MINISTÉRIO PÚBLICO DO TRABALHO - PROCURADORIA GERAL DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO - CETI
SAUN Quadra 5, Lote C, Torre A – 6º Andar – Brasília - DF – CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

RESOLUÇÃO CETI/MPT n.º 24

Institui o Processo de Inventário e Mapeamento de Ativos de Informação no âmbito do Ministério Público do Trabalho.

O **COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI)** do Ministério Público do Trabalho, no uso das atribuições que lhe confere a Portaria PGT nº 739/2016, que instituiu e regulamentou, no âmbito do Ministério Público do Trabalho, o Sistema Integrado de Governança da Gestão Estratégica - SIGGE, e as alterações feitas pela Portaria PGT nº 615.2022,

CONSIDERANDO que, de acordo com a Resolução CNMP n. 70, compete ao CETI definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação;

CONSIDERANDO a necessidade de aprimorar os padrões de governança em tecnologia da informação no Ministério Público do Trabalho;

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 as diretrizes da Lei de Acesso à Informação (LAI), de nº 12.527/2011 de 18 de novembro de 2011;

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. 294, de 28 de maio de 2024, que Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências;

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 e estabelece, através do Plano de Tratamento de Riscos, como a organização

responderá às ameaças identificadas no processo de inventário de ativos de informação e suas respectivas avaliações de riscos;

CONSIDERANDO a Norma ISO/IEC 27005 (ABNT NBR ISO/IEC 27005:2023), que fornece diretrizes para o gerenciamento de riscos de segurança da informação.

CONSIDERANDO o Acórdão do Tribunal de Contas da União (TCU) 1768/2022 – Plenário, 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
DEFINIÇÕES E DIRETRIZES

Art 1º. Instituir o Processo de Inventário e Mapeamento de Ativos de Informação (PIMAI) no âmbito do Ministério Público do Trabalho.

Art 2º. Para os efeitos desta Resolução, aplicam-se, além do constante na Política de Segurança da Informação e Comunicação (POSIC) do Ministério Público do Trabalho, os seguintes termos e definições:

I. **Acesso** - ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

II. **Agente público** - todo aquele que exerce cargo, emprego ou função no Ministério Público do Trabalho, ainda que transitoriamente ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores e membros do MPT, estagiários, menores aprendizes e colaboradores).

III. **Agente de Mapeamento** - membro ou servidor ocupante de cargo efetivo do Ministério Público do Trabalho incumbido de chefiar e gerenciar o PIMAI em sua área de atuação e para os ativos de informação sob sua propriedade, gestão ou custódia técnica.

IV. **Ativo de informação** - também chamado de ativo de Tecnologia da Informação (**Ativo de TI**) ou ativo de Tecnologia da Informação e Comunicação (**Ativo de TIC**), é *qualquer componente ou recurso que precise ser gerenciado de forma a garantir a entrega de um serviço de TI* (Resolução CNMP Nº 171), sendo ativos cibernéticos de armazenamento, transmissão e processamento da informação, contemplando hardwares, softwares, dados, sistemas, infraestrutura, documentos e outros recursos

que possuem valor, tangível ou intangível, para o Ministério Público do Trabalho, cada um devendo ser tratado como uma entidade única, organizada e gerenciada, podendo ser, entre outros:

a) Hardwares: computadores, servidores, notebooks, impressoras e dispositivos móveis (incluindo telefones, tablets, etc.);
b) Softwares: sistemas operacionais, máquinas virtuais, aplicativos corporativos, licenças de uso, aplicativos de negócio (finalístico, administrativo, Gerencial, Regulação, Serviços, Inteligência de Negócio (BI), Inteligência Artificial, etc.);
c) Infraestrutura de rede: roteadores, switches, cabos, pontos de acesso; redes de telecomunicações e suas partes de infraestrutura;
d) Dados: bancos de dados, documentos armazenados em formato digital (arquivos digitais) e informações digitais estratégicas ou que possuem valor para a organização;
e) Serviços de tecnologia da informação e comunicação (TIC): como contratos em nuvem, plataformas SaaS e soluções de backup;
f) Processos de negócios, tangíveis ou intangíveis, que sejam processados, armazenados ou transitados em recursos de TIC (licenciamentos de software, certificados, bibliotecas, scripts, etc.).

V. **Autenticidade** - propriedade de que a informação foi produzida, expedida, modificada ou destruída por um ativo de informação, uma determinada pessoa física, ou por um determinado órgão ou entidade externa ao MPT.

