PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

RESOLUÇÃO NORMATIVA TRT7 Nº 5, DE 3 DE MARÇO DE 2023

Dispõe sobre a nova Política de Segurança de Tecnologia da Informação e Comunicação (POSIC) do Tribunal Regional do Trabalho da 7ª Região (TRT-7) e dá outras providências.

O EGRÉGIO PLENO DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, em Sessão Ordinária hoje realizada, sob a Presidência do Excelentíssimo Senhor Desembargador do Trabalho Durval César de Vasconcelos Maia, Presidente do Tribunal, presentes os Excelentíssimos(as) Senhores(as) Desembargadores(as) José Antonio Parente da Silva, Maria Roseli Mendes Alencar, Francisco Tarcísio Guedes Lima Verde Junior, Plauto Carneiro Porto, Regina Gláucia Cavalcante Nepomuceno, Jefferson Quesado Junior, Francisco José Gomes da Silva, Clóvis Valença Alves Filho, João Carlos de Oliveira Uchoa, e o Excelentíssimo Procurador-Regional do Trabalho Nicodemos Fabrício Maia,

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça (CNJ), que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional;

CONSIDERANDO o Decreto nº 10.222, de 5 de fevereiro de 2020, que Aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO o Manual de Boas Práticas em Segurança da Informação, 4ª Edição, do Tribunal de Contas da União (TCU);

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27002:2013, que normatiza o Código de Prática para Controles da Segurança da Informação;

CONSIDERANDO a Resolução nº 1, de 22 de janeiro de 2021 do Tribunal Regional do Trabalho da 7ª Região, que institui a Política de Privacidade e Proteção de Dados Pessoais do TRT-7;

CONSIDERANDO a Norma Complementar nº 17/IN01/DSIC/GSIPR que estabelece as diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Dispor sobre a nova Política de Segurança de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 7ª Região que visa a proteção da informação de vários tipos de ameaças, minimizando os riscos.

Parágrafo único. As disposições desta Resolução Administrativa são válidas para todos(as) os(as) usuários(as) internos(as) e externos(as), 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.

Parágrafo único. A segurança da informação abrange aspectos físicos, tecnológicos e humanos do TRT da 7ª Região.

CAPÍTULO II
DOS CONCEITOS E DAS 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, *softwares*, 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

autorizadas não tenham conhecimento da informação, de forma proposital ou acidental. A confidencialidade, por exemplo, pode ser obtida por meio da conversão de dados de um formato legível em um formato codificado (criptografia);

III - integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação. A integridade, por exemplo, pode ser obtida por meio do uso de assinatura digital e de cópias de segurança;

IV - disponibilidade: propriedade da informação que está acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou de uma entidade. A disponibilidade, por exemplo, pode ser obtida por meio do uso de fonte de energia alternativa em caso de falhas no fornecimento pela concessionária;

V - autenticidade: propriedade que garante a veracidade da autoria da informação. A autenticidade, por exemplo, pode ser obtida por meio do uso de certificados digitais;

VI - segurança da informação: preservação da confidencialidade, da integridade, da autenticidade e da disponibilidade da informação;

VII - recurso de tecnologia da informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como as instalações físicas que os abrigam;

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

IX - usuário(a) interno(a): magistrados(as), servidores(as), ocupantes de cargo efetivo ou cargo em comissão, requisitados ou cedidos lotados no TRT-7, bem como, funcionários(as) de empresas prestadoras de serviços terceirizados, auditores(as), consultores(as) e estagiários(as), quando autorizados(as) a obter acesso a informações e sistemas;

X - usuário(a) externo(a): Inativos(as), pensionistas(as), advogados(as), procuradores(as), partes em processo, peritos(as), fornecedores(as) e sociedade em geral, que fazem uso dos serviços de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo TRT-7;

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

XII - vulnerabilidade: qualquer fraqueza que possa ser explorada e comprometa a segurança de sistemas ou de informações.;

XIII - risco: chance da ameaça se concretizar, de um evento ocorrer e de suas consequências para a organização.;

XIV - ataque: qualquer ação que comprometa a segurança da informação do Tribunal Regional do Trabalho da 7ª Região;

XV - impacto: consequência avaliada de um evento em particular.

