MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO –

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 21, de 22 de março de 2021

Institui a Política Nacional de Segurança de Tecnologia 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*);

CONSIDERANDO a Lei 12.965/2014 (Marco Civil da Internet), a Lei 12.527/2011 (Lei de Acesso à Informação), 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e legislação correlata.

RESOLVE:

Art. 1º Instituir a Política Nacional de Segurança de Tecnologia da Informação do Ministério Público do Trabalho mediante o estabelecimento de diretrizes e

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

responsabilidades para a elaboração de normas e procedimentos a serem cumpridos por membros, servidores e demais usuários que acessam informações do MPT.

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

§2º A estrutura normativa de SegTI no MPT compreende:

I. Em Nível Estratégico, a Política Nacional de SegTI definida nesta resolução, onde são estabelecidas as diretrizes gerais do MPT;

II. Em Nível Tático, as normas de SegTI, que estabelecem os controles específicos a serem implementados para cumprir as diretrizes estabelecidas na Política;

III. Em Nível Operacional, as notas técnicas de SegTI, que consistem em procedimentos que instrumentalizam as normas por meio de escolhas tecnológicas e de configurações específicas de controle em todas as unidades do MPT.

§ 3º Para os efeitos desta resolução, das normas e das notas técnicas a serem produzidas em consonância com as diretrizes ora estabelecidas, consideram-se os termos e definições constantes no Anexo.

Art. 2º São princípios da SegTI 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. A Compartimentação ou Segregação 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 O Gestor da Informação é responsável por classificar e definir os requisitos de garantia das propriedades da informação que está sob sua responsabilidade.

§ 1º Para fins de aplicação desta política e normas de SegTI, considera-se Gestor da Informação:

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

I - Membro do Ministério Público do Trabalho, em relação às informações produzidas em decorrência de suas atividades institucionais;

II - Chefe de unidade administrativa do MPT na qual a informação é produzida ou manipulada;

III - Servidor designado, por nomeação ou delegação, atendido o princípio da necessidade de conhecer.

§ 2º Os gestores da informação devem observar o disposto em normatização do MPT que verse sobre a classificação, o tratamento e a gestão da informação.

Art. 4º O Custodiante da Informação é quem, por força de suas atribuições funcionais ou contratuais, gerencia ou administra os meios técnicos para a preservação da informação consoante os requisitos de segurança definidos pelo Gestor da Informação.

§1º Para fins de aplicação desta política e normas de SegTI, considera-se custodiante o agente responsável pelos processos de tratamento da informação, tais como:

a) gestores de sistemas de tecnologia da informação do MPT;

b) administradores e desenvolvedores de sistemas e serviços de tecnologia da informação;

c) os fiscais de contratos que envolvam tratamento de informações.

§2º São responsabilidades do Custodiante da Informação:

a) garantir o funcionamento dos mecanismos de SegTI conforme os requisitos de segurança previamente definidos;
b) identificar desvios em relação à política e às normas de SegTI, de modo que as ocorrências impliquem a adoção de providencias e as ações corretivas necessárias;
c) participar da investigação de incidentes de segurança relacionados à informação sob sua custódia.

Art. 5º São diretrizes relativas à Gestão da Informação, necessárias à garantia integral de suas propriedades e princípios:

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

I. A informação produzida ou recebida pelo MPT deverá ser tratada, em todo o seu ciclo de vida, 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. Para toda informação deverá ter um proprietário, que é o gestor de informação, e um ou mais custodiantes;

IV. Toda informação deverá ser classificada, reclassificada ou desclassificada, consoante normatização do MPT que trata da classificação da informação, 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;

V. As informações classificadas como em qualquer grau de sigilo deverão ter mecanismos de tratamento que garantam sua compartimentação, com camadas adicionais de segurança e o uso de criptografia para o armazenamento;

VI. O compartilhamento de informações classificadas em qualquer grau de sigilo com outras instituições deverá ser realizado mediante um processo definido de credenciamento de segurança, exigindo a aplicação de normas e instrumentos para compartimentação com preservação do mesmo grau de sigilo;

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

VIII. As informações disponíveis em repositórios de acesso público devem ser publicadas em plataformas de gerenciamento de conteúdo que permitem a verificação automática da integridade e da autenticidade e auditoria.

