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

Resolução CETI nº 4, de 7 de março de 2016.

Institui a Política Nacional de Segurança da Informação do Ministério Público do Trabalho.

O COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI) do Ministério Público do Trabalho, no uso das atribuições que lhe conferem a Portaria PGT n.º 723, de 9 de setembro de 2015;

CONSIDERANDO que, de acordo com a Resolução CNMP n.º 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 que a informação constitui ativo essencial, a demandar proteção contra os vários tipos de ameaças externas e internas que possam comprometer sua integridade, sua confidencialidade e sua disponibilidade;

CONSIDERANDO a classificação, o tratamento e a gestão da informação sigilosa e da informação pessoal contida na documentação, em qualquer suporte, do Ministério Público do Trabalho – MPT.

CONSIDERANDO a necessidade de garantir a continuidade dos serviços de tecnologia da informação, a minimização de riscos e a maximização dos resultados nas ações de Tecnologia da Informação;

CONSIDERANDO os padrões ISO/IEC 27.000 (*Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*), ABNT/NBR ISO/IEC 27.001 (Tecnologia da Informação - Técnicas de Segurança - Sistema de Gestão da Segurança da Informação – Requisitos) e ABNT/NBR ISO/IEC 27.002 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação).

RESOLVE:

Art. 1º Instituir a Política Nacional de Segurança da Informação do Ministério Público do Trabalho mediante o estabelecimento de diretrizes e responsabilidades para a elaboração de normas e procedimentos a serem cumpridos por membros, servidores e colaboradores.

§1º Entende-se por segurança da informação a garantia das propriedades da informação durante todo o seu ciclo de vida, por meio da adoção de controles.

§2º A estrutura normativa de segurança da informação compreende:

I. Em Nível Estratégico, a Política de Segurança da Informação, definida nesta resolução;

II. Em Nível Tático, as normas de Segurança da Informação, que estabelecem escolhas tecnológicas de controle a serem implementadas para cumprir as diretrizes estabelecidas na Política;

III. Em Nível Operacional, os procedimentos de Segurança da Informação, consistentes em ritos que instrumentalizem a política e as normas por meio de configurações específicas de mecanismos de controle em todas as unidades do MPT.

§ 3º Para os efeitos desta resolução e das notas técnicas a serem produzidas em consonância com as diretrizes ora estabelecidas, consideram-se as seguintes definições:

I. Propriedades ou atributos da informação: autenticidade, confidencialidade, disponibilidade, integridade e não repúdio;

II. Autenticidade: propriedade ou atributo de identidade do criador, manipulador, armazenador, transmissor ou responsável pelo descarte da informação;

III. Confidencialidade: propriedade ou atributo de proteção, em consonância com o grau de sigilo da informação;

IV. Disponibilidade: propriedade ou atributo que garante o acesso à informação quando houver necessidade;

V. Integridade: propriedade ou atributo que garante a preservação do conteúdo da informação conforme a exatidão e a intenção de quem a criou ou manipulou;

VI. Não repúdio (ou irretratabilidade): propriedade ou atributo destinado à preservação da autenticidade da informação mediante neutralização da negação da identidade do criador, manipulador, armazenador, transmissor ou responsável pelo descarte da informação;

VII. Ciclo de vida: propriedade ou atributo que compreende a criação, a manipulação, o armazenamento, a transmissão e o descarte da informação;

VIII. Custodiante: agente provedor dos meios técnicos para a preservação da informação consoante os requisitos de segurança definidos pelo gestor;

IX. Gestor: agente, nomeado por autoridade competente, definidor dos requisitos para a garantia das propriedades da informação que está sob sua gestão;

X. Incidente de segurança da informação: qualquer evento, acidental ou intencional, que violar as propriedades da informação em seu ciclo de vida.

Art. 2º São princípios da Segurança da Informação no MPT:

I. a Garantia do Menor Privilégio, consistente no acesso à informação em medida suficiente para a execução das operações nela fundadas, conforme a classificação de graus de sigilo, a necessidade de conhecer e o justo interesse institucional e da sociedade.

