 1º A análise de risco conduzida em um PCSTIC deverá classificar um impacto no mínimo como nível significativo naquele cenário em que seu tratamento respectivo no PRDTIC envolver, no máximo, uma recuperação de desastre online.

§ 2º A análise de risco de um PCSTIC poderá classificar um impacto como de nível significativo mesmo quando seu tratamento respectivo no PRDTIC não envolver, no máximo, uma recuperação de desastre online, mas quando seu impacto for de fato significativo para os objetivos da organização.

Art. 9º A manifestação, ou indício de manifestação, de um risco em TIC definido em PCSTIC com impacto de nível máximo dará origem ao reconhecimento de uma crise de TIC de nível crítico.

§1º A análise de risco de um PCSTIC deverá classificar um impacto como de nível máximo naquele cenário em que seu tratamento respectivo no PRDTIC envolver, no máximo, uma recuperação de desastre offline.

§2º A análise de risco de um PCSTIC poderá classificar um impacto como de nível máximo mesmo quando seu tratamento respectivo no PRDTIC não envolver, no máximo, uma recuperação de desastre offline, mas quando seu impacto for de fato máximo para os objetivos da organização.

Art. 10. Toda e qualquer crise de TIC deverá ser abordada por meio dos procedimentos, protocolos e os demais elementos descritos neste plano.

CAPÍTULO IV

DAS CRISES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DE NÍVEL GRAVE

Art. 11. Para efeitos de registro de duração, uma crise de TIC de nível grave inicia quando da detecção de manifestação, ou de indício de manifestação, de um risco em TIC definido em PCSTIC com impacto de nível significativo para um serviço de TIC crítico.

Art. 12. Uma crise de TIC de nível grave deve ser decretada pela unidade gestora ou pela unidade técnica do respectivo serviço de TIC.

Art. 13. Imediatamente após o decreto da crise de nível grave, o Secretário de Tecnologia da Informação e Comunicação ou seu adjunto deverá definir nominalmente a composição do grupo gestor da respectiva crise.

§ 1º A composição do grupo gestor específico de uma crise de TIC de nível grave deve contar, no mínimo, com os seguintes integrantes:

I - Secretário de Tecnologia da Informação e Comunicação ou seu adjunto;

II - titular da Unidade Gestora do serviço de TIC, seu adjunto, ou seu substituto;

III - titular da Unidade Técnica do serviço de TIC, seu adjunto, ou seu substituto;

IV - um integrante da Subsecretaria de Infraestrutura de TIC indicado pelo titular da unidade ou seu substituto;

V - um integrante da subsecretaria de desenvolvimento ou setor de gestão técnica responsável pelo código ou sustentação do serviço de TIC em crise indicado pelo titular da unidade ou pelo seu substituto; e

VI - Subsecretário de Segurança Cibernética ou seu substituto.

§ 2º Caso o serviço de TIC em crise envolva o tratamento de dados pessoais, a Unidade de Proteção de Dados Pessoais - UPDP do MPF também deverá indicar um integrante para o grupo gestor da respectiva crise.

Art. 14. Após o decreto da crise de TIC de nível grave, o grupo gestor da respectiva crise deverá realizar a reunião inicial de tratamento de crise em TIC dentro de uma hora.

Art. 15. A cada vinte e quatro horas de duração da crise de nível grave, ou em resposta a evento importante observado, o grupo gestor deverá realizar reunião regular de tratamento de crise para relatar e acompanhar as atividades do PRDTIC e de outras que se fizerem necessárias.

Art. 16. Após a implementação com sucesso do PRDTIC, ou de ações extras, e verificação de finalização da manifestação do impacto originador, o grupo gestor da crise deverá se reunir para registrar o término da crise de nível grave.

CAPÍTULO V

DAS CRISES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DE NÍVEL CRÍTICO

Art. 17. Para efeitos de registro de duração, uma crise de TIC de nível crítico inicia quando da detecção de manifestação, ou de início de manifestação, de um risco em TIC definido em PCSTIC com impacto de nível máximo para um serviço de TIC crítico.

