



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 13ª REGIÃO

**Setor: SEGEJUD**

**Processo: 0000327-25.2021.5.13.0000**

**RESOLUÇÃO ADMINISTRATIVA N.º 104/2021**

Dispõe sobre a Política de Segurança da Informação e Comunicações (POSIC) e sobre o Sistema de Gestão de Segurança da Informação (SGSI) do Tribunal Regional do Trabalho da 13ª Região

O Egrégio **TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO**, em Sessão Administrativa, em formato híbrido, realizada em **04/11/2021**, sob a Presidência de Sua Excelência o Senhor Desembargador **LEONARDO JOSÉ VIDERES TRAJANO**, com a presença da Representante da Procuradoria Regional do Trabalho, Sua Excelência a Senhora Procuradora **ANDRESSA ALVES LUCENA RIBEIRO COUTINHO**, presentes Suas Excelências os Senhores Desembargadores **THIAGO DE OLIVEIRA ANDRADE**, **EDVALDO DE ANDRADE**, **PAULO MAIA FILHO**, **CARLOS COELHO MIRANDA FREIRE**, **UBIRATAN MOREIRA DELGADO** e **WOLNEY DE MACEDO CORDEIRO**,

**CONSIDERANDO** que o Tribunal produz e recebe informações no exercício de suas competências constitucionais, legais e regulamentares, e que tais informações devem permanecer íntegras e disponíveis, bem como seu eventual sigilo deve ser resguardado;

**CONSIDERANDO** que as informações do Tribunal são armazenadas e disponibilizadas em diferentes formas, tais como meio impresso e eletrônico, estando vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

**CONSIDERANDO** a necessidade de atualizar a Política de Segurança da Informação e Comunicações da instituição, visando garantir a integridade, confidencialidade e disponibilidade das informações;

**CONSIDERANDO** o número progressivo de incidentes no ambiente da rede mundial de computadores e a necessidade de

processos de trabalho orientados para a boa gestão da Segurança da Informação;

**CONSIDERANDO** a importância da Segurança da Informação para o processo judicial eletrônico e para a continuidade da prestação jurisdicional;

**CONSIDERANDO** que a Segurança da Informação abrange a proteção de dados pessoais;

**CONSIDERANDO** a legislação federal, assim como resoluções, normas, recomendações e boas práticas publicadas pelo CNJ, CSJT, TCU e ABNT relacionadas à Segurança da Informação;

**resolveu**, por unanimidade de votos,

## **CAPÍTULO I**

### **DAS DISPOSIÇÕES GERAIS**

**Art. 1º** Estabelecer, por meio desta RA, a Política de Segurança da Informação e Comunicações (POSIC) e o Sistema de Gestão de Segurança da Informação (SGSI) do Tribunal Regional do Trabalho da 13ª Região, tendo como princípios básicos:

I- A preservação da confidencialidade, integridade e disponibilidade das informações;

II- A privacidade e a proteção de dados pessoais;

III- A continuidade da prestação jurisdicional;

IV- A gestão da Segurança da Informação por meio de uma abordagem baseada em riscos;

V- A conformidade com dispositivos legais, normas e boas práticas relacionadas à Segurança da Informação e à proteção de dados pessoais;

VI- A disseminação da cultura de Segurança da Informação na instituição.

**Art. 2º** Para efeitos desta RA, aplicam-se as seguintes definições:

I - O direito a informação como direito fundamental de todos os cidadãos; informação: conjunto de dados relacionados entre si que levam à compreensão de algo e que trazem determinado conhecimento, podendo estar na forma escrita, verbal ou de imagem, e em meio digital ou físico;

II- Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

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

IV- Política de Segurança da Informação e Comunicações (POSIC): conjunto de intenções e diretrizes gerais formalmente expressas pela alta administração com o objetivo de garantir a Segurança da Informação no âmbito da instituição;

V- Sistema de Gestão de Segurança da Informação (SGSI): parte do sistema de gestão institucional que visa estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a Segurança da Informação; VI- Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados;

VII- Integridade: propriedade de que a informação não seja alterada, de forma não autorizada ou acidental, por indivíduos, entidades ou processos;

VIII- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduos, entidades ou processos autorizados;

IX- Ativo ou recurso de Tecnologia da Informação e Comunicações (TIC): qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, e as instalações físicas que os abrigam;

X- Usuário: qualquer pessoa física ou jurídica que tenha acesso a informações produzidas ou custodiadas pela instituição, de forma autorizada; XI- Incidente de Segurança da Informação: um evento ou uma série de eventos indesejados ou inesperados, que comprometeram ou tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação;

XII- Risco de Segurança da Informação: probabilidade de impacto negativo nos objetivos da organização caso as suas informações não estejam protegidas adequadamente;

XIII- Segurança cibernética: conjunto de práticas que visa proteger os recursos de TIC da instituição de ataques;

XIV- Computação em nuvem: paradigma para habilitar o acesso via rede a um grupo escalável e elástico de recursos de TIC, físicos ou virtuais, compartilháveis, com provisionamento via autoatendimento e administração sob demanda

**Art. 3º** As disposições desta RA aplicam-se a todos os usuários internos e externos da instituição.

**Art. 4º** As informações produzidas ou custodiadas pelo Tribunal devem ser adequadamente classificadas e protegidas, independente da forma de apresentação ou armazenamento.

