PORTARIA Nº 3.451/2025
DE 07 DE OUTUBRO DE 2025

Institui, no âmbito do Ministério Público de Sergipe, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR e dá outras providências.

O PROCURADOR-GERAL DE JUSTIÇA, no uso de suas atribuições conferidas pela Lei Complementar Estadual nº 02, de 12 de novembro de 1990, e

Considerando os princípios que regem a segurança da informação, quais sejam, confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio, conforme disciplina o Decreto Federal nº 12.572, de 4 de agosto de 2025;

Considerando o disposto na Resolução nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público (CNMP), que institui a Política de Segurança Institucional do Ministério Público – PNTI/MP;

Considerando o crescente número de ataques cibernéticos sofridos por órgãos do poder público e a necessidade imprescindível de fortalecer a segurança cibernética do ecossistema digital do Ministério Público;

Considerando que a segurança é um dos valores da Diretoria de Tecnologia da Informação e Comunicação do Ministério Público de Sergipe (MPSE);

Considerando que o Plano Estratégico de Tecnologia da Informação do MPSE dispõe como objetivo estratégico garantir a segurança da informação;

Considerando a Norma ISO 27002, que dispõe sobre a necessidade de analisar criticamente a segurança de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas;

Considerando a Portaria nº 2.136/2022, que institui, no âmbito do Ministério Público de Sergipe, a Política de Privacidade e de Proteção de Dados Pessoais;

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

Considerando que a Resolução CNMP nº 294/2024 determina, em seu art. 8º, inciso VI, a instituição e implementação de Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) pelas unidades e ramos do Ministério Público, as quais comporão a Rede Nacional de Cooperação em Cibersegurança do Ministério Público (REDECiber-MP);

Considerando a necessidade de estabelecer uma estrutura especializada e coordenada para a prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do Ministério Público de Sergipe, em alinhamento às diretrizes nacionais e às necessidades institucionais,

RESOLVE:

Art. 1º Fica instituída, no âmbito do Ministério Público de Sergipe (MPSE), a **Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR**.

Art. 2º Para os efeitos desta Portaria, consideram-se:

I – **ameaça**: causa potencial de um incidente indesejado, que pode resultar em dano à segurança da informação;

II – **artefato malicioso**: qualquer programa ou código malicioso que seja prejudicial à segurança da informação da Instituição;

III – **incidente cibernético**: ocorrência que comprometa, ou tenha potencial de comprometer, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, ou tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

IV – **risco de TIC**: efeito da incerteza em projetos, iniciativas ou serviços de TIC, caracterizado por uma possível alteração negativa em relação ao resultado esperado; e

V – **vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Art. 3º São atribuições da Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR:

I – planejar, coordenar e executar atividades de tratamento e resposta a incidentes cibernéticos;

II – receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado à rede de computadores do MPSE;

III – atuar de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da Instituição;

IV – apresentar-se como um único ponto de contato na rede para comunicar incidentes cibernéticos;

V – comunicar imediatamente o incidente cibernético que envolver dados pessoais ao Encarregado de Proteção de Dados Pessoais do MPSE;

VI – realizar o monitoramento contínuo das vulnerabilidades técnicas dos serviços que tratam dados pessoais, de acordo com o item 28 do Relatório de Conformidade previsto no art. 161 da Resolução nº 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP), promovendo medidas de prevenção, mitigação e resposta;

VII – definir um modelo de gestão de incidentes cibernéticos, com processos e procedimentos para as fases do ciclo de tratamento de incidentes;

VIII – garantir que os incidentes cibernéticos no ambiente do MPSE sejam monitorados, registrados e tratados;

IX – deliberar sobre os procedimentos a serem executados ou as medidas de recuperação para os tipos de incidentes cibernéticos;

X – criar e manter um Plano de Recuperação de Incidentes Cibernéticos que descreva os devidos procedimentos de tratamento e recuperação para incidente cibernético;

XI – criar e manter uma base de dados com as vulnerabilidades na rede de computadores do MPSE e seus respectivos riscos identificados e gerenciados;

XII – apoiar as ações de treinamento e conscientização em segurança cibernética, fornecendo casos práticos de incidentes cibernéticos, desde que seja assegurada a confidencialidade e os devidos níveis de sigilo;