Art. 18. Uma crise de TIC de nível crítico deve ser decretada pelo Secretário de Tecnologia da Informação ou seu adjunto, sob provocação da unidade gestora ou da unidade técnica do respectivo serviço de TIC, ou por iniciativa própria.

Art. 19. Imediatamente após o decreto da crise de nível crítico, o Secretário-Geral ou seu adjunto, com apoio do Secretário de Tecnologia da Informação e Comunicação ou de seu adjunto, deverá definir nominalmente a composição do grupo gestor da respectiva crise.

§ 1º A composição do grupo gestor específico de uma crise de TIC de nível crítico deve contar, no mínimo, com os seguintes integrantes:

I - Secretário-Geral, seu adjunto, ou integrante da Secretaria-Geral indicado pelo titular da unidade ou seu adjunto;

II - Secretário de Tecnologia da Informação e Comunicação ou seu adjunto;

III - Secretário de Comunicação Social, seu adjunto, ou integrante da Secretaria de Comunicação Social indicado pelo titular da unidade ou seu adjunto;

IV - titular da Unidade Gestora do serviço de TIC, seu adjunto, ou seu substituto;

V - titular da Unidade Técnica do serviço de TIC, seu adjunto, ou seu substituto;

VI - Subsecretário de Infraestrutura de TIC ou seu substituto;

VII - Subsecretário da subsecretaria de desenvolvimento ou chefe do setor de gestão técnica responsável pelo código ou sustentação do serviço de TIC em crise ou seus substitutos; e

VIII - Subsecretário de Segurança Cibernética ou seu substituto.

§ 2º Caso o serviço de TIC em crise envolva o tratamento de dados pessoais, a Unidade de Proteção de Dados Pessoais - UPDP do MPF também deverá indicar um integrante para o grupo gestor da respectiva crise.

§ 3º O Secretário-Geral ou seu adjunto, com apoio do Secretário de Tecnologia da Informação e Comunicação ou de seu adjunto, poderá solicitar à Comissão Estratégica de Tecnologia da Informação - CETI a indicação de integrante adicional ao grupo gestor da respectiva crise.

Art. 20. Após o decreto da crise de TIC de nível crítico, o grupo gestor da respectiva crise deverá realizar a reunião inicial de tratamento de crise em TIC dentro de uma hora.

Art. 21. A cada vinte e quatro horas de duração da crise de nível crítico, ou em resposta a evento importante observado, o grupo gestor deverá realizar reunião regular de tratamento de crise para relatar e acompanhar para relatar e acompanhar as atividades do PRDTIC e de outras que se fizerem necessárias.

Art. 22. Após a implementação com sucesso do PRDTIC, ou de ações extras, e verificação de finalização da manifestação do impacto originador, o grupo gestor da crise deverá se reunir para registrar o término da crise de nível crítico.

CAPÍTULO VI

DAS REUNIÕES DE TRATAMENTO DE CRISES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 23. As reuniões de crises de TIC poderão ser realizadas via presencial ou online.

Art. 24. As reuniões iniciais de tratamento de crise de TIC deverão necessariamente produzir os seguintes resultados:

I - confirmação da manifestação do risco em TIC definido em PCSTIC com impacto de nível correspondente, ou a verificação de que o indício de manifestação não se confirmou, encerrando o estado de crise, com produção de relatório simples narrando o acontecimento;

II - avaliação inicial da extensão do impacto, decisão sobre acionamento do PRDTIC do PCSTIC respectivo, ou de ações extras, e estimativa de retorno à normalidade;

III - preparação de informações básicas para o público interno e externo do MPF, incluindo, no mínimo, impacto originador, instituição do grupo gestor, ações básicas sendo tomadas e estimativa de retorno;

IV - provocação, caso necessária, de membro para atuação na área finalística; e

V - preparação de documento histórico com a cadeia de eventos relacionados à crise já acontecidos.