VI. **Colaborador** - pessoa jurídica ou pessoa física que desempenhe atividade de interesse do Ministério Público do Trabalho, realize estágio ou preste serviço, em caráter permanente ou eventual, com ou sem remuneração.

VII. **Confidencialidade** - propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada.

VIII. **Contêineres dos ativos de informação** - local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

IX. **Continuidade de negócios** - capacidade estratégica e tática do Ministério Público do Trabalho se planejar e responder a incidentes de segurança cibernética e da informação que causem interrupções de seus negócios, minimizando seus impactos e recuperando perdas dos ativos de informação e de suas atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

X. **Custodiante(s) do ativo de informação** – Um dos três papéis de responsabilidade do ativo de informação, conforme sua definição e responsabilidades elencadas nos artigos 5º e 6º desta Resolução.

XI. **Disponibilidade** - qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados.

XII. **Documento** - unidade de registro de informações, qualquer que seja o suporte ou formato.

XIII. **Estimativa de riscos** - processo utilizado para atribuir valores à probabilidade e consequências de um risco.

XIV. **Estratégia de continuidade de negócios** - abordagem que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.

XV. **Gestão de Riscos de Segurança da Informação** - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

XVI. **Gestor de Segurança Cibernética** – Área (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou pessoa formalmente designada, que é responsável pela orquestração e condução das ações de segurança cibernética no âmbito do Ministério Público do Trabalho a fim de atingir os requisitos de segurança da informação de ativos de informação processados, armazenados ou transitados em recursos de tecnologia da informação e comunicação (TIC);

XVII. **Gestor de Segurança da Informação** - Área (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou pessoa formalmente designada, que é responsável pela orquestração e condução das ações de segurança da informação e comunicações no âmbito do Ministério Público do Trabalho;

XVIII. **Gestor do ativo de informação** – Um dos três papéis de responsabilidade do ativo de informação, conforme sua definição e responsabilidades elencadas nos artigos 5º e 6º desta Resolução.

XIX. **Informação** - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XX. **Infraestrutura crítica de informação** - são os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Ministério Público do Trabalho e a sua segurança cibernética e da informação;

XXI. **Integridade** - propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXII. **Inventário** - consiste no registro sistemático e operacional, na catalogação e documentação detalhada dos ativos de informação, com informações de dados e propriedades que podem ser utilizados para definir o valor do ativo para a organização, bem como servir como base para controle, auditoria e gestão ao longo

do tempo, incluindo a identificação de riscos associados - como vulnerabilidades, ameaças e impactos potenciais - e o atendimento aos requisitos de segurança cibernética, com vistas à proteção da confidencialidade, integridade e disponibilidade das informações;

XXIII. **Mapeamento** – processo de identificar, localizar, atualizar e compreender os ativos de informação existentes, com a finalidade de obter dados, propriedades e informações do ativo em um panorama geral do ambiente tecnológico, entendendo onde eles estão, como se conectam, qual seu papel nos processos da organização e quem são seus responsáveis;

XXIV. **Parte interessada** - toda pessoa física, jurídica ou área de negócio do MPT (Secretaria, Coordenadoria, Divisão, Departamento, Setor, etc.) que participa do processo ou rito administrativo sobre o qual demande acesso à informação, podendo ser quem provocou o processo ou o ato, o proponente, a parte citada ou a parte que se defende;

XXV. **Política de Segurança da Informação e Comunicações** (POSIC) - documento institucional com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança cibernética, da informação e comunicações;

XXVI. **Proprietário do ativo de informação** - Um dos três papéis de responsabilidade do ativo de informação, conforme sua definição e responsabilidades elencadas nos artigos 5º e 6º desta Resolução.

XXVII. **Responsáveis pelo ativo de informação** – o conjunto dos três papeis de responsabilidade do ativo (**proprietário**, **gestor** e **custodiante**), podendo haver um único responsável exercendo os três papeis ao mesmo tempo, ou um responsável exercendo dois papeis, um responsável para cada papel.

XXVIII. **Riscos de segurança da informação** - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio do MPT;

XXIX. **Segurança Cibernética** - ou cibersegurança, é a atividade prática de proteger ativos de informação e dados, armazenados, em trânsito e em processamento, de ameaças digitais provenientes de dentro ou de fora de uma organização, sendo que as atividades de cibersegurança necessitam de pessoas, processos, infraestrutura complexa e profissionais altamente capacitados, cuja expertise hoje é reconhecida nos profissionais de TI;

