RESOLUÇÃO Nº 294, DE 28 DE MAIO 2024.

Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências.

O CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, no exercício das atribuições conferidas pelo art. 130-A, §2º, inciso I, da Constituição da República, e com fundamento no art. 147 e seguintes de seu Regimento Interno, em conformidade com a decisão plenária proferida na Sessão Ordinária, realizada em 28 de maio de 2024, nos autos da Proposição n. 1.00917/2023-35;

Considerando a atuação reguladora e integradora do Conselho Nacional do Ministério Público (CNMP), além do papel fiscalizador atribuído pelo Texto Constitucional;

Considerando a Lei n. 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial;

Considerando a Lei n. 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

Considerando a Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos estados, do Distrito Federal e dos municípios (Marco Civil da Internet);

Considerando a Lei n. 13.709, de 14 de agosto 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (Lei Geral de Proteção de Dados Pessoais – LGPD);

Considerando a Lei n. 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública;

Considerando a aprovação pelo Plenário do CNMP do novo Planejamento Estratégico Nacional do Ministério Público (PEN-MP), que elenca dentre seus objetivos estratégicos prover soluções tecnológicas integradas e inovadoras;

Considerando a Resolução CNMP n. 156, de 13 de dezembro 2016, que instituiu a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, com a finalidade de integrar as ações de planejamento e de execução das atividades de segurança institucional no âmbito do Ministério Público e garantir o pleno exercício das suas atividades;

Considerando a Resolução CNMP n. 171, de 27 de junho de 2017, que Institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP);

Considerando a Resolução CNMP n. 225, de 24 de março de 2021, que institui o Plano de Classificação de Documentos do Ministério Público (PCD) e a Tabela de Temporalidade e Destinação de Documentos do Ministério Público (TTD);

Considerando a Resolução CNMP n. 235, de 10 de agosto de 2021, que dispõe sobre a adoção do “MP On-Line” pelas unidades e ramos do Ministério Público;

Considerando a Resolução CNMP n. 257, de 14 de março de 2023, que institui a Estratégia Nacional do Ministério Público Digital (MP Digital) no âmbito do Conselho Nacional do Ministério Público;

Considerando a Resolução CNMP n. 260, de 28 de março de 2023, que instituiu a Doutrina de Inteligência do Ministério Público brasileiro;

Considerando a importância de se estabelecer objetivos, princípios e diretrizes de Segurança Cibernética alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2022, que trata da segurança da informação, segurança cibernética e proteção à privacidade;

Considerando o disposto no art. 15, § 3º e art. 18, VII, da Resolução CNJ n. 396, de 7 de junho de 2021, que instituiu

a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

Considerando o Acórdão do Tribunal de Contas da União (TCU) no Processo n. 036.301/2021-3 (Relatório de Acompanhamento), que fez auditoria de acompanhamento e mapeamento da maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança cibernética (SegCiber); e

Considerando o fenômeno da transformação digital e a crescente utilização da rede mundial de computadores e de recursos tecnológicos para acesso e processamento de dados por parte do Ministério Público, o que torna imprescindível fortalecer a segurança cibernética do ecossistema digital, RESOLVE:

## CAPÍTULO I
## DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP).

Parágrafo único. A PNCiber-MP é parte integrante da Política de Segurança Institucional do Ministério Público – PSI/MP, instituída pela Resolução n. 156, de 13 de dezembro de 2016, e com ela se compatibiliza para o fim de regulamentar o subgrupo de medidas voltadas à segurança da informação nos meios de tecnologia da informação e comunicação, em consonância com o disposto no art. 7º, § 2º, inciso I, e no art. 8º da citada Resolução.

Art. 2º A PNCiber-MP tem por finalidade estabelecer princípios, diretrizes e o sistema de governança mínimo, que nortearão o planejamento, as ações e o controle da cibersegurança, no âmbito das unidades e ramos do Ministério Público.

Art. 3º A cibersegurança compreende um conjunto ações que visam a prevenir, a detectar, a tratar e a responder às ameaças digitais, utilizando-se um conjunto adequado de controles, incluindo políticas, regras, processos, procedimentos, estruturas organizacionais, tecnologias e pessoas, com a finalidade de garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, conforme o perfil de riscos do Ministério Público.

Parágrafo único. A cibersegurança integra o conjunto de medidas de contrainteligência das unidades e ramos do Ministério Público, nos termos da Resolução n. 260, de 28 de março de 2023.

