RESOLUÇÃO Nº 278, de 01.08.2017

(Processo TRT nº537/2017)

"Por unanimidade aprovar a Proposição da Presidência, no sentido de alterar a Resolução TRT7 n° 313/2010, Instituindo a Política de Segurança da Informação e Comunicações (POSIC), nos seguintes termos:

A Política de Segurança da Informação e Comunicações (POSIC)

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º A Política de Segurança da Informação e Comunicações (POSIC) do Tribunal Regional do Trabalho da 7ª Região é regida pela presente Resolução e visa a proteção da informação de vários tipos de ameaças, minimizando os riscos.

Parágrafo único. As disposições desta Resolução Administrativa são válidas para todos os usuários internos e externos, inclusive para as pessoas que se encontrem a serviço do TRT da 7ª Região autorizadas a utilizar, em caráter temporário, os recursos de tecnologia da informação e documentais, mediante solicitação do dirigente da Unidade do Órgão responsável pela informação.

Art. 2º A POSIC, como parte das diretrizes estratégicas desta Corte, tem por objetivo geral estabelecer as diretrizes e o suporte administrativo suficientes para assegurar a confidencialidade, a integridade e a disponibilidade das informações no âmbito do TRT da 7ª Região, de modo a resguardar a legitimidade de sua atuação e contribuir para o cumprimento de suas atribuições legais.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta POSIC, fica estabelecido o significado dos seguintes termos e expressões:

I - Ativo: aquilo que tem valor, seja tangível ou intangível, para o TRT da 7ª Região, tais como: informações, software, equipamentos, instalações, serviços, pessoas e imagem institucional;

II - 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;

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

IV - Disponibilidade: propriedade da informação que está acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

V - Segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade da informação;

VI - Recurso de Tecnologia da Informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como as instalações físicas que os abrigam;

VII - Incidente: evento adverso, confirmado ou sob suspeita, relacionado à área da informação ou dos sistemas de computação ou das redes de computadores;

VIII - Usuário: Magistrados, Servidores ocupantes de cargo efetivo ou cargo em comissão, requisitados ou cedidos, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários, pensionistas, bem como inativos, quando autorizados a obter acesso a informações e sistemas.

IX - Ameaça: agente externo ao ativo de informação que se aproveita de suas vulnerabilidades para gerar um dano à confidencialidade, integridade ou à disponibilidade da informação.

X - Vulnerabilidade: qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações.

XI - Risco: chance da ameaça se concretizar, de um evento ocorrer e de suas consequências para a organização.

XII - Ataque: qualquer ação que comprometa a segurança de informação do Tribunal Regional do Trabalho da 7ª Região.

XIII - Impacto: consequência avaliada de um evento em particular.

XIV - Gestão de Continuidade de TIC: conjunto de ações de prevenção e procedimentos de recuperação, no âmbito de TI, 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.

CAPÍTULO III
DA CONFORMIDADE

Art. 4º A presente POSIC está em conformidade com a seguinte legislação e normas:

I - Decreto nº 3.505, de 13 de junho de 2000, que institui a Politica de Segurança da Informação nos Órgãos e entidades da Administração Pública Federal;

II - Instrução Normativa GSI/PR nº 1, de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

III - Manual de Boas Práticas em Segurança da Informação, 3ª Edição, do TCU;

IV - Norma 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que cria diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Admin-

istração Pública Federal;

V - Resolução nº 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário;

VI - Resolução Administrativa n. 372/2015 do Tribunal Regional do Trabalho da 7ª Região que definiu o Planejamento Estratégico de TI (PETI) para o sexênio 2015/2020;

VII - Relatório da TC 1.233/2012-3, do TCU - "Relatório de auditoria. Avaliação de controles gerais de tecnologia da informação. Constatação de irregularidades, precariedades já tratadas em outro processo. Determinações, recomendações e alertas.";

VIII - "Control Objectives for Information and related Technology 5 – COBIT 5", modelo de gestão de Governança em TI;

IX - Norma NBR ISO/IEC 27001:2013, que define os requisitos para sistemas de gestão de segurança da informação;

X - Norma NBR ISO/IEC 27002:2013, que fornece os controles baseados em melhores práticas para a Segurança da Informação;

XI - Diretrizes para Gestão de Segurança da Informação no Âmbito do Poder Judiciário, do Conselho Nacional de Justiça;

XII - Resolução Administrativa nº 313, de 9 de novembro de 2010, do TRT da 7ª Região.

