**PODER JUDICIÁRIO FEDERAL**
**TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO**

# RESOLUÇÃO ADMINISTRATIVA PROAD Nº 5807/2019

**O EGRÉGIO PLENO DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO**, em Sessão Extraordinária hoje realizada, sob a Presidência do Excelentíssimo Senhor Desembargador Plauto Carneiro Porto, presentes os Excelentíssimos Senhores Desembargadores, Regina Gláucia Cavalcante Nepomuceno, José Antônio Parente da Silva, Cláudio Soares Pires, Maria José Girão, Maria Roseli Mendes Alencar, Francisco Tarcísio Guedes Lima Verde Júnior, Jefferson Quesado Júnior, Durval César de Vasconcelos Maia, Fernanda Maria Uchôa de Albuquerque, Francisco José Gomes da Silva, Paulo Régis Machado Botelho e a Excelentíssima Procuradora-Regional do Trabalho Mariana Ferrer Carvalho Rolim,

**RESOLVE,**

Por unanimidade, aprovar a proposição da Presidência nos seguintes termos:

## PROPOSIÇÃO DA PRESIDÊNCIA

Excelentíssimos Senhores Desembargadores do Tribunal Regional do Trabalho da 7ª Região:

**CONSIDERANDO** o Relatório de Auditoria TRT7.SCI.GABIN n.11/2019 (PROAD 5497/2019);

**CONSIDERANDO** o Manual de Boas Práticas em Segurança da Informação, 3ª Edição, do TCU;

**CONSIDERANDO** a 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 Administração Pública Federal;

**CONSIDERANDO** a 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;

**CONSIDERANDO** a 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;

**CONSIDERANDO** o 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.";

**CONSIDERANDO** o "Control Objectives for Information and related Technology 5 – COBIT 5", modelo de gestão de Governança em TI;

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

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

**CONSIDERANDO** as Diretrizes para Gestão de Segurança da Informação no Âmbito do Poder Judiciário, do Conselho Nacional de Justiça;

**PROPONHO AO TRIBUNAL PLENO DESTE REGIONAL**, com fundamento no artigo 55, inciso I do Regimento Interno deste Tribunal, a revogação da Resolução nº 313/2010 (Alterada pela Resolução TRT7 nº 278/2017), instituindo a nova política de segurança da informação no âmbito desta Corte: 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.

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

## 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 comprometa 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 da 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.

**XV** - Sistema de Gestão de Segurança da Informação: 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 melhorar a segurança da informação.

## 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 Política 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 Administração 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;

## 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 DA POLÍTICA

**Art. 6º** A segurança da informação no TRT7 alinha-se às estratégias organizacionais e aos seguintes princípios:

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

**II** - Adoção da publicidade como regra e do sigilo como exceção;

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

**IV** - Liderança e comprometimento em relação ao sistema de gestão da segurança da informação pela Alta Administração.

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

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

**IX** - A realização de auditorias periódicas para verificação do cumprimento desta política e de suas normas complementares.

## CAPÍTULO V
## DAS DIRETRIZES DA POLÍTICA

**Art. 7º** A Presidência expedirá atos específicos sobre as normas complementares de segurança da informação, no mínimo, para:

**I** - O estabelecimento do processo denominado sistema de gestão de segurança da informação - SGSI;

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

**III** - Inventário de ativos de TIC;

**IV** - Gestão de Riscos de Segurança da Informação e Comunicações;

**V** - Gestão de continuidade dos serviços de TIC, incluindo backup e recuperação de dados;

**VI** - O estabelecimento de norma para controle de acesso e uso dos recursos de TIC listados a seguir, mas não limitado à: equipamentos de informática, correio eletrônico, rede corporativa, redes sociais, sistemas de informação, ambiente de colaboração, internet e tratamento de mídias;

**VII** - A segurança física e do ambiente dos centros de dados;

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

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

**X** - O estabelecimento de normas relativas à segurança das operações, nas comunicações e no relacionamento com fornecedores.