## CAPÍTULO II
## DOS PRINCÍPIOS

Art. 4º. São princípios norteadores da PNCiber-MP:

I – proteção aos direitos e garantias fundamentais dos usuários da atividade cibernética do Ministério Público;

II – integração, cooperação e intercâmbio científico, operacional e tecnológico entre os atores relacionados à cibersegurança;

III – atuação preventiva e proativa a incidentes cibernéticos;

IV – confiabilidade dos ativos e sistemas de informação, expressa pela confidencialidade, integridade e disponibilidade;

V – segurança das aplicações e demais projetos de tecnologia da informação e comunicação;

VI – conscientização, educação e capacitação nacional e internacional para criação de uma cultura de cibersegurança;

VII – atualidade dos recursos de tecnologia da informação e das técnicas e processos de cibersegurança;

VIII – valorização dos profissionais e carreiras das áreas de tecnologia e segurança da informação;

IX – comprometimento dos órgãos superiores dos ramos do Ministério Público da União e dos órgãos de

administração do Ministério Público dos Estados;

X – visão institucional e sistêmica da cibersegurança;

XI – orientação da gestão de cibersegurança conforme o perfil de riscos dos ramos e unidades do Ministério Público;

XII – articulação entre as ações de cibersegurança e de proteção de dados e ativos de informação;

XIII - privacidade desde a concepção e por padrão.

## CAPÍTULO III
## DOS OBJETIVOS

Art. 5º. A PNCiber-MP tem como objetivos:

I – aumentar a resiliência às ameaças cibernéticas, visando à manutenção da disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação do Ministério Público brasileiro;

II - definir padrões mínimos para orientar a tomada de decisões e a elaboração de normas, processos, práticas, procedimentos e técnicas de cibersegurança;

III – estimular a implementação de modelos governança em matéria de cibersegurança e a utilização de critérios, indicadores e metas para aferição dos níveis de maturidade;

IV – impulsionar a criação de uma rede nacional de cooperação entre as unidades e ramos do Ministério Público para a prevenção, tratamento e resposta a incidentes cibernéticos;

V – buscar a harmonização e uniformização das metodologias de tratamento e resposta a incidentes cibernéticos, por meio de estudos e da difusão de boas práticas, resguardadas as especificidades locais e a autonomia institucional;

VI – fomentar a conscientização, educação, capacitação e participação em eventos, nacionais e internacionais, em cibersegurança, de modo a tornar membros, servidores e demais colaboradores do Ministério Público agentes ativos na prevenção e repressão a ameaças cibernéticas;

VII – contribuir para a salvaguarda da imagem do Ministério Público, evitando sua exposição e exploração negativas;

VIII – impelir as unidades e ramos do Ministério Público, por suas administrações superiores, à melhoria contínua da infraestrutura de cibersegurança com vistas à profissionalização e perenidade das atividades.

## CAPÍTULO IV
## DOS INSTRUMENTOS

Art. 6º São instrumentos da PNCiber-MP:

I – o Planejamento Estratégico Nacional do Ministério Público (PEN-MP);

II - a Política de Segurança Institucional do Ministério Público (PSI/MP);

III – a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP);

IV – o Plano Estratégico Nacional de Tecnologia da Informação (PEN-TI);

V – os Planos de Segurança Institucional das unidades e ramos do Ministério Público;

VI - os Planos Estratégicos de Tecnologia da Informação (PETI) das unidades e ramos do Ministério Público;

VII – Protocolos, Instruções, Manuais e Enunciados Técnicos expedidos pelas instâncias de governança e gestão dessa Política.

Parágrafo único. Os planos de segurança institucional previsto no inciso V deste artigo deverão contemplar o planejamento, a organização, a coordenação das atividades e do uso de recursos para a execução das ações

estratégicas e o alcance dos objetivos da PNCiber-MP, com a atribuição de responsabilidades, a definição de cronogramas e a apresentação da análise de riscos e das ações de continuidade que garantam o atingimento dos resultados esperados.

## CAPÍTULO V
## DA GOVERNANÇA E DA GESTÃO

Art. 7º A governança da cibersegurança no Ministério Público será descentralizada, e se dará por meio das seguintes instâncias:

I – do Conselho Nacional do Ministério Público:

a) Comissão de Preservação da Autonomia do Ministério Público, por meio do Comitê de Políticas de Segurança Institucional do Ministério Público (CPSI-MP);

b) Comissão de Planejamento Estratégico, por meio de representantes da Estratégia Nacional do MP Digital e do Comitê de Políticas de Tecnologia da Informação do Fórum Nacional de Gestão do Ministério Público (CPTI/FNG-MP).