Art. 6º A proteção de dados pessoais nos meios de tecnologia da informação deve estar alinhada à Política Nacional de Proteção de Dados Pessoais do MPT, de forma a atender as exigências da Lei 13.709/2018, bem como atos normativos da Agência Nacional de Proteção de Dados.

Art. 7º São diretrizes relativas aos usuários dos serviços de tecnologia da informação do MPT:

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

II. Todo aquele que obtiver acesso à informação classificada em qualquer grau de sigilo fica obrigado a resguardar seus requisitos de segurança, mediante Termo de Compromisso de Manutenção de Sigilo;

III. Os contratos de prestação de serviços devem prever a necessidade de assinatura individual de Termo de Compromisso de Manutenção de Sigilo para acesso à informação classificada em qualquer grau de sigilo;

IV. O tema SegTI deve ser abordado em cursos de formação e em programas de ambientação;

V. Os servidores lotados na área de tecnologia da informação deverão receber treinamentos específicos em segurança da informação, conforme as respectivas atribuições.

Art. 8º São diretrizes relativas à Gestão de Ativos e do Ambiente Físico:

I. Paralelamente ao inventário e aos controles de patrimônio, os ativos que suportam os serviços e sistemas de informação devem ser mapeados como itens de configuração a fim de garantir o controle e a cadeia de dependência e facilitar o tratamento de incidentes;

II. A alienação, a doação e o descarte de ativos que armazenem informação classificada em qualquer grau de sigilo deverão respeitar procedimento formal para a eliminação irreversível dos dados;

III. Em caso de manutenção por terceiros em ativos que armazenam informação classificada em qualquer grau de sigilo, devem-se adotar mecanismos de preservação do sigilo;

IV. As instalações físicas dos serviços e 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;

V. É proibido às áreas de tecnologia da informação das unidades do MPT executar manutenções, seja de hardware ou de software, em equipamentos particulares dos usuários.

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

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. 9º São diretrizes relativas à gestão das operações e das comunicações:

I. A criação, manutenção e desativação de serviços e sistemas de informação do MPT requerem a indicação de um responsável e devem obedecer a procedimentos específicos, que permitam o acompanhamento durante todo o ciclo de vida;

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

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

IV. Os serviços, os sistemas e as redes de comunicação de dados do MPT devem ser gerenciados e monitorados 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 quaisquer das propriedades da informação;

VI. Todos os registros de eventos (*logs*) dos ativos que suportam serviços e sistemas de informação do MPT devem ser coletados e armazenados, com temporalidade de retenção mínima que atenda à Lei 12.965/2014 (Marco Civil da Internet) e, para dados pessoais protegidos pela Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) conforme regulamentação da Autoridade Nacional de Proteção de Dados Pessoais;

VII. Os relógios de todos os ativos que suportam serviços e sistemas 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.

Parágrafo único. Os registros de eventos (*logs*) deverão ser centralizados com adoção de mecanismos de segurança que garantam a integridade, autenticidade e confidencialidade dos dados.