XIII – criar e manter um canal de comunicação para usuários internos e pessoas externas à Instituição para que elas reportem incidentes cibernéticos, suspeitos ou concretos;

XIV – tratar incidentes cibernéticos, o que consiste em receber, filtrar, classificar e responder a solicitações e alertas e realizar as análises dos incidentes cibernéticos, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e identificar tendências;

XV – tratar artefatos maliciosos, o que consiste em receber informações ou cópia de artefato malicioso que foi utilizado em ataque, ou em qualquer atividade desautorizada ou maliciosa, e analisar esse material;

XVI – emitir alertas e advertências imediatas como uma reação diante de um incidente cibernético, com o objetivo de advertir ou dar orientações sobre como se deve agir diante do problema;

XVII – executar análise de falha sobre os registros de falha para assegurar que as falhas foram satisfatoriamente resolvidas;

XVIII – investigar as causas de incidentes cibernéticos;

XIX – notificar as autoridades competentes do MPSE a respeito dos eventos e incidentes cibernéticos que ensejem aplicação de penalidades previstas em normativos internos e externos;

XX – tratar vulnerabilidades, identificando-as, analisando sua natureza e consequências, e propondo soluções e mecanismos para tratamento no sentido de eliminá-las ou diminuir seus efeitos;

XXI – quantificar e monitorar os tipos, volumes e custos de incidentes cibernéticos;

XXII – mapear a necessidade de controles para limitar a frequência e os danos de futuras ocorrências de incidentes cibernéticos; e

XXIII – emitir relatório periódico, ou sob demanda, contendo resumo das ocorrências de incidentes e vulnerabilidades cibernéticas.

Art. 4º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR será composta por:

I – Presidente do Comitê Estratégico de Tecnologia da Informação – CETI;

II – 1 (um) servidor indicado pela Divisão de Suporte – DTIC;

III – 1 (um) servidor indicado pela Divisão de Infraestrutura – DTIC;

IV – 1 (um) servidor indicado pela Divisão de Governança de TIC – DTIC;

V – 1 (um) servidor indicado pela Divisão de Projetos de TIC – DTIC; e

VI – 1 (um) servidor indicado pela Divisão de Produção de Software – DTIC.

Parágrafo único. A ETIR funcionará sob a coordenação do Presidente do Comitê Estratégico de Tecnologia da Informação e será secretariada por um dos servidores indicados.

Art. 5º O Plano de Recuperação de Incidentes Cibernéticos, a ser elaborado e mantido pela ETIR, deverá conter, no mínimo:

I – descrição do tipo de incidente cibernético;

II – descrição das ações de tratamento e recuperação;

III – identificação das pessoas envolvidas na solução;

IV – identificação das autoridades internas, externas, policiais, entidades públicas e privadas que precisam ser contatadas; e

V – estimativa de repercussões, caso as recomendações não sejam seguidas.

§ 1º Caso um incidente cibernético não esteja previsto e descrito no Plano, a ETIR deverá se reunir de forma emergencial para discutir e propor ações de tratamento e recuperação a serem executadas o mais rápido possível, a fim de minimizar os danos causados pelo incidente.

§ 2º O Plano deverá ser constantemente atualizado e mantido na base de conhecimento da equipe, de forma que os incidentes cibernéticos possam ser previstos e tratados com eficiência e eficácia.

Art. 6º Esta Portaria entrará em vigor na data de sua publicação no Diário Oficial Eletrônico do Ministério Público de Sergipe (MPSE).

Art. 7º Ficam revogadas as disposições em contrário, especialmente a Portaria nº 71/2021.

Dê-se ciência, cumpra-se e publique-se.

Nilzir Soares Vieira Junior
Procurador-Geral de Justiça

Expediente assinado eletronicamente por **Nilzir Soares Vieira Junior***, em **07/10/2025 09:31:53**, conforme art. 1º, III,"b", da Lei 11.419/2016.

A validade deste documento pode ser conferida no site http://sistemas.mpse.mp.br/mpse/Administrativo/Publico.html#/Expediente/ConsultaPublica informando o número do expediente: **20.27.0010.0002224/2025-68**