II – das Unidades e Ramos do Ministério Público:

a) Administração Superior;

b) Comissão ou Comitê Estratégico de Tecnologia da Informação;

Parágrafo único. Compete às instâncias de governança, nos seus respectivos níveis de atuação:

I - resguardar as diretrizes, princípios, objetivos e ações estatuídas nesta Política;

II – propor alterações na PNCiber-MP;

III – aprovar Estratégias, Planos e Ações nas suas respectivas instâncias de atuação;

IV - recomendar ações a serem realizadas;

V - propor medidas visando ao desenvolvimento da cultura de cibersegurança no Ministério Público;

VI - propor iniciativas visando a adoção de boas práticas relativas à cibersegurança.

Art. 8º Compete às Administrações Superiores das unidades e ramos realizar a governança e a gestão da cibersegurança, devendo:

I – implementar, no que lhe couber, a Política Nacional de Cibersegurança do Ministério Público;

II – elaborar a Política ou Plano de Cibersegurança interna, observadas as normas de segurança da informação editadas pelo CNMP;

III – destinar recursos orçamentários discriminados em rubrica específica para as ações, capacitações, certificações e participações em eventos, nacionais e internacionais de cibersegurança;

IV – destinar recursos orçamentários discriminados em rubrica específica para auditorias externas, implementação e sustentação de soluções de mercado de cibersegurança;

V – promover ações de capacitação e certificações e participações em eventos nacionais e internacionais dos recursos humanos em temas relacionados à cibersegurança;

VI – instituir e implementar Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), que comporá a REDECiber-MP;

VII – coordenar e executar as ações de cibersegurança no âmbito de sua atuação;

VIII – aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da cibersegurança;

IX – incentivar a instituição de retribuição pecuniária para os profissionais atuantes em cibersegurança como forma de valorização e retenção de talentos;

X – definir e manter quantitativos mínimos no quadro de pessoal específico de cibersegurança.

Parágrafo único. As unidades e ramos do Ministério Público poderão instituir cargo específico para o desempenho das funções de cibersegurança, nos termos da lei, respeitadas a disponibilidade orçamentária e as regras de contratação do Poder Público.

Art. 9º. As unidades e os ramos do Ministério Público deverão instituir área responsável pela governança da cibersegurança, a qual caberá:

I – assessorar a Administração Superior da unidade ou ramo ministerial em todas as questões relacionadas à cibersegurança;

II – propor alterações na política ou plano de cibersegurança e deliberar sobre assuntos a ela relacionados, incluindo atividades de priorização de ações e gestão de riscos de segurança;

III – propor normas internas relativas à cibersegurança;

IV – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre cibersegurança;

V – consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão da cibersegurança; e

VI – propor o quadro de pessoal mínimo de atuação na área de cibersegurança do ramo ou unidade;

VII - desenvolver e implementar ações estratégicas e táticas nos aspectos de segurança da informação com vista ao cumprimento de aspectos regulatórios internos e externos;

VIII - dar transparência e visibilidade às ações de segurança da informação.

§ 1º As competências previstas neste artigo poderão ser atribuídas a instância ou órgão já existente na estrutura administrativa, considerando as suas atribuições.

§ 2º A área de governança de cibersegurança, preferencialmente, deverá ter um gestor próprio.

§ 3º As unidades e ramos ministeriais editarão atos para definir a forma de funcionamento da governança, observado o disposto nesta Resolução e na legislação de regência.

Art. 10. A gestão da cibersegurança no Ministério Público se dará por meio das seguintes instâncias:

I – do Conselho Nacional do Ministério Público:

a) Comitê Gestor Nacional de Cibersegurança do Ministério Público – CGNCiber-MP;

b) Comitê de Gerenciamento de Crises – Comitê de Crise; e

c) Rede Nacional de Cooperação em Cibersegurança do Ministério Público (REDECiber-MP).

II – das Unidades e ramos do Ministério Público:

a) Comitê, Comissão, Gabinete, Gestor de Cibersegurança, de Segurança Institucional, Segurança da Informação ou órgão semelhante;

b) Áreas de Tecnologia da Informação (TI);

c) Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Parágrafo único. Compete às instâncias de gestão a execução de estratégias, planos e ações para a implementação da PNCiber-MP.

Art. 11. As unidades e ramos do Ministério Público deverão constituir estrutura administrativa responsável pela cibersegurança, prevista na letra “a”, inciso II, do artigo 10, ou atribuir essas competências a instância ou órgão já existente.