CAPÍTULO IV
DOS OBJETIVOS DA POLÍTICA

Art. 5º São objetivos específicos da POSIC:

I - Dotar o TRT da 7ª Região de instrumentos jurídicos, normativos e organizacionais que o capacite tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

II - Orientar a adoção de mecanismos, medidas e procedimentos de proteção a dados, informações e conhecimentos relativos à privacidade das pessoas, ao interesse institucional e aos direitos de propriedade intelectual, segundo legislação vigente.

III - Orientar as ações permanentes de conscientização, capacitação e educação sobre a importância da proteção de dados, informações e conhecimentos, com o propósito de internalizar o compromisso com a segurança da informação.

CAPÍTULO V
DOS PRINCÍPIOS E DAS DIRETRIZES DA POLÍTICA

Art. 6º São diretrizes da POSIC:

I - O estabelecimento de uma estrutura organizacional para gestão da segurança da informação no âmbito do Tribunal Regional do Trabalho da 7ª Região;

II - O desenvolvimento de sistema de classificação e tratamento da informação, com o objetivo de garantir os níveis de segurança desejados;

III - A utilização de critérios menos restritivos na classificação da informação;

IV - O estabelecimento de equipe e processo para tratamento de incidentes de segurança da informação na rede do Tribunal;

V - O desenvolvimento e a implementação de inventário de ativos e gestão de riscos;

VI - O desenvolvimento e a implementação de gestão de continuidade dos serviços de TIC;

VII - A realização de auditorias periódicas, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.

VIII - O estabelecimento de normas complementares para, pelo menos: uso de recursos de TIC e controle de acesso, uso de correio eletrônico, acesso à internet, procedimentos de backup e recuperação de dados;

IX - O estabelecimento de normas relativas ao desenvolvimento e à implementação dos Sistemas de Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados;

X - A conformidade dos processos de aquisição de soluções de TI com os preceitos legais e com os princípios de segurança da informação;

XI - O desenvolvimento e a implementação de programas de conscientização e capacitação sobre segurança da informação.

CAPÍTULO VI
DAS PENALIDADES

Art. 7º O descumprimento da POSIC, bem como das normas e dos procedimentos dela decorrentes, acarretará responsabilização administrativa, sem prejuízo das responsabilidades civis e penais, eventualmente cabíveis.

CAPÍTULO VII
DA ORGANIZAÇÃO
Seção I
Da Estrutura

Art. 8º A Segurança da Informação do Tribunal Regional do Trabalho possui a seguinte estrutura:

I - Comissão de Segurança Institucional (CSI);

II - Comitê Gestor de Segurança da Informação (CGSI);

III - Gestor de Segurança da Informação e Comunicações (GSI);

IV - Seção de Escritório de Segurança da Informação (ESI);

V - Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR).

Art. 9º São membros permanentes do CGSI um representante da Diretoria-Geral e os titulares da Secretaria de Tecnologia da Informação, do Escritório de Segurança da Informação, da Seção de Gestão Documental, da Divisão de Comunicação Social, representante da AMATRAVII e representante do SINDISSÉTIMA.

Parágrafo único. O CGSI será coordenado pelo Secretário de Tecnologia da Informação, cujo substituto será o titular do Escritório de Segurança.

Art. 10. O ESI deve ser vinculado diretamente à Secretaria de Tecnologia da Informação, com estrutura organizacional e de pessoal compatíveis
com o grau de responsabilidade e demanda.

Parágrafo único. Caberá ao Coordenador do ESI o papel de Gestor de Segurança da Informação e Comunicações.

Art. 11. Norma complementar definirá a composição e detalhamento das competências da ETIR.

Seção II
Das Competências e Responsabilidade

Art. 12. Compete ao Comitê Gestor de Segurança da Informação (CGSI) deliberar sobre as ações voltadas a gestão da segurança da Informação no âmbito do TRT da 7ª Região, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução e em normas complementares.

Art. 13. O CGSI se reunirá ordinariamente com a Comissão de Segurança Institucional, pelo menos duas vezes por ano, e de forma extraordinária, quando se fizer necessário.