## CAPÍTULO VI
## DA ORGANIZAÇÃO

### Seção I
### Da Estrutura

**Art. 8º** A gestão da segurança da informação do Tribunal Regional do Trabalho da 7ª Região possui a seguinte estrutura:

**I** - Comitê Gestor de Segurança da Informação (CGSI);

**II** - Gestor de Segurança da Informação (GSI);

**III** - Núcleo de Apoio à Gestão de TIC e Segurança da Informação (NGTIC);

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

**Art. 9º** São membros permanentes do Comitê Gestor de Segurança da Informação:

**I** - 1(um) representante da Diretoria-Geral;

**II** - 1(um) representante da Secretaria-Geral da Presidência;

**III** - Diretor(a) da Secretaria de Tecnologia da Informação e Comunicação (SETIC);

**IV** - Coordenador(a) do NGTIC;

**V** - Titular da Seção de Gestão Documental;

**VI** - Diretor da Divisão de Comunicação Social;

**VII** - 1(um) representante da AMATRAVII;

**VIII** - 1(um) representante do SINDISSÉTIMA.

**Parágrafo único.** O CGSI será coordenado pelo Diretor(a) da SETIC, cujo substituto será o titular do NGTIC.

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

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

## Seção II
## Das Competências e Responsabilidade

**Art. 12.** O Comitê Gestor de Segurança da Informação - CGSI é órgão colegiado de natureza consultiva e de caráter permanente, que tem por finalidade:

**I** - propor diretrizes para a Política de Segurança da Informação - POSIC, bem como analisar periodicamente sua efetividade;

**II** - estabelecer o sistema de gestão de segurança da informação - SGSI, com subsídio no monitoramento e na avaliação periódica das práticas de segurança da informação;

**III** - propor normas complementares e procedimentos inerentes à segurança da informação;

**IV** - manifestar-se sobre propostas de alteração ou de revisão da POSIC, bem como sobre minutas de ato normativo e iniciativas de natureza estratégica ou que necessitem de cooperação entre unidades, que versem sobre segurança da informação;

**V** - manifestar-se sobre matérias atinentes à segurança da informação que lhe sejam submetidas;

**VI** - assessorar, em matérias correlatas, a Presidência do TRT7.

**VII** - propor os critérios e os indicadores para o monitoramento e a avaliação da eficácia, da eficiência e da efetividade da POSIC.

**Art. 13.** O CGSI se reunirá ordinariamente pelo menos duas vezes por ano, e de forma extraordinária, quando se fizer necessário.

**§ 1º** As deliberações do CGSI serão consignadas em ata e encaminhadas ao Comitê de Governança de TIC 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.** O NGTIC, quanto à gestão da segurança da informação, possui as seguintes responsabilidades:

**I** - Promover cultura de segurança da informação;

**II** - Coordenar as ações voltadas ao aprimoramento da segurança da informação;

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

**IV** - Indicar os recursos necessários às ações de segurança da informação;

**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;

**VIII** - Monitorar e reportar ao CGSI o andamento das ações relativas à segurança da informação.

**Parágrafo único.** Caberá ao Coordenador do NGTIC o papel de Gestor de Segurança da Informação.

**Art. 15.** Compete ao Gestor de Segurança da Informação (GSI);

**I** - 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.

**II** - Ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação;

**III** - Assegurar que o entendimento do ambiente de segurança da informação está atual e completo;

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

**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 VII
## DAS PENALIDADES

**Art. 17.** 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 VIII
## DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

**Art. 18**. O NGTIC, 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. 19.** O TRT da 7ª Região exigirá dos fornecedores e colaboradores externos termo de compromisso de não divulgação de dados, informações e conhecimentos sigilosos ou sensíveis a que, direta ou indiretamente, tenham acesso no exercício das atividades.

**Art. 20.** Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal devem observar, no que couber, as disposições desta Resolução e normas complementares.

**Art. 21.** 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:

**I** - à estratégia do negócio;

**II** - às regulamentações;

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

**IV** - aos tópicos que exigem a implementação de controles de segurança específicos;

**Art. 22.** As dúvidas e os casos omissos serão dirimidos pelo Comitê de Governança de TIC, e em última instância, pela Presidência do Tribunal, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução.

**Art. 23.** Esta Resolução entra em vigor na data de sua publicação.

Fortaleza, 19 de junho de 2020.
**Plauto Carneiro Porto**
Presidente do Tribunal



**Fonte:** Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2999, 22 jun 2020. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 2.