Dispõe sobre a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 11ª. Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 11ª. REGIÃO, no uso de suas atribuições legais e regimentais,

Considerando a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal com integridade, confidencialidade e disponibilidade.

Considerando que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

Considerando a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade.

RESOLVE:

Art. 1º Atualizar a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional do Trabalho da 11ª. Região.

Art. 2º Para os efeitos deste Ato, aplicam-se as seguintes definições:

I – Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

II – Integridade: Salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

III – Disponibilidade: Garantia de que usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessários;

IV – Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infra-estrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem.

V – Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT;

VI - Plano de Continuidade do Negócio: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

Art. 3º Foram observadas as seguintes refêrencias legais e normativas na elaboração desta PSI:

I - Decreto N° 4.553 de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Publicado em 30 de dezembro de 2002;

II - Lei N° 8.112 de 11 de novembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

III - Decreto N° 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Publicado em 14 de junho de 2000;

IV - Instrução Normativa GSI Nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. E as subsequentes Normas complementares IN01/DSIC/GSIPR 01, 02, 03, 04, 05, 06, 07 e 08;

V - Aplicação de boas práticas em Tecnologia da Informação recomendadas pela Corte de Contas da União (TCU) e assinaladas na edição dos Acórdãos 71/2007 - Plenário, 1092/2007- Plenário e 2023/2005 – Plenário;

VI - ABNT (2006) "Tecnologia da Informação – Sistema de gestão da segurança da informação – Requisitos (NBR ISO/IEC 27001)". ABNT. 2006;

VII - ABNT (2005) "Tecnologia da Informação – Código de prática para a gestão da segurança da informação (NBR ISO/IEC 27002)". ABNT. 2005.

Art. 4º A PSI neste Tribunal é guiada pelos seguintes princípios:

I – Responsabilidade: as responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas;

II – Conhecimento: para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários;

III – Ética: todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados ao prover um sistema de informação e ao estabelecer um sistema de segurança;

IV – Legalidade: processos de segurança devem levar em consideração os objetivos e a Missão do Ministério da Justiça; bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais;

V – Integração: os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente;

VI – Celeridade: as ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível;

VII – Revisão: as sistemas de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo.

Art. 5º Esta política se aplica, no que couber, às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito deste Tribunal ou quem quer que venha a ter acesso a dados ou informações protegidos por esse regulamento.

Art. 6º O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade da prestação jurisdicional deste Tribunal.

§1º Os recursos de tecnologia da informação pertencentes a este Tribunal, disponíveis para o usuário, serão utilizados em atividades estritamente relacionadas às suas funções institucionais.

§ 2º A utilização dos recursos de tecnologia da informação será monitorada, sendo seus registros mantidos pela Secretaria de Tecnologia da Informação.

Art. 7º As informações geradas no âmbito deste Tribunal são de sua propriedade, independente da forma de sua apresentação ou armazenamento, e serão adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades institucionais deste Tribunal.

Parágrafo único: Toda informação gerada neste Tribunal deverá ser classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

Art. 8º Será criado o Comitê de Segurança da Informação, composto por pelo menos um representante de cada uma das seguintes áreas: Judiciárias de primeiro e segundo graus, Jurídica, Administrativa, Presidência, Corregedoria, Tecnologia da Informação e o Gestor de Segurança da Informação.

Art. 9º Será criado o Escritório de Segurança da Informação, vinculado à Secretaria de Tecnologia da Informação com o objetivo de prover soluções de segurança que agreguem valor aos serviços prestados por este Tribunal.

Art. 10º O descumprimento das normas referentes à PSI deste Tribunal sujeitará o infrator às sanções administrativas e penais previstas em legislação vigente.

Art. 11º Visando detalhar as obrigações indicadas nesta PSI, normas complementares, discutidas e aprovadas pelo Comitê de Segurança da Informação , serão mantidas em documentos a parte, disponíveis a partir da página principal da intranet institucional ou em site específico mantido por este Tribunal.

Art. 12º Os instrumentos normativos gerados a partir desta PSI devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 2 (dois) anos.

Art. 13º O presente Ato entra em vigor a partir da data de sua publicação.

Art. 14º Fica revogado o Ato n.º 66/2007 de 05 de Julho de 2007.

Manaus, 25 de Outubro de 2010.

Luíza Maria de Pompei Falabela Veiga
Desembargadora Federal Presidente do TRT da 11ª Região