## CAPÍTULO VI
## DO SISTEMA NACIONAL DE CIBERSEGURANÇA DO MINISTÉRIO PÚBLICO

Art. 12. Fica instituído o Sistema Nacional de Cibersegurança do Ministério Público (SNCiber-MP), com a finalidade de resguardar e implementar as diretrizes, princípios, objetivos e ações estatuídas nesta Política.

Art. 13. O SNCiber-MP adotará metodologia cooperativa de governança e gestão da cibersegurança, sob a

coordenação do Conselho Nacional do Ministério Público, e será composto pelo:

I – Comitê Gestor Nacional de Cibersegurança do Ministério Público (CGNCiber-MP;

II – Comitê de Gerenciamento de Crises; e

III– Rede Nacional de Cooperação em Cibersegurança do Ministério Público (REDECiber-MP).

SEÇÃO I

Do Comitê Gestor Nacional de Cibersegurança do Ministério Público

Art. 14. Fica instituído Comitê Gestor Nacional de Cibersegurança do Ministério Público – CGNCiber-MP, órgão executivo responsável por fomentar, planejar, promover a coordenação, a cooperação e a articulação das ações das unidades e ramos ministeriais no cumprimento e acompanhamento da implementação da PNCiber-MP.

Parágrafo único. O CGNCiber-MP integrará o Sistema Nacional de Segurança Institucional, e será vinculado à CPAMP/CNMP.

Art. 15. Integram o CGNCiber-MP:

I – um membro indicado pelo CPSI, que exercerá a coordenação-geral;

II – dois membros indicados pela Estratégia Nacional do MP Digital sendo um originário de um dos ramos do MPU e outro dos Ministério Público dos Estados;

III – quatro servidores com conhecimento técnico ou gerencial em cibersegurança, indicados pelos Procuradores-Gerais, sendo dois dos ramos do Ministério Público da União e dois do Ministério Público dos Estados;

IV – um servidor com conhecimento técnico ou gerencial em cibersegurança do CNMP, indicado pela Secretaria-Geral do CNMP.

§ 1º Os integrantes e seus suplentes serão designados pela Presidência do CNMP, mediante encaminhamento da CPAMP, após indicação das demais áreas.

§ 2º O Coordenador poderá indicar dentre os servidores um coordenador operacional.

§ 3º O Coordenador do CGNCiber-MP e o servidor indicado como coordenador operacional serão requisitados e designados pelo CNMP com dedicação exclusiva, nos termos do Regimento Interno.

§ 4º A requisição e designação dos demais integrantes se darão por dedicação exclusiva ou parcial, mediante ajustes entre o CNMP e as chefias de suas respectivas unidades ou ramos, na condição de auxiliares ou colaboradores.

§ 5º Os membros indicados deverão possuir conhecimento técnico ou gerencial mínimo na área de cibersegurança ou desempenhar ou ter desempenhado funções ou atividades na área de TI.

§ 6º O Comitê poderá convidar representantes de órgãos de segurança pública, do Judiciário, das Forças Armadas e especialistas técnicos de outros órgãos públicos ou privados que pretendam subsidiar os respectivos trabalhos.

§ 7º O Comitê reunir-se-á ordinariamente, em periodicidade trimestral, mediante convocação de seu coordenador.

§ 8º O Comitê reunir-se-á extraordinariamente, mediante convocação de seu coordenador.

§ 9º A CPAMP e a Administração do CNMP prestarão os apoios necessários para o funcionamento do CGNCiber-MP.

§ 10. O Coordenador do CGNCiber-MP participará das reuniões ordinárias do CPSI-MP.

§ 11. O quantitativo de servidores previstos no inciso III poderá ser alterado, mediante deliberação das instâncias de governança, justificadamente, mediante provocação CGNCiber-MP.

Art. 16. Competirá ao CGNCiber-MP, sem prejuízo de outras atribuições:

I – exercer a coordenação geral das atividades da REDECiber-MP relativas à prevenção, ao tratamento e à resposta aos incidentes cibernéticos;

II - articular-se com as Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) das unidades

e ramos do Ministério Público, com o fim de promover e coordenar a mútua cooperação, auxiliando, quando solicitado, na gestão de incidentes de cibersegurança;

III – realizar a articulação, a interlocução e, se necessário, o acionamento de órgãos e instituições públicas especializadas no enfrentamento e repressão a ataques cibernéticos, nos termos desta Resolução;

IV - buscar a cooperação internacional, com ênfase no compartilhamento de informações sobre ameaças, vulnerabilidades e incidentes cibernéticos, promovendo troca de experiências e oportunidades de capacitação;