II. a Necessidade de Conhecer, condição indispensável, inerente à atividade institucional, por meio da qual se define o acesso à informação classificada em qualquer grau de sigilo.

III. a Classificação da Informação, consistente em atribuição do grau de sigilo, pela autoridade competente, com base no qual se definirá a adoção dos controles de segurança.

IV. o Compartimentação de Funções, consistente na separação dos tipos de acesso à informação ou do ambiente operacional onde a informação é manipulada, em consonância com a classificação do sigilo e a necessidade de conhecer.

Art. 3º São diretrizes relativas à Gestão da Informação, necessárias à garantia integral de suas propriedades e princípios:

I. A informação produzida ou recebida pelo MPT deverá ser armazenada, transmitida, manipulada e descartada por meio da aplicação de controles compatíveis com sua classificação em qualquer grau de sigilo;

II. O acesso e o uso das informações do MPT atenderão aos interesses institucionais e, conforme a lei, aos interesses da sociedade;

III. Toda informação deverá ser classificada, reclassificada ou desclassificada por autoridade competente da instituição a fim de se definir o seu nível de acesso e as medidas de segurança a serem adotadas, considerando seu valor, criticidade e sensibilidade para o MPT e para outras instituições, nos limites da lei e dos ditames constitucionais;

IV. Para toda informação, classificada em qualquer grau de sigilo, deverá ser nomeado um gestor, que definirá os requisitos para a preservação das propriedades da informação; e um custodiante, que proverá os mecanismos operacionais de segurança a fim de atender aos requisitos definidos pelo gestor;

V. As informações classificadas como secretas ou em graus análogos de sigilo deverão ser alocadas em ambientes operacionais compartimentados para armazenamento, atualização, manipulação e tráfego;

VI. A utilização dos ativos de informação, bem como dos sistemas e serviços correlatos, deve atender exclusivamente ao interesse da instituição;

VII. A integridade e a autenticidade das informações classificadas como públicas e disponíveis, conforme a lei, em repositórios de acesso público, será periodicamente verificada e auditada.

Art. 4º São diretrizes relativas aos membros, servidores e colaboradores:

I. Membros, servidores e colaboradores deverão ser conscientizados a respeito da necessidade de preservação da Segurança da Informação em sistemas da instituição;

II. Todo aquele que obtiver acesso a informação classificada em qualquer grau de sigilo fica obrigado a resguardar seus requisitos de segurança;

III. Os contratos de prestação de serviços devem prever a necessidade de assinatura de termo compromisso de confidencialidade sobre o eventual acesso a informação classificada em qualquer grau de sigilo;

IV. A conscientização e a educação em segurança da informação devem ser promovidas com o objetivo de criar, no âmbito do MPT, uma cultura de segurança da informação;

V. O tema segurança da informação deve ser abordado em cursos de formação e em programas de ambientação;

VI. A divulgação a respeito dos requisitos legais e constitucionais para a proteção da privacidade e da intimidade deve ser realizada a todos.

Art. 5º São diretrizes relativas à Gestão de Ativos e do Ambiente Físico:

I. paralelamente ao inventário e aos controles de patrimônio, os ativos envolvidos nos serviços e sistemas de informação devem ser considerados como itens de configuração a fim de garantir o controle de quais itens participam dos processos de Tecnologia da Informação e o mapeamento da respectiva cadeia de dependência;

II. a alienação, a doação, o descarte e o uso de ativos que armazenem informação classificada, em qualquer grau de sigilo, ainda que temporariamente, deverá respeitar procedimento formal;

III. as instalações físicas dos sistemas de informação devem ser identificadas, classificadas e protegidas por perímetros físicos de segurança, franqueando-se o acesso físico conforme a classificação da informação no mais alto grau de sigilo;

IV. os riscos de qualquer natureza – como os derivados de acessos físicos ou eletrônicos não autorizados, da interceptação em canais de comunicação, dos danos físicos acidentais ou intencionais, dos eventos naturais, da paralização de serviços essenciais e de distúrbios causados por radiação – deverão mapeados de modo que, mediante plano de ação revisado periodicamente, sejam progressivamente reduzidos ou eliminados por meio de barreiras de segurança, controles de acesso e replicações;

Parágrafo Único: As diretrizes relativas à Gestão de Ativos e do Ambiente Físico devem ser aplicadas, no que couberem, aos ativos instalados fora das dependências das unidades do MPT.