§ 1º As deliberações do CGSI serão consignados em ata e encaminhadas à Comissão de Segurança Institucional para aprovação.

§ 2º O CGSI poderá convidar para participar das reuniões, sem direito a voto, representantes de outras unidades, órgãos, entidades públicas ou organizações da sociedade civil, a fim de colaborar na execução dos trabalhos a serem realizados.

Art. 14. Compete ao Escritório de Segurança da Informação a coordenação das ações voltadas ao aprimoramento da segurança da informação do TRT da 7ª Região, segundo os objetivos, princípios e diretrizes estabelecidos nesta Resolução e deliberações do CGSI.

Art. 15. O Escritório de Segurança da Informação possui as seguintes responsabilidades:

I - Promover cultura de segurança da informação;

II - Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - Propor recursos necessários às ações de segurança da informação;

IV - Coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;

V - Criar ações e métodos que visam à integração das atividades de gestão de riscos, gestão de vulnerabilidades técnicas, gestão de continuidade de TIC, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física dos ativos de TI, segurança lógica de dados;

VI - Realizar e acompanhar estudos de novas tecnologias quanto aos possíveis impactos na segurança da informação;

VII - Propor normas e procedimentos relativos à segurança da informação no âmbito do TRT da 7ª Região.

VIII - Monitorar e reportar ao CGSI o andamento das ações relativas à segurança da informação no âmbito do TRT da 7ª Região.

IX - Manter contatos com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação, visando: ampliar e compartilhar o conhecimento sobre o tema; receber notificações sobre correções, ataques e vulnerabilidades.

Art. 16. Cabe às demais unidades que compõem a estrutura organizacional do TRT da 7ª Região dar cumprimento à POSIC no âmbito de suas respectivas atribuições.

Parágrafo único. Compete aos dirigentes e às chefias imediatas providenciar para que o pessoal sob sua responsabilidade conheça integralmente as medidas de segurança estabelecidas no âmbito do TRT da 7ª Região, zelando por seu fiel cumprimento.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 17. O Escritório de Segurança da Informação, em conjunto com as demais unidades organizacionais do TRT da 7ª Região, promoverá a comunicação e a ampla divulgação da Política de que trata esta Resolução para que todos a conheçam e a cumpram no âmbito de suas atividades e atribuições.

Art. 18. A POSIC deve ser implementada no âmbito do TRT da 7ª Região, segundo as prioridades identificadas pelo CGSI e pelo ESI.

Art. 19. O TRT da 7ª Região exigirá dos usuários termo de compromisso de não divulgação de dados, informações e conhecimentos sigilosos ou sensíveis a que, direta ou indiretamente, tenham acesso no exercício de cargos, funções ou empregos públicos.

Parágrafo único. As empresas terceirizadas ou quaisquer entidades que disponibilizem pessoal para exercer atividades junto ao TRT da 7ª Região
deverão garantir a adoção das medidas previstas neste artigo.

Art. 20. O Escritório de Segurança da Informação deve estabelecer os critérios e os indi-

cadores para o monitoramento e a avaliação da eficácia, da eficiência e da efetividade da POSIC.

Parágrafo único. Para os fins deste artigo, o Escritório de Segurança da Informação poderá contar com o apoio e a colaboração das demais
unidades organizacionais do TRT da 7ª Região, em especial, da Secretaria de Gestão Estratégica.

Art. 21. A POSIC deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

Art. 22. As dúvidas e os casos omissos serão dirimidos pelo CGSI, e em última instância, pela Comissão de Segurança Institucional, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução.

Art. 23. A Presidência expedirá atos específicos sobre as normas complementares, observadas as diretrizes da presente Resolução.

Art. 24. Esta Resolução entra em vigor na data de sua publicação."

(Trata-se de Proposição da Presidência, com aval da Comissão de Segurança Institucional e fundamento no artigo 55, inciso I do Regimento Interno deste Tribunal, para alterar a Resolução TRT7 n° 313/2010, instituindo a Política de Segurança da Informação e Comunicações - POSIC.)

Disponibilizada no DEJT nº 2289, de 10.08.2017, Caderno Administrativo do TRT da 7ª Região