V - difundir alertas, recomendações e estatísticas sobre incidentes cibernéticos para os integrantes da REDECiber-MP;

VI – estabelecer critérios, indicadores que permitam monitorar a execução desta PNCiber-MP e dos seus instrumentos pelas unidades e ramos do Ministério Público;

VII – estabelecer critérios, metodologias e indicadores que permitam avaliar o nível de maturidade em cibersegurança das unidades e ramos do Ministério Público;

VIII - acompanhar a adoção de boas-práticas, bem como o cumprimento dos indicadores definidos para a gestão da cibersegurança;

IX - criar e manter atualizado um canal eletrônico de comunicação do Comitê, contendo alertas, recomendações e estatísticas sobre incidentes cibernéticos, ressalvada necessidade de sigilo das informações necessárias à preservação da segurança;

X - admitir, por ato fundamentado e em caráter eventual, a colaboração de entidades públicas ou privadas com as atividades da REDECiber-MP;

XI – promover o estudo e o debate acerca das melhores práticas em cibersegurança, com o fim de harmonização e uniformização da atuação das unidades e ramos ministeriais;

XII – propor políticas, diretrizes, estratégias, normas e recomendações relacionadas à cibersegurança do Ministério Público, submetendo-as às instâncias de governança nacionais prevista nesta Resolução, quando conveniente e oportuna a aprovação pelo Plenário do CNMP;

XIII- elaborar protocolos, instruções, manuais e outros instrumentos de atuação ou orientação, na esfera de suas competências;

XIV - expedir orientações e enunciados técnicos;

XV – adotar, elaborar e divulgar glossário temático técnico, mantendo-o atualizado;

XVI – propor as ações e as prioridades para a capacitação em âmbito nacional na área de cibersegurança;

XVII – definir diretrizes e trilhas de treinamentos para membros e servidores na área de cibersegurança;

XVIII – deliberar sobre a criação de grupos temáticos de discussão e sua composição, com o fim de especializar o debate sobre temas específicos e de produzir subsídios para as atividades da rede, submetendo os nomes à CPAMP, que tomará as providencias necessárias para a suas formalizações.

XIX - elaborar e submeter às instâncias de governança nacional a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança do Ministério Público;

XX – acompanhar e exercer o gerenciamento de crises de segurança cibernéticas, quando solicitado, no âmbito das unidades e ramos do Ministério Público;

XXI – acompanhar e participar, quando convidado, das reuniões ordinárias do Comitê de Políticas de Tecnologia da Informação do Ministério Público (CPTI-MP);

XXII – apoiar e participar de exercícios nacionais e internacionais relativos à simulação de eventos e incidentes de cibersegurança, especialmente dos entes governamentais;

XXIII – apoiar e participar de feiras, congressos, fóruns, dentre outros eventos nacionais e internacionais relativos à

cibersegurança;

XXIV – propor e promover exercícios e simulação de eventos de ataques cibernéticos, no âmbito das unidades e ramos do Ministério Público, com o fim de aumentar a resiliência;

XXV – propor atividades de comunicação e de promoção da conscientização em matéria de cibersegurança, a fim de contribuir para o desenvolvimento de uma cultura no âmbito do Ministério Público sobre o tema;

XXVI - elaborar e apresentar ao Plenário do CNMP, em caráter reservado e por meio da CPAMP, relatório anual de suas atividades, propondo as providências que julgar necessárias sobre a situação do Ministério Público no País, no âmbito da cibersegurança;

XXVII – auxiliar o Plenário do CNMP na interpretação de suas competências e os casos omissos dessa Política;

XXVIII - manter atualizados critérios e indicadores que auxiliem na classificação de uma atividade cibernética hostil como um incidente cibernético relevante, que possa comprometer a segurança das informações institucionais ou mesmo o funcionamento de serviços finalísticos.

Art. 17. A organização e o funcionamento do Comitê serão regulamentados em ato do Presidente da CPAMP, após consulta ao CPSI-MP e à Estratégia Nacional do MP Digital.

## SEÇÃO II

## Do Comitê de Gerenciamento de Crise Cibernética

Art. 18. O Comitê de Gerenciamento de Crise Cibernética (Comitê de Crise) será instituído nos casos em que o incidente cibernético relevante inviabilizar o regular funcionamento dos ramos e unidades ministeriais.

§ 1º A instituição do Comitê de Crise se dará por ato do presidente da CPAMP, em até vinte e quatro horas, após a solicitação da unidade ou ramo ministerial.