Art. 6º São diretrizes relativas à gestão das operações e das comunicações:

I. Os ambientes operacionais de desenvolvimento, de testes e de produção devem ser compartimentados a fim de evitar que as informações classificadas em qualquer grau de sigilo sejam indevidamente manipuladas;

II. Todos os serviços ou sistemas desenvolvidos ou adquiridos pelo MPT deverão possuir, como condição de ingresso em produção, o respectivo modelo de interação entre seus próprios elementos e com elementos de outros sistemas, se houver;

III. Os contratos de entrega e de prestação de serviços devem incluir cláusulas que garantam o cumprimento da política, das normas e dos procedimentos de segurança da informação do MPT, sob pena de sanções para os casos de violação;

VI. Os serviços, os sistemas e as redes de comunicação de dados do MPT devem ser gerenciadas e monitoradas a fim de garantir e avaliar constantemente sua disponibilidade, desempenho, capacidade e segurança;

V. As mudanças dos serviços e sistemas de informação do MPT devem ser necessariamente planejadas e controladas a fim de minimizar o risco de indisponibilidade e de prejuízos a qualquer das propriedades da informação;

VI. Todos os registros de eventos (logs) dos ativos que suportam os sistemas de informação do MPT devem ser coletados e armazenados, com garantida de integridade, de modo que sejam utilizados como evidências de auditoria;

VII. Os relógios de todos ativos do sistema de informação do MPT deverão estar sincronizados com a mesma referência de tempo;

VIII. Os procedimentos de operação devem ser documentados, atualizados e disponibilizados aos envolvidos no processo de operação dos sistemas e serviços.

Art. 7º São diretrizes relativas ao controle de acesso lógico à informação:

I. Todas as normas que tratam do controle de acesso devem seguir o princípio do menor privilégio, considerando a classificação da informação em qualquer grau de sigilo, a necessidade de conhecer e o justo interesse institucional e da sociedade;

II. O registro, o provisionamento e o cancelamento de direitos de acesso a serviços e sistemas de informação do MPT devem ser controlados mediante procedimentos formais;

III. Os usuários dos serviços e sistemas de informação do MPT devem estar conscientes de suas responsabilidades para manter o efetivo controle de acesso, particularmente em relação ao uso de senhas, consideradas, sem exceção, pessoais e intransferíveis;

IV. O acesso aos serviços e sistemas do MPT por meio equipamentos particulares ou de terceiros respeitará procedimentos de controle formais, de modo que os proprietários desses equipamentos assumam compromisso de respeitar a política, as normas e os procedimentos de segurança da informação;

V. O controle e a compartimentação de acesso entre a rede corporativa do MPT e redes externas, privadas ou públicas, deverão ser normatizados de forma a contemplar requisitos da política, das normas e dos procedimentos de segurança da informação;

VI. Os limites de uso da rede do MPT por dispositivos remotos ou móveis serão definidos de forma a garantir o respeito à segurança da informação no MPT.

Art. 8º São diretrizes relativas à aquisição, ao desenvolvimento e à manutenção de sistemas de informação:

I. Os requisitos de segurança da informação deverão ser identificados, qualificados e monitorados durante todas as etapas do projeto, do desenvolvimento ou da aquisição de serviços e sistemas de informação, a incluir documentações, códigos-fonte e dados relacionadas a testes;

II. Os modelos de interação e de segurança deverão ser documentados para todo serviço ou sistema que armazene, manipule ou transmita informação classificada em qualquer grau de sigilo;

III. Controles criptográficos e controles para a salvaguarda das chaves de criptografia deverão ser criados para a proteção da informação classificada em qualquer grau de sigilo;

IV. Os métodos de teste de software e de homologação dos sistemas deverão incluir, antes do ingresso em produção, as validações necessárias para identificar, avaliar e tratar possíveis vulnerabilidades de segurança;

V. Os contratos de aquisição e prestação de serviços de sistemas de informação deverão incluir cláusulas que garantam o cumprimento da política, das normas e dos procedimentos de segurança da informação do MPT, com previsão de sanções administrativas, civis e penais para os casos de violação.

