

PORTARIA Nº 1.047, DE 16 DE JULHO DE 2013

MINISTÉRIO DO TRABALHO E EMPREGO

GABINETE DO MINISTRO

DOU de 17/07/2013 (nº 136, Seção 1, pág. 92)

Aprova a Política de Segurança da Informação e Comunicações - Posic do Ministério do Trabalho e Emprego.

O MINISTRO DE ESTADO DO TRABALHO E EMPREGO - INTERINO, no uso das suas atribuições legais e considerando o disposto na Norma Complementar 03/IN01/DSIC/GSIPR, de 10 de junho de 2009, e deliberações do Comitê de Segurança da Informação e Comunicações - CSIC, resolve:

Art. 1º - Aprovar a Política de Segurança da Informação e Comunicações - Posic do Ministério do Trabalho e Emprego - MTE.

Seção I

Do Escopo

Art. 2º - A Política de Segurança da Informação e Comunicações - Posic objetiva, observando a legislação e normas específicas em vigor, instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade, autenticidade e legalidade dos dados, informações e documentos do MTE, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional.

Art. 3º - A Posic trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do MTE, em todo o seu ciclo de duração - criação, manuseio, divulgação, armazenamento, transporte e descarte -, visando à continuidade de seus processos vitais, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4º - Esta Posic se aplica a todas as unidades da estrutura regimental do MTE, incluindo as unidades descentralizadas, órgãos colegiados, bem como a servidores, prestadores de serviço, colaboradores, fornecedores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este Ministério.

Parágrafo único - Esta Política também se aplica, no que couber, ao relacionamento do MTE com outros órgãos e entidades públicas ou privadas.

Seção II

Dos Conceitos e Definições

Art. 5º - Para efeitos desta Posic, fica estabelecido o significado dos seguintes termos e expressões:

I - ameaça: conjunto de fatores externos ou causa potencial de um incidente, que pode resultar em dano para um sistema ou para o MTE;

II - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - autenticidade: propriedade que assevera que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso;

IV - Comitê de Segurança da Informação e Comunicações: grupo de representantes de unidades do

MTE com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações;

V - confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental;

VI - criticidade: grau de importância da informação para a continuidade das atividades e serviços do MTE;

VII - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

VIII - incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IX - integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;

X - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócios, caso essas ameaças se concretizem;

XI - gestão de riscos de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XII - recursos de tecnologia da informação e comunicações: recursos que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, *notebooks*, servidores de rede, equipamentos de conectividade e infraestrutura;

XIII - resiliência: capacidade de enfrentamento ágil de situações inesperadas e de superação das adversidades para restabelecer processo de normalidade;

XIV - usuário: todo aquele que está autorizado a obter acesso a informações e sistemas; e

XV - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para o MTE, os quais podem ser evitados por uma ação interna de segurança da informação.

Seção III

Dos Princípios

Art. 6º - São princípios desta Posic:

I - a legalidade, a impessoalidade, a moralidade, a publicidade, a eficiência, a celeridade e a ética na proteção do ativo de informação;

II - a responsabilidade individual na utilização dos ativos de informação; e

III - o respeito à privacidade das informações pessoais.

Seção IV

Das Diretrizes Gerais

Art. 7º - Compete à Secretaria-Executiva, assessorada pelo Comitê de Segurança da Informação e Comunicações, normatizar a implantação e operacionalização das diretrizes previstas nesta Seção.

Subseção I

Da Gestão da Segurança da Informação e Comunicações

Art. 8º - A Gestão da Segurança da Informação e Comunicações não se limita à tecnologia da informação e comunicações, compreendendo as ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos.

Art. 9º - A Gestão de Segurança da Informação e Comunicações deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicações.

Subseção II

Do Tratamento e Classificação da Informação

Art. 10 - A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do MTE.

Art. 11 - O MTE deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 12 - Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo MTE e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Subseção III

Da Sensibilização, Conscientização e Capacitação

Art. 13 - O MTE desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Subseção IV

Da Contratação de Terceiros

Art. 14 - Todos os contratos, convênios, acordos e instrumentos congêneres firmados pelo MTE devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta Posic e das normas dela derivadas.

Parágrafo único - O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Posic e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no MTE.

Subseção V

Da Gestão de Riscos

Art. 15 - As áreas responsáveis por ativos da informação devem implementar processo contínuo de gestão de riscos no âmbito de suas competências, o qual será aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações.

Subseção VI

Da Gestão de Continuidade

Art. 16 - Todas as áreas do MTE devem promover a continuidade de suas atividades e serviços do MTE, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo

hábil, quando for o caso.

Art. 17 - A resiliência do MTE contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática pró-ativa de todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional do MTE.

Art. 18 - As informações institucionais, se eletrônicas, devem ser guardadas nos ambientes de armazenamento, homologados pela área de tecnologia de informação do MTE e, se não eletrônicas, devem ser mantidas em local que as salvaguardem adequadamente, conforme as exigências legais.