§ 2º O Comitê de Crise terá a seguinte composição:

I – os integrantes do CGNCiber-MP previstos no art. 15 desta Resolução;

II– o gestor de segurança institucional, da informação, cibernético ou semelhante, da unidade ou ramo ministerial;

III – o chefe da área de tecnologia da informação da unidade ou ramo;

IV – o chefe ou responsável pela ETIR local;

V – outros integrantes indicados pela unidade ou ramo atingido ou pelo CGNCiber-MP.

§ 3º A coordenação do Comitê de Crise ficará a cargo do coordenador do CGNCiber-MP, a quem caberá dirigir seus trabalhos;

§ 4º O Comitê de Crise acompanhará a situação ensejadora da crise presencialmente ou remotamente, observando, sugerindo ou realizando ações que identifiquem, interrompam, tratem ou recuperem as informações perdidas, restabeleçam os sistemas utilizados e os serviços prestados.

§ 5º Instituído do Comitê de Crise, os integrantes do CGNCiber-MP poderão ser afastados de suas atividades nas suas respectivas unidades e ramos, mediante ajuste com as suas chefias.

§ 6º O Comitê de Crise perdurará até que a unidade ou ramo manifeste-se pela sua desnecessidade ou por ato do presidente da CPAMP, motivadamente, a pedido do coordenador;

§ 7º Eventual custeio de despesas decorrentes das atividades a serem desenvolvidas pelo Comitê de Crise será de responsabilidade da unidade ou ramo ministerial interessado ou do CNMP, mediante ajuste prévio.

§ 8º Solicitado a instituição de Comitê de Crise pela unidade ou ramo, ficam seus integrantes autorizados a adentrarem no espaço físico, lógico, remoto, ciberespaço etc. da Instituição, com o compromisso de manterem sigilo de tudo o que tiverem conhecimento em razão do serviço.

§ 9. A participação de pessoas estranhas à organização fica vinculada à anuência da unidade ou ramo interessado, de acordo com suas regras de negócios, contratos ou acordos firmados.
§ 10. Encerrado os trabalhos do Comitê de Crise, será elaborado relatório de tudo o ocorrido, especialmente sobre os desafios, as soluções encontradas e sugestões de melhorais, que será encaminhado à chefia da unidade ou ramo ministerial em caráter reservado e, mediante avaliação da oportunidade, da conveniência e mantidos os sigilos legais, poderá ser compartilhado na REDECiber-MP como lições aprendidas.
§ 11 O Comitê de Crise colaborará com o órgão ministerial responsável pela persecução penal, quando houver instauração de procedimento criminal, em decorrência do incidente cibernético que teve sua intervenção.
§ 12. O CGNCiber-MP deliberará sobre a forma de participação da REDECiber-MP na gestão de crise.

## SEÇÃO III
## Da Rede Nacional de Cooperação em Cibersegurança do Ministério Público

Art. 19. A Rede Nacional de Cooperação em Cibersegurança do Ministério Público – REDECiber-MP atuará com a finalidade de aprimorar e manter a colaboração entre as unidades e ramos do Ministério Público para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em cibersegurança de seus ativos de informação.
Art. 20. A REDECiber-MP será coordenada pelo CGNCiber-MP e contará com a participação obrigatória dos ramos do Ministério Público da União e das unidades dos Ministérios Públicos dos Estados, tendo por objetivos:
I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
III - divulgar informações sobre ataques cibernéticos; e
IV - promover a cooperação entre os participantes da Rede.
§ 1º As unidades e ramos do Ministério Público atuarão na REDECiber-MP por meio das suas Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).
§ 2º Compete às unidades e ramos do Ministério Públicos integrantes da REDECiber-MP, sem prejuízo das demais obrigações estabelecidas nesta Resolução:
I – instituir, implementar e apoiar as atividades das suas Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);
II – participar e colaborar ativamente com as atividades da REDECiber-MP;
III – comunicar em tempo hábil ao CGNCiber-MP, por meio de suas ETIR, a existência de incidentes que impactem ou que possam impactar os serviços prestados ou contratados, incluindo as medidas de mitigação adotadas e as soluções implementadas;
IV – promover ações de profissionalização através de capacitação, certificação, participação em eventos, de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, de abrangência nacional e internacional;
V – manter atualizada a infraestrutura utilizada por suas equipes de prevenção, de tratamento e de resposta a incidentes cibernéticos;
VI – sanar, com urgência, as vulnerabilidades cibernéticas de maior impacto, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo CGNCiber-MP;
VII – cooperar, quando possível, com os demais integrantes da REDECiber-MP para o enfrentamento a incidentes cibernéticos que demandem incremento da capacidade de resposta; e
VIII - comunicar em tempo hábil ao CGNCiber-MP, por meio de suas ETIR, a existência de informações obtidas

durante o tratamento e resposta a incidentes cibernéticos que ofereçam risco imediato a outros participantes da Rede ou outros órgãos públicos.