Art. 9º São diretrizes relativas à gestão de risco:

I. O processo de gestão de risco para os serviços e sistemas de informações do MPT deverá ser normatizado de forma a contemplar diretrizes de planejamento, mapeamento, análise quantitativa, análise qualitativa, avaliação, priorização, tratamento e prevenção;

II. A gestão de risco dos serviços e sistemas de informação do MPT constituirá processo contínuo cujas ações dependerão da classificação do grau de sigilo e da criticidade da informação;

III. Os riscos à segurança da informação deverão ser reduzidos progressivamente a níveis objetivamente definidos por autoridade competente, considerando seu grau de sigilo, valor, criticidade e sensibilidade para o MPT e outras instituições, nos limites da lei e dos ditames constitucionais

Art. 10 São diretrizes relativas à gestão de incidentes em segurança da informação:

I. O processo de gestão de incidentes em segurança da informação deverá ser normatizado de forma a contemplar atividades de detecção, priorização, análise, tratamento, comunicação e prevenção;

II. As atividades de análise e de tratamento de incidentes em segurança da informação deverão ser cobertas por procedimentos que visem à preservação da integridade de evidências a fim de não comprometer sua validade em processos administrativos, civis ou penais;

III. O processo de gestão de incidentes em segurança da informação deve conter procedimentos para coordenação do tratamento do incidente entre as unidades do MPT e, sempre que necessário, em articulação com órgãos externos.
Art. 11 São diretrizes relativas ao modelo de medição da segurança da informação:

I. A medição de segurança da informação deverá ser realizada mediante modelo normatizado com o objetivo de avaliar a eficácia dos controles e medidas de segurança e de forma a garantir a verificação da extensão de conformidade com as diretrizes gerais e requisitos específicos de segurança da informação;

II. O modelo a que se refere o inciso I deverá considerar a coleta, a seleção de controles, os métodos de medição, a função de medição, o modelo analítico, os indicadores e os critérios para a tomada de decisão;

III. A análise e a interpretação fundadas no modelo de medição devem fornecer ao CETI informações para a tomada de decisões estratégicas a respeito do aprimoramento da gestão da segurança da informação.

Art. 12 São Diretrizes relativas à auditoria e à conformidade:

I. O seguimento da Política e das normas de segurança da informação será aferido mediante processos de auditoria interna e de conformidade;

II. As atividades da auditoria interna devem estar definidas em programas de auditoria que contenham objetivos, estipulação de abrangência, procedimentos, critérios, métodos e responsabilidades;

III. O processo de conformidade deve contemplar a análise crítica dos requisitos de segurança da informação estabelecidos na Política e Normas de Segurança da Informação do MPT, em normas constitucionais, legais e regulamentares aplicáveis e em resoluções do Conselho Superior do MPT e do Conselho Nacional do Ministério Público relacionadas, direta ou indiretamente, à segurança da informação;

IV. O modelo de medição de segurança da informação deve ser considerado fonte de evidências da eficácia dos controles e das medidas de segurança e de conformidade.

V. Os processos de auditoria e conformidade devem compreender a proteção da propriedade intelectual.

Art. 13. São diretrizes relativas à gestão de continuidade de negócio:

I. O processo de gestão de continuidade de negócio será normatizado para garantir a manutenção e a recuperação das operações em tempo compatível com a criticidade dos serviços e sistemas e de forma a assegurar as propriedades da informação classificada em qualquer grau de sigilo;

II. Os sistemas classificados como críticos por autoridade competente receberão planos de continuidade de negócio específicos;

III. Os sistemas classificados como não críticos por autoridade competente receberão planos para a manutenção de necessária infraestrutura tecnológica;

IV. Análises de risco deverão anteceder os planos de continuidade de negócio;

V. Os planos de continuidade de negócio devem ser testados e reavaliados conforme periodicidade definida por autoridade competente.