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Art. 10 São diretrizes relativas à aquisição, ao desenvolvimento e à manutenção de serviços e sistemas de informação:

I. Os requisitos de SegTI deverão ser identificados, qualificados, desenvolvidos, testados e monitorados durante todas as etapas do projeto, a incluir documentações, códigos-fonte e dados relacionadas a testes;

II. Em qualquer hipótese deverá ser observado o modelo de requisitos básicos de segurança do MPT, a ser definido em norma específica, o que não esgota a necessidade em definir novos requisitos que levem em consideração as características peculiares de cada sistema;

III. Deverão ser implementados controles criptográficos e controles para salvaguarda das chaves de criptografia, para a proteção da informação classificada em qualquer grau de sigilo;

IV. Sistemas com acesso disponibilizado na internet deverão obrigatoriamente incluir requisitos que mitiguem ataques cibernéticos, como validação de todos os dados de entrada, controle rígido de acesso e autenticação, controle de injeção de dados, hospedagem em rede segregada, conforme o nível de segurança;

V. 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, sendo vedada a utilização de dados reais sem a devida descaracterização e, para o caso de dados pessoais, a sem devida anonimização;

VI. 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;

VII. 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 SegTI do MPT, com previsão de sanções administrativas, civis e penais para os casos de violação;

VIII. Todo serviço ou sistema de informação, desenvolvido ou adquirido, deverá gerar registro de *log*, em arquivo próprio e com cópia em um serviço centralizado de *logs*, contendo eventos de acesso e das operações realizadas para permitir a auditoria e rastreabilidade de acesso aos dados na ocorrência de incidentes de segurança;

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

IX. Todo serviço ou sistema de informação, atualizações e novas versões deverão passar por testes de vulnerabilidade e intrusão antes de entrar em operação;

X. As equipes de desenvolvimento deverão receber treinamento em desenvolvimento seguro.

§1º Para fins de aplicação dos incisos I, II, III, IV e VIII os sistemas em produção deverão ser adaptados para incluir a implementação de requisitos de segurança, conforme cronograma a ser aprovado pelo CETI.

§2º No caso de serviços e sistemas com interface para Internet, deverão ser implementadas, obrigatoriamente, boas práticas de segurança em aplicações WEB, conforme norma específica.

§3º Os serviços e sistemas de informação que estão em operação deverão passar por testes de vulnerabilidade e intrusão, conforme cronograma a ser aprovado pelo CETI.

Art.11 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, a necessidade de conhecer e o justo interesse institucional e da sociedade;

II. O registro, a concessão, a alteração, a revogação e a desabilitação de direitos de acesso à 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 SegTI;

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 SegTI.

Art. 12 São diretrizes relativas ao acesso remoto aos serviços e sistemas de informação do MPT:

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

I. Os acessos remotos realizados a partir da internet para a rede corporativa do MPT só poderão ser ultimados por intermédio de programas ou serviços que garantam a autenticação dos usuários e a criptografia dos dados nas camadas de rede, transporte ou aplicação, conforme arquiteturas e modelos de comunicação adotados nacionalmente pelo MPT;

II. Os serviços de acesso remoto deverão registrar em arquivos de *log* todos os acessos dos usuários, incluindo as tentativas mal sucedidas e em conformidade com a temporariedade definida por Lei;

III. O usuário é responsável pela administração e segurança do equipamento contra a ameaças de acesso não autorizado à informação por outras pessoas que utilizam o local, sendo recomendada a configuração de usuário e senha locais;

IV. O equipamento utilizado para acesso remoto à rede e serviços do MPT deve estar em conformidade com as configurações de segurança definidas em norma específica;

V. O acesso remoto deverá ser autorizado mediante procedimento formal, com a definição do trabalho permitido, o período de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar.

Art. 13 São diretrizes para implementação ou contratação de serviços de nuvem:

I. Independente do modelo de implantação ou de serviços, a governança de dados é sempre do MPT;

II. Todo contrato de prestação de serviço em nuvem deve, no mínimo, conter:

a) Especificação objetiva do modelo de implantação e de serviço;

b) Especificação da política de localização e soberania dos dados;

c) Definição dos Acordos de Nível Serviço;

d) Especificação das regras para proteção de dados pessoais;

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

e) Especificação dos controles de segurança da informação;

f) Matriz de responsabilidades da contratada e contratante;

g) Penalidades aplicadas à contratada em caso de descumprimento das cláusulas contratuais relativas à segurança da informação.