Art. 21. Sem prejuízo das atividades permanentes, a REDECiber-MP se reunirá, em caráter ordinário, semestralmente, ou, em caráter extraordinário, por convocação do seu Coordenador.

§ 1º Cada unidade ou ramo ministerial indicará um integrante da sua respectiva ETIR para participar das reuniões da REDECiber-MP.

§ 2º As reuniões serão precedidas de convocação formal e do encaminhamento da respectiva pauta, com antecedência mínima de 15 (quinze) dias da data aprazada, a todos os integrantes e comunicada às chefias das unidades e ramos.

§ 3º O Coordenador da REDECiber-MP poderá convidar órgãos externos ao Ministério Público ou entidades privadas com especialização na área de cibersegurança para participar das reuniões, na condição de ouvintes, consultores especializados ou colaboradores eventuais, respeitadas a disponibilidade orçamentária e as regras de contratação pelo Poder Público.

§ 4º As reuniões da REDECiber-MP serão realizadas, preferencialmente, por mecanismo de videoconferência e, presencialmente, na sede de qualquer das unidades ou ramo ministeriais, mediante ajustes entre o CNMP e as respectivas chefias.

Art. 22. Poderá ser admitida, por ato fundamentado do CGNCiber-MP e respeitadas a disponibilidade orçamentária e as regras de contratação pelo Poder Público, a colaboração eventual de entidades públicas ou privadas, dispensada a adesão formal à REDECiber-MP, nas hipóteses em que seja notória a especialização da entidade na área de cibersegurança, com vistas ao atendimento de demandas específicas e delimitadas pelo ato respectivo, tais como:

I – realização de auditorias externas em matéria de cibersegurança;

II – oferta de capacitações e treinamentos em cibersegurança;

III – auxílio no atendimento a incidentes cibernéticos relevantes que extrapolem a capacidade de enfrentamento pelos integrantes da Comitê de Crise;

IV – fornecimento de informações técnicas e estratégias especializadas em segurança cibernética e inteligência de ameaças cibernéticas (cyber threat intelligence).

## CAPÍTULO VII
## DA CIBERSEGURANÇA NAS UNIDADES E RAMOS DO MINISTÉRIO PÚBLICO

Art. 23. As unidades e ramos ministeriais instituirão seus próprios Sistemas de Gestão em Cibersegurança (SGCiber), com a definição das atribuições e responsabilidades de cada agente e órgão interno nos processos de prevenção, tratamento e resposta a incidentes.

§ 1º Independentemente da nomenclatura adotada, as unidades ministeriais deverão instituir Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) à qual caberá, sem prejuízo das suas atribuições internas conferidas pelo respectivo SGCiber, a função de servir como canal de interação com o CGNCiber-MP e com a Rede Nacional de Cooperação em Cibersegurança do Ministério Público (REDECiber-MP).

§ 2º Compete às unidades e ramos ministeriais instituir as suas próprias Políticas de Cibersegurança, nas quais deverão considerar as especificidades locais e critérios para avaliação da relevância dos incidentes cibernéticos.

§ 3º O planejamento, a gestão e a execução das ações em cibersegurança pelas unidades e ramos do Ministério Público deverão considerar os seguintes princípios:

I - o elemento humano como fundamental e objeto de especial atenção;

II - a gestão dos recursos de tecnologia como fator crítico;

III - inovação e atualização dos ativos corporativos e softwares;

IV - construção e implementação de processos bem definidos, organizados de forma lógica e integrada, com o fim de proporcionar adequada interação e harmonia entre os elementos humano e tecnológico dedicados à prevenção, tratamento e resposta a incidentes.

§ 4º O quadro de pessoal na área de cibersegurança deverá ter, preferencialmente, atuação exclusiva.

## CAPÍTULO VIII
## DA ESTRATÉGIA E DO PLANO NACIONAL DE CIBERSEGURANÇA DO MINISTÉRIO PÚBLICO

Art. 24. A Estratégia e o Plano Nacional de Cibersegurança do Ministério Público serão elaborados pelo CGNCiber-MP e submetidos às instâncias de governança nacional para aprovação.

Art. 25. A Estratégia Nacional de Cibersegurança do Ministério Público objetiva criar as melhores condições para que a Instituição possa se antecipar às ameaças cibernéticas.