XXX. **Segurança da Informação** - atividade sistêmica, de responsabilidade de toda a organização. Conforme Resolução CNMP Nº 156/2016 a Segurança da Informação é um dos grupos de medidas da segurança orgânica (Art. 3º) e compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza

ao Ministério Público ou proporcionar vantagem a atores antagônicos (Art. 7º), sendo que, após a Transformação Digital, ocorrida ao longo das duas últimas décadas, boa parte ou quase toda segurança da informação é realizada através da Segurança Cibernética;

XXXI. **Usuário do ativo de informação –** individuo interno ou externo, ou recurso informático que consome ou faz uso de um ativo de informação do MPT e que deve:

a) cumprir as normas do Ministério Público do Trabalho de uso de recursos de TI;

b) fazer uso do ativo de informação atendendo e respeitando a Política de Segurança da Informação e Comunicações (POSIC) do MPT;

c) fazer uso e/ou consumo adequado do ativo de informação apenas para os propósitos do negócio e de acordo com as diretrizes, estabelecidas ou intrínsecas;

d) fazer uso adequado das informações ingeridas, armazenadas, transitadas, processadas ou produzidas pelo ativo de informação, respeitando as normas internas do MPT, bem como a Lei de Acesso à Informação (Lei Nº 12.527, de 18 de novembro de 2011) e a Lei Geral de Proteção de Dados (Lei Nº 13.709, de 14 de agosto de 2018).

XXXII. **Valor do ativo de informação** - valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos do Ministério Público do Trabalho, quanto o quão cada ativo de informação é imprescindível aos seus interesses;

XXXIII. **Vulnerabilidade** - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um ativo de informação ou para todo Ministério Público do Trabalho, os quais podem ser evitados por uma ação interna de segurança cibernética e/ou da informação.

Art 3º. O PIMAI é um processo dinâmico, periódico, repetitivo (iterativo), estruturado e evolutivo, devendo observar, para sua consecução, a capacidade operacional e de infraestrutura de gestão de segurança cibernética do Ministério Público do Trabalho.

Art 4º. Farão parte do PIMAI os **Mapeamentos de Ativos de Informação (MAI)**, que são processos exclusivos de mapeamento de ativos com tempo de execução definido e marcos de começo meio e fim.

§1º Deverão ser executados MAI periódicos, a fim de identificar novos ou atualizar dados de ativos já inventariados, e atualização dos responsáveis de cada ativo.

§2º Os MAI serão realizados através de questionários direcionados a todas as áreas da Procuradoria-Geral e das Procuradorias Regionais do Trabalho, ou através mecanismos automatizados.

Art 5º. São definidos como responsáveis dos ativos de informação:

I. **CUSTODIANTE** – uma ou mais entidades, devendo ser área(s) organizacionais (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, e/ou um ou mais indivíduos (membro ou servidor responsável(ies) pela guarda, controle e proteção dos ativos de informação que, embora não seja o proprietário ou responsável, estão sob sua custódia (física, técnica, de riscos, etc.).

II. **GESTOR** – uma única entidade, devendo ser uma área organizacional (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou indivíduo (membro ou servidor), responsável por administrar e otimizar o ativo de informação, garantindo que ele seja utilizado de forma eficiente, reduzindo custos e riscos, e proporcionando uma fonte única de informações para a tomada de decisões estratégicas.

III. **PROPRIETÁRIO** – uma única entidade, devendo ser uma área organizacional (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou indivíduo (membro ou servidor), que é responsável primário pelo ativo de informação, quem responde formalmente pelo ativo.

§1º O Custodiante é o único papel de responsabilidade do ativo de informação que pode ser exercido por mais de uma entidade - área(s) organizacional(is) e/ou membro(s) e servidor(es), podendo, portanto, haver mais de um custodiante (técnico, físico, de riscos, administrativo, etc.) para cada ativo.

§2º O gestor do ativo de informação pode acumular os papeis de gestor e custodiante;

§3º O proprietário do ativo de informação pode acumular os papeis de proprietário e gestor, de proprietário e custodiante, ou os três papeis, neste último caso se tornando uma única entidade responsável pela propriedade, gestão e custodia do ativo.

Art 6º. Cabem aos responsáveis do ativo de informação:

I. **CUSTODIANTE**:

a) zelar pelo armazenamento, operação, administração e preservação de ativos de informação que estão sob sua custódia física, administrativa, de riscos e técnica, apenas por fazer uso do ativo, ou por designação formal de custódia;

b) participar do processo de gestão de riscos que envolvam os ativos sobre sua custódia;

c) no que lhe couber, deve responder, solidariamente, com o proprietário e gestor do ativo, pelos impactos causados pelos riscos de segurança cibernética e segurança da informação do ativo ao próprio ativo, ao Ministério Público do Trabalho, ou a terceiros.