§1º A política de localização e soberania dos dados deve especificar os locais onde os dados devem estar armazenados ou onde nunca poderão estar armazenados.

§2º A contratada para prestação de serviços em nuvem deve declarar explicitamente seguir a Lei 13.709, de 14/08/2018, Lei Geral de Proteção de Dados Pessoais – LGPD.

§3º É um critério para a localização do armazenamento dos dados, que o país ou a respectiva unidade federativa possua uma lei para capaz de prover o mesmo nível de proteção de dados pessoais que a Lei 13.709, de 14/08/2018, Lei Geral de Proteção de Dados Pessoais -LGPD.

§4º Todo contrato de prestação de serviço em nuvem deve incluir relatórios mensais de conformidade para verificação tanto da execução do contrato quanto para verificação da efetividade dos controles objetivos de qualidade e, principalmente, de segurança da informação e proteção de dados pessoais.

§5º Os contratos de serviços de nuvem devem prever tanto o envio de dados do MPT para a nuvem, bem como a transferência de dados da nuvem para armazenamento na infraestrutura do MPT.

Art. 14 São diretrizes relativas à gestão de risco em tecnologia da informação:

I. O processo de gestão de risco para os serviços e sistemas de informações do MPT deverá ser implementado conforme norma específica, 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 e da criticidade da informação;

III. Os riscos à SegTI 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;

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 ser 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.

Art. 15 São diretrizes relativas à gestão de continuidade de serviços de tecnologia da informação:

I. O processo de gestão de continuidade de serviços de tecnologia da informação deverá ser implementado, conforme norma específica, 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;

II. Os serviços e sistemas classificados como críticos por autoridade competente serão atendidos por planos de continuidade específicos;

III. Os serviços e sistemas classificados como não críticos por autoridade competente serão atendidos por planos de continuidade da infraestrutura tecnológica;

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

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

Art. 16 São diretrizes relativas ao tratamento de incidentes em SegTI:

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

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

II. As atividades de análise e de tratamento de incidentes em SegTI 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 tratamento de incidentes em SegTI deve conter procedimentos para coordenação e articulação entre as unidades do MPT e, sempre que necessário, com órgãos externos.

§1º O processo de tratamento de incidentes será operacionalizado por uma equipe de tratamento e resposta de incidentes de segurança da informação CSIRT/MPT, formalmente designada.

§2º O processo de tratamento de incidentes deve prever a articulação da equipe de resposta de incidentes com as áreas especializadas do MPT e com as áreas de tecnologia da informação das Regionais.

§3º O processo de tratamento de incidentes será iniciado por meio de alertas de sistemas de monitoramento de segurança, notificações internas registradas no sistema de atendimento ao usuário e notificações externas.

Art. 17 São diretrizes relativas ao modelo de medição da SegTI:

I. A medição de SegTI 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 SegTI;

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 SegTI.

Art. 18 São Diretrizes relativas à auditoria e à conformidade em SegTI:

I. A política e as normas serão aferidas mediante processos de auditoria interna e de conformidade;

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

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 SegTI estabelecidos na política e normas 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 SegTI;

IV. O modelo de medição de SegTI 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. 19 São responsabilidades do CETI, consoante diretrizes definidas pelo Procurador-Geral do Trabalho:

I. Aprovar a política e as de normas de SegTI;

II. Aprovar o escopo e a periodicidade:

a) das análises de risco;
b) dos testes dos planos de continuidade;
c) das auditorias e das verificações de conformidade de SegTI;
d) dos testes de vulnerabilidade e intrusão em serviços e sistemas de tecnologia da informação.

III. Apreciar o resultado das análises de risco e decidir sobre os riscos a serem mitigados e os riscos residuais aceitáveis;

IV. Apreciar o resultado das auditorias e das verificações de conformidade de SegTI e determinar as ações corretivas necessárias.