XVI - 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;

XVII - Sistema de Gestão de Segurança da Informação (SGSI): é a abordagem organizacional usada para proteger a informação corporativa e seus critérios de confidencialidade, integridade e disponibilidade. O SGSI inclui políticas, processos, planos e controles usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e para melhorar a segurança da informação;

XVIII - encarregado(a) pelo tratamento de dados pessoais: magistrado ou magistrada, indicado ou indicada pelo Tribunal para atuar como canal de comunicação entre o Tribunal, os(as) titulares dos dados pessoais e a autoridade nacional de proteção de dados;

XIX - não repúdio: Também conhecido como princípio da irretratabilidade, está relacionado à garantia da impossibilidade de o emissor negar a autoria de determinada mensagem ou transação, bem como, na utilização da assinatura digital de documentos eletrônicos, em que não é possível que determinada pessoa que assinou tal documento possa negar que o tenha feito.

CAPÍTULO III
DOS OBJETIVOS DA POLÍTICA

Art. 4º São objetivos específicos da POSIC:

I - dotar o TRT da 7ª Região de instrumentos jurídicos, normativos e organizacionais que o capacite tecnológicamente 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 de procedimentos de proteção a dados, informações e a 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 de educação sobre a importância da proteção de dados, informações e de conhecimentos, com o propósito de internalizar o compromisso com a segurança da informação;

IV - aumentar a resiliência às ameaças cibernéticas.

CAPÍTULO IV
DOS PRINCÍPIOS DA POLÍTICA

Art. 5º A segurança da informação no TRT-7 alinha-se às estratégias organizacionais e aos seguintes princípios:

I - abordagem da segurança da informação em todos os níveis organizacionais;

II - adoção da publicidade como regra e a do sigilo como exceção;

III - conformidade com os preceitos legais e com os princípios de segurança da informação;

IV - liderança e comprometimento pela Alta Administração em relação ao sistema de gestão da segurança da informação;

V - segregação de funções, para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos de informação;

VI - pessoalidade e utilidade do acesso aos ativos de informação;

VII - prevenção, com base em análise de riscos;

VIII - foco nos resultados de segurança;

Parágrafo único. A Política de Privacidade e Proteção de Dados Pessoais do TRT-7 é parte integrante e harmoniza-se, no que couber, com esta política de segurança da informação.

CAPÍTULO V
DAS DIRETRIZES DA POLÍTICA

Art. 6º São diretrizes desta política:

I - O estabelecimento de uma estrutura organizacional e de um Sistema de Gestão em Segurança da Informação baseado em riscos no âmbito do Tribunal Regional do Trabalho da 7ª Região;

II - a realização de auditorias periódicas para verificação do cumprimento desta política e de suas normas complementares;

III - o desenvolvimento e a implementação de programas de conscientização e capacitação sobre segurança da informação;

IV - a responsabilização do usuário pelos atos que comprometam a segurança dos ativos de informação;

V – o estabelecimento de troca de informações e boas práticas com outros membros do poder público em geral e do setor privado com objetivo colaborativo;

VI - alinhamento da segurança crítica com os padrões nacionais e internacionalmente reconhecidos;

VII - a destinação de recursos orçamentários discriminados em rubrica específica para promoção do aprimoramento da segurança cibernética do TRT7;

VIII - a adoção de soluções integradoras e que permitam a macro gestão de diversos ativos e de diferentes tecnologias, permitindo a coleta de dados sobre ameaças de segurança de várias fontes e oferecendo detecção e resposta automatizadas e eficazes;

Art. 7º O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade da prestação jurisdicional deste Tribunal.

Parágrafo único. Os recursos de tecnologia da informação pertencentes ao TRT-7, disponíveis para o(a) usuário(a), serão utilizados em atividades relacionadas às suas funções institucionais.

Art. 8º A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

Art. 9º As informações, sistemas e os métodos gerados ou criados pelos(as) usuários(as), no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são propriedade do Tribunal e serão utilizadas exclusivamente para fins relacionados às atividades a ele afetas.

Parágrafo único. Quando as informações, sistemas e os métodos forem gerados ou criados por terceiros(as) para uso exclusivo do Tribunal, ficam os(as) criadores obrigados(as) ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

Art. 10. A Presidência expedirá atos específicos sobre as normas complementares de segurança da informação, no mínimo, para:

I - controle de acesso e uso aceitável dos ativos, tais como microcomputadores, *notebooks*, correio eletrônico, rede corporativa, redes sociais, teletrabalho, sistemas de informação, ambiente de colaboração em nuvem, *internet*, tratamento de mídias e centros de dados;

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

III - cópia de Segurança (*backup*);

IV - gestão da continuidade dos serviços de TIC;

V - gestão contínua de vulnerabilidades técnicas;

VI - inventário de ativos de TIC;

VII - gestão de riscos de segurança da informação e comunicações;

VIII - adoção do protocolo de prevenção de incidentes cibernéticos do Poder Judiciário;

IX - adoção do protocolo de investigação de ilícitos cibernéticos do Poder Judiciário;

X - adoção do protocolo de gerenciamento de crises cibernéticas do Poder Judiciário;

XI - macroprocesso denominado sistema de gestão de segurança da informação;

CAPÍTULO VI
DOS SISTEMAS DE INFORMAÇÃO

Art. 11. A segurança da informação deve ser parte integrante de todo o processo de ciclo de vida dos sistemas de informação.