Art. 26. A Estratégia deverá, no âmbito da cibersegurança:

I - identificar os principais desafios;

II - definir os eixos estruturantes;

III - designar os objetivos estratégicos; e

IV - estabelecer as ações estratégicas.

Parágrafo único. A Estratégia será atualizada bienalmente.

Art. 27. O Plano Nacional de Cibersegurança do Ministério Público implementa as determinações da Estratégia Nacional de Cibersegurança e deve:

I - estabelecer ações;

II - definir prioridades;

III - estipular prazos; e

IV - designar responsáveis e recursos.

Parágrafo único. O Plano será atualizado alinhado com a estratégia.

## CAPÍTULO IX
## DISPOSIÇÕES FINAIS

Art. 28. Esta Resolução se aplica ao Conselho Nacional do Ministério Público (CNMP).

Art. 29. O CNMP destinará no seu plano de gestão recurso orçamentário específico para as atividades do CGNCiber-MP.

Art. 30. A Resolução CNMP n. 156, de 13 de dezembro de 2016, passa a vigorar com a seguinte redação:

“Art. 18. .....

V – pelo Comitê Gestor Nacional de Cibersegurança do Ministério Público.”

Art. 31. A Resolução CNMP n. 171, de 27 de junho de 2017, passa a vigorar com a seguinte redação:

“Art. 13. .....

VI – gestor ou responsável pela cibersegurança na unidade ou ramo ministerial.”

Art. 32. Disposições de níveis tático e operacional serão objeto de instrumentos complementares a esta Política, definidas no âmbito do CGNCiber e da REDECiber-MP.

Art. 33. As informações específicas sobre os incidentes cibernéticos e sobre as configurações e características técnicas de ativos de informação de cada unidade do Ministério Público e do Conselho Nacional do Ministério Público são consideradas imprescindíveis à segurança da sociedade e do Estado.
Art. 34. O Comitê de Políticas de Tecnologia da Informação do Ministério Público (CPTI-MP) deverá manter discussão permanente sobre cibersegurança nas suas atividades.
Art. 35. As unidades e ramos do Ministério Público, em até cento e oitenta dias após a publicação dessa Resolução, instituirão suas ETIR, previstas no inciso VI do artigo 8º.
Art. 36. A Estratégia e o Plano Nacional de Cibersegurança elaborados pelo CGNCiber-MP serão apresentados às instâncias de governança para aprovação, em até cento e oitenta dias, após a sua constituição.
Art. 37. As unidades e ramos do Ministério Público poderão colaborar ou participar de outras instâncias governamentais de defesa cibernética previstas em atos normativos próprios.
Art. 38. Esta Resolução entra em vigor na data de sua publicação.
Brasília, 28 de maio de 2024.

PAULO GUSTAVO GONET BRANCO
Presidente do Conselho Nacional do Ministério Público

RESOLUÇÃO Nº 295, DE 28 DE MAIO DE 2024.

Altera a Resolução CNMP nº 286, de 12 de março de 2024, que estabelece diretrizes para as atividades de auditoria interna no Ministério Público.

O CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, no exercício das atribuições conferidas pelo art. 130-A, §2º, I, da Constituição Federal, e com fundamento no art. 147 e seguintes de seu Regimento Interno, em conformidade com a decisão plenária proferida na 8ª Sessão Ordinária, realizada em 28 de maio de 2024, nos autos da Proposição nº 1.00431/2024-05;
Considerando o disposto nos artigos 70 e 74 da Constituição Federal; e
Considerando a necessidade de uniformização dos procedimentos de auditoria interna no âmbito do Ministério Público, RESOLVE:
Art. 1º O art. 23 da Resolução CNMP nº 286, de 12 de março de 2024, passa a vigorar com a seguinte redação:
"Art. 23. O cargo de titular da unidade de auditoria interna será exercido, preferencialmente, por membro ou servidor do quadro efetivo do Ministério Público, nomeado pela Chefia da instituição ministerial."
Art. 2º Esta resolução entra em vigor na data de sua publicação.
Brasília/DF, 28 de maio de 2024.

PAULO GUSTAVO GONET BRANCO
Presidente do Conselho Nacional do Ministério Público

RESOLUÇÃO DE 11 DE JUNHO DE 2024

RESOLUÇÃO Nº 296, DE 11 DE JUNHO DE 2024.

Altera a Resolução CNMP nº 174, de 4 de julho de 2017, que disciplina, no âmbito do Ministério Público, a instauração e a tramitação da Notícia de Fato e do Procedimento Administrativo.