Art. 19 - A área de tecnologia da informação do MTE deverá manter Plano de Contingências, gradado de acordo com o grau de probabilidade de ocorrência do evento ou sinistro, estabelecendo o conjunto de estratégias e procedimentos que devem ser adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

Subseção VII

Do Tratamento de Incidentes de Rede Computacional

Art. 20 - A área de tecnologia da informação manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, instituída pelo Comitê de Segurança da Informação e Comunicações, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Subseção VIII

Do Uso dos Recursos de Tecnologia da Informação e Comunicações

Art. 21 - Os recursos de tecnologia da informação e comunicações disponibilizados pelo MTE devem ser utilizados de acordo com seu propósito e seu uso deverá ser regulamentado em conformidade com a legislação vigente.

Parágrafo único - É expressamente proibido o acesso, guarda e encaminhamento de material não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios e recursos de comunicações disponibilizados pelo MTE.

Subseção IX

Da Auditoria e Conformidade

Art. 22 - O cumprimento desta Posic deve ser avaliado, periodicamente, em conformidade com normas complementares, manuais de procedimentos e legislação específica de segurança da informação e comunicações, buscando a certificação do atendimento dos requisitos de segurança da informação.

Art. 23 - A área de tecnologia da informação manterá registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e rede interna do MTE.

Subseção X

Dos Controles de Acesso

Art. 24 - Devem ser instituídas normas que estabeleçam procedimentos, processos e mecanismos de controle de acesso às informações, instalações e sistemas de informação do MTE, com o objetivo de garantir a segurança dos servidores e a proteção dos seus ativos.

Art. 25 - Por questão de segurança, é obrigatório o uso de crachá de identificação para acesso e permanência nas instalações do MTE.

Art. 26 - O usuário é responsável pela segurança dos ativos de informação que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, tais como: crachá, broche institucional, carimbo, login, senha eletrônica, certificado digital, assinatura digital e endereço de

correio eletrônico.

Art. 27 - Toda informação veiculada eletronicamente será alvo de controle e monitoração, e seu uso deve ser tão somente para fins corporativos relacionados às atividades do MTE.

Subseção XI

Da Propriedade Intelectual

Art. 28 - As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do MTE e não cabe a seus criadores qualquer forma de direito autoral.

Parágrafo único - Os direitos autorais relativos a programas de computador desenvolvidos por servidores ou colaboradores do MTE, durante a vigência de contrato ou de vínculo estatutário, no exercício de suas funções e com recursos do Ministério, pertencerão exclusivamente ao MTE.

Art. 29 - É vedada a utilização de informações produzidas por terceiros para uso exclusivo do MTE em quaisquer outros projetos ou atividades de uso diverso do estabelecido pelo Ministério, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Ministro, nos demais casos.

Seção V

Das Penalidades

Art. 30 - O usuário responderá disciplinar, civil e/ou penalmente pelo prejuízo que vier a ocasionar ao MTE, em decorrência do descumprimento das regras previstas nesta Posic e demais normas internas e legislação vigente.

Art. 31 - A desobediência às normas estabelecidas implicará na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

Seção VI

Das Competências e Responsabilidades

Art. 32 - Compete a Coordenação-Geral de Planejamento e Gestão Estratégica dar o suporte administrativo necessário à gestão da Posic.

Art. 33 - Cabe aos usuários de informações e sistemas do MTE:

I - conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta Posic, bem como os demais normativos e resoluções relacionados à segurança da informação e comunicações;

II - obedecer aos requisitos de controle especificados pelos gestores da informação;

III - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR; e

IV - assinar os termos de confidencialidade, responsabilidade e outros que venham ser instituídos por normas ou procedimentos decorrentes desta Posic.

Art. 34 - Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá:

I - comunicar, de imediato, todo incidente de segurança que ocorra no âmbito de sua unidade à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

II - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de segurança da informação e comunicações;

III - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação e comunicações; e

IV - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação e comunicações por parte dos usuários sob sua supervisão.

Art. 35 - Cabe às empresas de prestação de serviço contratadas fornecer toda a documentação dos sistemas, produtos e serviços relacionados ao objeto do contrato.

Seção VII

Da Divulgação

Art. 36 - Deverá ser dada ampla divulgação desta Posic a todos os servidores e colaboradores do MTE, inclusive com publicação permanente na página da intranet do MTE.

Parágrafo único - Cabe ao Gestor de Segurança da Informação e Comunicações providenciar a divulgação interna desta Posic.

Art. 37 - Na apresentação de prestador de serviços contratado será entregue um exemplar desta Posic.

Seção VIII

Da Atualização

Art. 38 - Esta Posic deverá ser atualizada, no máximo, a cada dois anos, a contar da data de sua publicação.

Seção IX

da Vigência

Art. 39 - Esta Posic entra em vigor na data de sua publicação.

Art. 40 - Fica revogada a Portaria nº 1.327, de 11 de junho de 2010.

PAULO ROBERTO DOS SANTOS PINTO