Art. 12. Na análise e na especificação dos requisitos de segurança da informação, para novos sistemas de informação ou melhoria dos existentes, deverá ser considerado, ao menos:

I - requisitos mínimos de autenticação, como, por exemplo, exigência ou não de duplo fator de autenticação;

II - processo de autorização de acessos;

III - possibilidade e necessidade do uso de criptografia;

IV - o impacto ao negócio em caso de falha da segurança da informação, tais como: indisponibilidade, perda de dados, alterações não autorizadas ou exposição indevida das informações;

V - manutenção de registros de transações e logs de auditoria;

Art. 13. Caso um sistema de informação não atenda algum requisito de segurança especificado, sua utilização fica condicionada à autorização prévia da Presidência do TRT-7 e a implementação de controles associados ao risco introduzido.

CAPÍTULO VII
DA ORGANIZAÇÃO

Seção I
Da Estrutura

Art. 14. A gestão da segurança da informação do Tribunal Regional do Trabalho da 7ª Região possui a seguinte estrutura:

I - Comitê de Segurança da Informação e Proteção de Dados (CSIPD);

II - Gestor(a) de Segurança da Informação;

III - Coordenadoria de Segurança da Informação (CSI);

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

V - encarregado(a) pelo tratamento de dados pessoais.

Art. 15. A CSI deve ser vinculada diretamente à Secretaria de Tecnologia da Informação e Comunicação (SETIC), com estrutura organizacional e de pessoal compatíveis com o grau de responsabilidade e demanda.

Seção II
Das Competências e das Responsabilidade

Art. 16. A composição, as atribuições e o funcionamento do Comitê de Segurança da Informação e Proteção de Dados serão definidos através de Ato da Presidência.

Art. 17. Caberá ao titular da Coordenadoria de Segurança da Informação e Comunicação o papel de Gestor de Segurança da Informação do Tribunal.

Art. 18. Ato da Presidência definirá a composição e o detalhamento das competências da Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.

Art. 19. Compete ao Gestor de Segurança da Informação:

I - elaborar, anualmente, relatório de avaliação do Sistema de Gestão de Segurança da Informação e encaminhá-lo ao Comitê de Segurança da Informação e Proteção de Dados;

II - implementar controles internos fundamentados na gestão de riscos da segurança da informação;

III - planejar a execução de programas, de projetos e de processos relativos à segurança da informação com as demais unidades do órgão;

IV - observar as normas e os procedimentos específicos aplicáveis em consonância com os princípios e as diretrizes desta Resolução e da legislação de regência.

V - analisar e monitorar os indicadores dos processos de segurança e implementar ou encaminhar as medidas necessárias em razão de mudanças nesses indicadores;

VI - monitorar e reportar ao Comitê de Segurança da Informação e Proteção de Dado, nas reuniões ordinárias, ou quando solicitado, o andamento dos projetos e das ações relativas à segurança da informação;

VII - ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação;

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

Art. 20. 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
DA POLÍTICA DE EDUCAÇÃO E DA CULTURA EM SEGURANÇA DA INFORMAÇÃO

Art. 21. O TRT-7 deverá desenvolver ações de capacitação, formação e de reciclagem em segurança da informação, assegurando que novos conhecimentos atinentes ao tema da segurança cibernética sejam permanentemente ofertados aos(às) profissionais das áreas de TIC e de Segurança da Informação, em nível acadêmico, técnico, gerencial, entre outros aplicáveis.

§ 1º Deve-se buscar o conhecimento multidisciplinar, entendendo que a segurança da informação abrange os contextos estratégico, tático e operacional do Tribunal.

§ 2º As ações descritas no *caput* deste artigo podem incluir, entre outras:

a) programas de formação académica;

b) programas de reciclagem;

c) programas de extensão educacional;

d) ações periódicas de capacitação;

e) cursos em plataformas do tipo MOOC – *Massive Open On-line Courses;*

f) programas de certificação especializada;

g) palestras, congressos, seminários e afins;

h) *workshops*.