Art. 20 São responsabilidades do Subcomitê de Governança Corporativa de Tecnologia da Informação:

I. Revisar a política nacional de SegTI;

II. Elaborar e revisar normas específicas sobre SegTI;

III. Acompanhar as ações do PDTI Nacional relativas à SegTI;

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

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

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

VI. Propor ao CETI o escopo e a periodicidade:

a) das análises de risco;

b) dos testes dos planos de continuidade;

c) das auditorias e das verificações de conformidade de SegTI;

d) dos testes de vulnerabilidade e intrusão em serviços e sistemas de tecnologia da informação.

VII. Apresentar ao CETI os relatórios de riscos de TI e propor ações para mitigação dos riscos verificados e critérios de aceitação do risco;

VIII. Apresentar ao CETI o resultado das auditorias e das verificações de conformidade de SegTI e propor as ações corretivas necessárias.

Parágrafo Único. O CETI poderá designar formalmente um grupo de trabalho nacional de segurança da informação, composto por servidores de TI do MPT com habilidades e competências correlatadas, para realização de projetos e execução de ações relativas à SegTI.

Art. 21 São responsabilidades dos Subcomitês Diretivos de Tecnologia da Informação – SDTI:

I. Zelar pelo cumprimento da política e das normas de SegTI;

II. Promover a conscientização e educação das práticas de SegTI;

III. Decidir sobre solicitações específicas de uso de recursos de TI, mediante parecer técnico da área de tecnologia da informação, em consonância com a política e normas de segurança, sem prejuízo de posterior revisão do CETI;

VI. Propor ao SGCTI alterações na política nacional e normas ao SGCTI.

Art. 22 São responsabilidades dos dirigentes das áreas de Tecnologia da Informação das unidades do MPT:

I. Realizar a análise de riscos de SegTI do ambiente computacional sob sua responsabilidade, aplicar controles para redução dos riscos e encaminhar relatórios de gestão de riscos ao SGCTI;

II. Implementar a continuidade de serviços de tecnologia da informação, conforme norma específica;

III. Notificar à equipe de tratamento de incidentes de SegTI e colaborar para o tratamento de incidentes relativos ao ambiente computacional sob sua responsabilidade em articulação com o CSIRT-MPT;

V. Garantir a conformidade do ambiente computacional sob sua responsabilidade com a política e normas de SegTI.

Art. 23 São responsabilidades dos usuários dos serviços e sistemas de informação do MPT:

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

II. Aceitar explicitamente o Termo de Compromisso de Manutenção de Sigilo, para acesso à informação classificada;

III. Buscar orientação entre os pares ou superiores hierárquicos em caso de dúvidas relacionadas à SegTI;

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

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

VI. Comunicar à equipe de tratamento de incidentes de SegTI sobre qualquer suspeita de ocorrência de ação que viole a política e normas de SegTI.

Parágrafo Único: essas responsabilidades também se aplicam para usuários em atividades de trabalho remoto.

Art. 24 Cabe às áreas 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 SegTI do MPT;

II. Incluir, nos contratos administrativos que envolvam serviços e sistemas de tecnologia da informação, cláusulas para garantir o cumprimento da a política, das normas e dos procedimentos de SegTI do MPT.

Art. 25 O cumprimento das diretrizes estabelecidas nessa política requer, no mínimo, a publicação das seguintes normas:

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

a) De uso de recursos de TI;

b) De controle de acesso lógico;

c) De gestão de continuidade de serviços de TI;

d) De gestão de riscos de SegTI;

e) De testes de vulnerabilidades e intrusão;

f) De segurança em desenvolvimento de sistemas e serviços de TI;

g) De gestão de incidentes de SegTI.

Art. 26 A equipe de resposta a incidentes de SegTI deverá ser formalmente constituída e seus componentes nomeados em até trinta dias após a publicação desta política.

Art. 27 Esta política deverá ser revisada ordinariamente a cada dois anos ou extraordinariamente por decisão do CETI.