Art. 25. As reuniões regulares de tratamento de crise de TIC deverão necessariamente produzir os seguintes resultados:

I - avaliação do impacto ainda em vigor, e nova estimativa de retorno à normalidade;
II - avaliação ou identificação de rumores a serem combatidos referentes à crise em curso;

III - confirmação de andamento às ações previstas no PRDTIC, ou das ações extras projetadas, ou decisão de implementação de nova abordagem;

IV - preparação de informações básicas para o público interno e/ou público externo do MPF; e

V - atualização do documento histórico com a cadeia de eventos relacionados à crise acontecidos depois da última reunião.

Art. 26. As reuniões de término de crise de TIC deverão necessariamente produzir os seguintes resultados:

I - relatório de encerramento de crise, contendo, no mínimo:

a) motivo de início da crise;

b) duração da crise;

c) documento histórico com toda a cadeia de eventos relacionados à crise acontecidos;

d) ações do PRDTIC tomadas;

e) ações não previstas no PRDTIC tomadas;

f) descrição do evento encerrador da crise;

g) ações a serem desenvolvidas para evitar nova crise semelhante;

h) proposta, se houver, para modificação do PRDTIC e de outros planos pertinentes para melhor atuação em crise semelhante;

i) proposta, se houver, relacionada a aspectos contratuais envolvendo fornecedores de serviços de TIC, quer por descumprimento de cláusula de performance, quer por vácuo contratual;

II - preparação de informações para o público interno e o externo do MPF, descrevendo a crise e sua resolução; e

III - encerramento da atuação do grupo gestor da crise.

Art. 27. O PCOM deverá ser acionado pelo Secretário de Tecnologia da Informação e Comunicação ou seu adjunto imediatamente após o decreto das crises de TIC e também depois de todas as reuniões do respectivo grupo gestor de crise de TIC, garantindo que os devidos comunicados sejam elaborados e divulgados, observando-se as responsabilidades definidas no próprio PCOM.

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 28. Compete ao Secretário-Geral ou ao seu adjunto:

I - definir nominalmente a composição do grupo gestor de crise de TIC de nível crítico após o decreto de crise respectiva, com a estrutura mínima prevista neste normativo;

II - atuar como patrocinador das atividades de condução da crise de TIC de nível crítico, interferindo em caso de necessidades que extrapolem as competências de atuação ordinária de cada secretaria envolvida.

Art. 29. Compete ao Secretário de Tecnologia da Informação e Comunicação do MPF ou ao seu adjunto:

I - decretar, sob provocação da unidade gestora ou da unidade técnica do respectivo serviço de TIC crítico, ou por iniciativa própria, uma crise de TIC de nível crítico;

II - definir nominalmente a composição do grupo gestor de crise de TIC de nível grave após o decreto de crise respectiva, com a estrutura mínima prevista neste normativo;

III - atuar como condutor e patrocinador das atividades de condução da crise de TIC de nível grave, interferindo em caso de necessidades que extrapolem as competências de atuação ordinária de cada unidade envolvida;

IV - atuar como condutor das atividades de condução da crise de TIC de nível crítico.

Art. 30. Compete às unidades gestoras de serviços de TIC:

I - conhecer os PCSTICs dos serviços de TIC críticos sob sua responsabilidade, com capacidade de reconhecer as manifestações, ou indícios de manifestações, dos riscos em TIC com impacto de nível significativo ou máximo;

II - decretar uma crise de TIC de nível grave em serviços de TIC críticos sob sua responsabilidade;

III - monitorar eventos que possam causar impactos de nível significativo ou máximo em serviços de TIC sob sua responsabilidade; e

IV - acionar imediatamente o Secretário de Tecnologia de Informação e Comunicação quando da detecção de manifestação ou indício de manifestação de risco de TIC com impacto de nível máximo em serviço de TIC crítico para conseguinte decreto de crise.