Art. 22. Para capacitação dos(as) servidores(as) devem ser considerados obrigatoriamente os seguintes temas, sem prejuízo de outros:

a) governança e gestão de segurança cibernética;

b) elaboração de políticas institucionais de segurança cibernética;

c) tratamento de incidentes de segurança cibernética;

d) forense computacional;

e) inteligência e investigação em crimes cibernéticos;

h) gerenciamento de identidades, acesso e privilégios;

i) segurança no desenvolvimento de *software*;

h) gestão de continuidade de TIC;

i) gestão de riscos de segurança da informação;

j) auditoria e conformidade de sistemas de informação;

k) segurança em computação em nuvem;

l) segurança em aplicações móveis;

m) segurança em redes sociais;

n) gerenciamento de vulnerabilidades técnicas;

o) gerenciamento de eventos e informações de segurança; e

p) detecção de comportamento anômalo de usuários(as) e aplicações.

Art. 23. Para capacitação e certificação dos(as) servidores(as) devem ser considerados também os temas para capacitação e lista de certificações recomendadas pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança da Informação da Presidência da República, previstos na norma complementar específica para atuação e adequações para profissionais da área da área segurança da informação no âmbito da Administração Pública Federal, direta e indireta.

Parágrafo único. O(A) servidor(a) beneficiário(a) de certificação profissional que se desligar, voluntariamente, da unidade de segurança da informação, em menos de 12(doze) meses após a certificação, deverá ressarcir ao TRT-7 todo o investimento realizado na referida certificação.

Art. 24. Deverá ser elaborado plano anual de capacitação destinada aos(às) servidores(as) da Coordenadoria de Segurança da Informação, integrado ao plano anual de capacitação de TIC, contendo:

I - carga-horária mínima de capacitação destinada aos(às) servidores(as) da Coordenadoria de Segurança da Informação em um ou mais temas listados nos arts. 22 e 23 desta Resolução, sem prejuízo de outras capacitações necessárias; e

II - certificação reconhecida internacionalmente em segurança cibernética, no prazo máximo de 2(dois) anos da lotação ou da vigência desta Resolução;

Art. 25. Compete à Escola Judicial do TRT7, conjuntamente com o Comitê de Segurança da Informação e Proteção de Dados do TRT7, a elaboração de programas de formação, capacitação e reciclagem de magistrados(as) e de servidores(as) que descrevam, com previsão bianual e de forma detalhada, as ações a serem realizadas, as metas a serem atingidas, os quantitativos previstos, os critérios de participação e a contabilização de horas, entre outros elementos que evidenciem o cumprimento da Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.

Parágrafo único. As ações previstas no *caput* deste artigo devem assegurar que todos(as) os(as) usuários(as) internos(as) possuam educação básica em segurança da informação e tenham a devida compreensão de suas responsabilidades na proteção das informações do TRT7;

Art. 26. Compete à Escola Judicial do TRT7 a adoção de procedimentos, normativos e práticas administrativas que viabilizem a inscrição, a participação e o pagamento de ações de capacitação previstas nesta política.

CAPÍTULO IX
DAS PENALIDADES

Art. 27. 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 X
DAS DISPOSIÇÕES FINAIS

Art. 28. A CSI, 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. 29. O TRT da 7ª Região exigirá dos(as) fornecedores(as) e dos(as) colaboradores(as) externos termo de compromisso de não divulgação de dados, informações e de conhecimentos sigilosos ou sensíveis a que, direta ou indiretamente, tenham acesso no exercício das atividades.

Art. 30. Os contratos, convênios, acordos de cooperação e os outros instrumentos congêneres celebrados pelo TRT-7l devem observar, no que couber, as disposições desta Resolução e normas complementares.

Art. 31. A POSIC, o processo de gestão e as normas complementares de segurança da informação devem ser revisados e atualizados periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata, com o objetivo de mantê-la atualizada em relação à(ao):

I - estratégia do negócio;

II - regulamentações;

III - ambiente de ameaça da segurança da informação atual e futuro;

IV - tópicos que exigem a implementação de controles de segurança específicos.

Art. 32. As dúvidas e os casos omissos serão dirimidos pelo Comitê de Segurança da Informação e Proteção de Dados, e em última instância, pela Presidência do Tribunal, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução.

Art. 33. Fica revogada a Resolução Normativa TRT7 nº 14, de 22 de junho de 2020.

Art. 34. Esta Resolução entra em vigor na data de sua publicação.

Fortaleza, 3 de março de 2023
DURVAL CÉSAR DE VASCONCELOS MAIA
Presidente do Tribunal