Art. 28 Os casos omissos serão resolvidos pelo CETI, em Nota Técnica, ouvidos os interessados.

Art. 29 Esta resolução entra em vigor na data de sua publicação.

Art.30 Revogam-se a Resolução CETI nº 4, de 7 de março de 2016 e a Resolução CETI n.º 5, de 7 de março de 2016.

LUIS FABIANO PEREIRA

Procurador do Trabalho

Presidente do Comitê Estratégico

de Tecnologia da Informação do MPT

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

ANEXO

Definições:

1. Ameaça: qualquer ação, acidental ou intencional, que pode prejudicar ou causas danos às propriedades da informação.
2. Autenticidade: propriedade ou atributo de identidade do criador, manipulador, armazenador, transmissor ou responsável pelo descarte da informação.
3. Classificação da informação: ação de definir o nível de sensibilidade da informação a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sigilo e criticidade para o MPT.
4. Informação classificada em qualquer grau de sigilo: conforme da Lei 12.527 (Lei de Acesso à Informação), Art. 24: *"A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada."*
5. Computação em nuvem: é um modelo que permite o acesso via rede, a partir de qualquer lugar e de forma adequada e sob demanda, a um agrupamento de recursos computacionais que podem ser rapidamente provisionados e disponibilizados, com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços.
6. Ciclo de vida da informação: transformações da informação desde sua criação, passando pela manipulação, armazenamento e transmissão, até o seu descarte.
7. Confidencialidade: propriedade ou atributo de proteção, em consonância com o grau de sigilo da informação.
8. Controles de segurança: conjunto de soluções tecnológicas, políticas, processos e procedimentos que reduzem o risco.
9. CSIRT/MPT: acrônimo de *Computer Security Incident Response Team* internacionalmente utilizado para designar equipe de tratamento e resposta de incidentes de segurança da informação.
10. Disponibilidade: propriedade ou atributo que garante o acesso à informação quando houver necessidade.
11. Gestão de riscos: processo que consiste na identificação, análise, avaliação e tratamento dos riscos em tecnologia da informação.
12. Incidente de SegTI: qualquer evento, acidental ou intencional, que violar as propriedades da informação em seu ciclo de vida.
13. Integridade: propriedade ou atributo que garante a preservação do conteúdo da informação conforme a exatidão e a intenção de quem a criou ou manipulou.
14. Modelo de interação de sistemas e serviços: é representação de como as partes de um sistema interagem entre si e com outros sistemas. Por exemplo: conexões TCP ou UDP relacionadas à interação tanto do usuário com a aplicação, quanto da aplicação com outros componentes, como banco de dados e outros serviços internos ou externos.

SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

15. 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.
16. Propriedades ou atributos da informação: autenticidade, confidencialidade, disponibilidade, integridade e não repúdio.
17. Recursos de Tecnologia da Informação: conjunto de bens, ativos, sistemas e serviços que compõem a arquitetura tecnológica do MPT na qual a informação é criada, manipulada, transmitida, armazenada e descartada.
18. Risco de Tecnologia da Informação: é a probabilidade de uma ameaça explorar uma vulnerabilidade que afeta as propriedades das informação causando impacto negativo aos negócios da instituição.
19. Segurança de Tecnologia da Informação – SegTI: é a garantia das propriedades da informação durante todo o seu ciclo de vida, por meio da adoção de controles de segurança.
20. Tratamento da informação: toda operação realizada com informações, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
21. Usuários: membros, servidores, colaboradores, aposentados, pensionistas, estagiários e menores aprendizes, bem como aos demais agentes públicos ou particulares que, oficialmente, executem atividades que interajam com a rede do MPT ou utilizem os serviços e sistemas de TI nela disponíveis.
22. Vulnerabilidade: é um estado de fragilidade ou fraqueza dos ativos, dos processos ou das pessoas, que expõe as propriedades da informação a uma potencial ameaça.