Art. 31. Compete às unidades técnicas de serviços de TIC:

I - conhecer os PCSTICs dos serviços de TIC críticos sob sua responsabilidade, com capacidade de reconhecer as manifestações, ou indícios de manifestações, dos riscos em TIC com impacto de nível significativo ou máximo;

II - decretar uma crise de TIC de nível grave em serviços de TIC sob sua responsabilidade;

III - monitorar eventos que possam causar impactos de nível significativo ou máximo em serviços de TIC sob sua responsabilidade;

IV - acionar imediatamente o Secretário de Tecnologia de Informação e Comunicação quando da detecção de manifestação ou indício de manifestação de crise de TIC com impacto de nível máximo em serviço de TIC crítico para conseguinte decreto de crise; e

V - implementar as ações previstas no PRDTIC, ou solicitar e acompanhar a implementação pela unidade responsável, quando autorizada pelo grupo gestor de crise respectiva.

Art. 32. Compete à Subsecretaria de Segurança Cibernética:

I - acompanhar a execução do PGC em crises de TIC, orientando as áreas envolvidas na execução das ações previstas e identificando possíveis pontos de melhora;

II - acompanhar e orientar os grupos gestores de crise de TIC nas execução das atividades técnicas de acordo com as boas práticas de cibersegurança;

III - documentar as reuniões dos grupos gestores de crises em TIC;

IV - manter repositório online com acesso controlado aos relatórios de crises de TIC já ocorridas, além de indicadores próprios de acompanhamento e de melhoria das situações de crises de TIC;

V - manter repositório online com acesso controlado aos PCSTICs;

VI - promover o acesso facilitado aos PCSTICs, mesmo em cenários de indisponibilidade de recursos tecnológicos;

VII - manter repositório online com acesso controlado aos resultados dos testes periódicos e ativações dos PCSTICs;

VIII - promover o ajuste dos PCSTICs de acordo com melhorias propostas nos relatórios de encerramento de crise de TIC; e

IX - intermediar comunicações com entidades análogas de outras instituições para encaminhar o tratamento de crises de TIC quando a temática de cibersegurança for envolvida.

Art. 33. Compete à Unidade de Proteção de Dados Pessoais do MPF:

I - indicar um integrante para o grupo gestor da crise de TIC caso o serviço de TIC respectivo envolva o tratamento de dados pessoais;

II - acompanhar e orientar os grupos gestores de crise de serviços de TIC que envolvam o tratamento de dados pessoais em suas atividades, de acordo com a legislação cabível e com as boas práticas de privacidade; e

III - intermediar comunicações com entidades análogas de outras instituições para encaminhar o tratamento de crises de TIC quando a temática de tratamento de dados pessoais for envolvida.

CAPÍTULO VIII

DA IMPLANTAÇÃO

Art. 34. O presente plano, após sua entrada em vigor, deve ser implantado nos seguintes prazos:

I - Até 3 (três) meses, para implementação do repositório online com acesso aos PCSTICs; e

II - Até 6 (seis) meses, para implementação do repositório online com acesso aos resultados dos testes periódicos e ativações dos PCSTICs e aos relatórios de crises de TIC já ocorridas, com indicadores próprios de acompanhamento e de melhoria das situações de crises de TIC.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 35. Compete à Secretaria de Tecnologia da Informação e Comunicação dirimir as dúvidas suscitadas na aplicação do disposto nesta Instrução Normativa, sendo os casos omissos resolvidos pela Secretaria-Geral.

Art. 36. Este plano entra em vigor em 90 (noventa) dias após sua publicação.

Parágrafo único. Durante o período da vacatio legis estabelecido no caput deste artigo, a Secretaria de Tecnologia da Informação e Comunicação deverá promover sua ampla divulgação junto às partes interessadas.

PAULO ROBERTO SAMPAIO ANCHIETA SANTIAGO

Este texto não substitui o [publicado no DMPF-e, Brasília, DF, 24 set. 2025. Caderno Administrativo, p. 3.](#)