Art. 14 São responsabilidades do CETI, consoante diretrizes definidas pelo Procurador-Geral do Trabalho:

I. Discutir e aprovar, inclusive em caráter revisional, as propostas de Política e de normas de segurança da informação;

II. Identificar os sistemas e os bancos de dados críticos do MPT;

III. Identificar e definir diretrizes de gestão dos bancos de dados públicos ou privados críticos armazenados no MPT para uso institucional;

IV. Definir o escopo e a periodicidade das análises de risco bem como o risco residual aceitável para cada serviço e sistema de informação, considerado todos os graus de sigilo;

V. Definir a periodicidade dos testes dos planos de continuidade de negócio;

VI. Definir a frequência e o escopo de auditorias e de verificações de conformidade.

VII. Classificar, reclassificar e desclassificar informações com maior grau de sigilo no âmbito do MPT;

VIII. Indicar gestores de serviços e sistemas que manipulem, armazenem ou trafeguem informações em qualquer grau de sigilo.

Art. 15 São responsabilidades dos dirigentes das áreas de Tecnologia da Informação das unidades do MPT:

I. Zelar pelo cumprimento da política e das normas de segurança da informação conforme sua área de atuação;

II. Propor, de forma colegiada, procedimentos de segurança da informação, conforme a Política e as normas de segurança da informação;

III. Tratar os incidentes de segurança da informação que ocorrem na sua área de atuação conforme norma específica de tratamento de incidentes.

Art. 16 São responsabilidades dos gestores dos sistemas de informação do MPT:

I. Classificar, reclassificar e desclassificar informações dos sistemas pelos quais são responsáveis, ressalvadas as informações com maior grau de sigilo no âmbito do MPT (artigo 14, VII);

II. Autorizar e atualizar as liberações de acesso à informação sob sua responsabilidade, de acordo com matriz de cargos e funções padronizada nacionalmente e consoante política e as normas de segurança da informação do MPT.

Art. 17 São responsabilidades dos custodiantes dos sistemas de informação do MPT:

I. Garantir o funcionamento dos mecanismos de segurança da informação conforme os requisitos de segurança previamente definidos;

II. Identificar desvios em relação à política e às normas de segurança da informação, de modo que as ocorrências impliquem a adoção de providencias e as ações corretivas necessárias;

III. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade.

Art. 18 São responsabilidades dos usuários dos serviços e sistemas de informação do MPT, a incluir membros, servidores e colaboradores:

I. Cumprir a política, as normas e os procedimentos de segurança da informação sob pena de responsabilidade administrativa, civil ou criminal, conforme prescrições, limites e ritos definidos em lei;

II. Buscar orientação entre os pares ou superiores hierárquicos em caso de dúvidas relacionadas à segurança da informação;

III. Proteger as informações sob sua custódia contra acesso indevido, modificação, destruição ou divulgação não-autorizados pelo MPT;

IV. Comunicar ao seu superior hierárquico imediato ou à autoridade competente qualquer descumprimento ou violação da política, das normas ou dos procedimentos de segurança da informação do MPT.

Art. 19 São responsabilidades da Gerência de Segurança Institucional do MPT:

I. Identificar riscos à segurança da informação;

II. Propor normas e procedimentos de segurança da informação.

Art. 20 Caberá aos Departamentos de Administração das unidades do MPT:

I. Alocar recursos para a implementação das medidas necessárias para cumprimento da política, das normas e dos procedimentos de segurança da informação do MPT;

II. Incluir, nos contratos administrativos que envolvam serviços e sistemas de informação, cláusulas alinhadas com a política, as normas e os procedimentos de segurança da informação do MPT.

Art. 21 Os casos omissos serão resolvidos pelo CETI, em Nota Técnica, ouvidos os interessados.

Art. 22 Esta resolução entra em vigor na data de sua publicação.

Luis Fabiano de Assis
Procurador do Trabalho
Presidente do Comitê Estratégico de Tecnologia da Informação do MPT