**Art. 5º** O uso adequado dos ativos de TIC visa garantir a continuidade da prestação jurisdicional deste Tribunal.

§1º Os ativos de TIC da instituição devem ser utilizados pelos usuários de forma responsável e comedida, visando evitar a indisponibilidade de serviços essenciais;

§2º A utilização dos ativos de TIC será monitorada pela instituição.

**Art. 6º** Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal devem observar, no que couber, as disposições desta RA, possuindo cláusulas inerentes à Segurança da Informação.

**Art. 7º** A segurança física e patrimonial deve observar, no que couber, as disposições desta RA, tendo por objetivo prevenir danos e interferências nas instalações da instituição que possam causar perda, roubo ou comprometimento das informações.

## **CAPÍTULO II**

### **DA ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO**

**Art. 8º** A estrutura normativa da Segurança da Informação é organizada conforme segue:

I- Política de Segurança da Informação e Comunicações - POSIC (nível estratégico): instituída pela presente RA, define os princípios básicos adotados pela instituição na gestão da Segurança da Informação, de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados, contemplando a estrutura, diretrizes e responsabilidades referentes à Segurança da Informação;

II- Normas de Segurança da Informação (nível tático): instituídas por Atos da Presidência do Tribunal, especificam, no plano tático, os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da POSIC;

III- Procedimentos de Segurança da Informação (nível operacional): formalizados por normas internas às unidades administrativas, instrumentalizam o disposto na POSIC e nas normas, permitindo a direta aplicação nas atividades da instituição.

§1º A POSIC será revisada anualmente, sendo alterada se assim for necessário;

§2º As normas e procedimentos de Segurança da Informação serão revisados sempre que alguma atualização for necessária;

§3º A estrutura normativa da Segurança da Informação deve ser divulgada a todos os usuários, bem como publicada nos sites da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento;

§4º As diretrizes referentes à proteção de dados pessoais serão objeto da Política de Proteção de Dados Pessoais (PPDP), complementar à POSIC e instituída por meio de Resolução Administrativa.

**Art. 9º** A estrutura funcional da gestão da Segurança da Informação é organizada conforme segue:

I- Comitê Gestor de Segurança da Informação (CGSI): instituído por Ato da Presidência do Tribunal, composto por representantes das áreas jurídica, administrativa e de TIC;

II- Comitê Gestor de Proteção de Dados Pessoais (CGPD): instituído por Ato da Presidência do Tribunal, composto por representantes das áreas jurídica, administrativa e de TIC;

III- Unidade de Segurança da Informação: conforme disposto no Manual de Organização da instituição, subordinada à diretoria da área gestora de TIC, composta por servidores efetivos do quadro de TIC; IV- Grupo de Resposta a Incidentes de Segurança da Informação (GRISI): instituído por Ato da Presidência do Tribunal, composto por servidores efetivos do quadro de TIC.

### **CAPÍTULO III**

#### **DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO**

**Art. 10** São objetivos do Sistema de Gestão de Segurança da Informação (SGSI) do Tribunal Regional do Trabalho da 13ª Região:

I- Fornecer uma estrutura consistente, baseada nas melhores práticas internacionais, para gerenciar a Segurança da Informação na instituição;

II- Implementar e gerenciar os processos relacionados à gestão da Segurança da Informação;

III- Implementar e gerenciar os protocolos de segurança cibernética;

IV- Incrementar o nível de proteção das informações, com base na tríade confidencialidade, integridade e disponibilidade.

**Art. 11** O SGSI do Tribunal Regional do Trabalho da 13ª Região abrange no mínimo os seguintes processos:

I- Gestão de riscos de Segurança da Informação: tem por objetivo identificar, avaliar e tratar os riscos que possam comprometer a confidencialidade, a integridade ou a disponibilidade da informação;

**II-** Gestão de incidentes de Segurança da Informação: tem por objetivo assegurar que incidentes de Segurança da Informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil;

**III-** Gestão de continuidade de TIC: tem por objetivo garantir que os serviços essenciais de TIC da instituição funcionem em níveis aceitáveis durante incidentes de Segurança da Informação, e que a recuperação total dos serviços seja realizada em prazo aceitável;

**IV-** Gestão de segurança dos serviços em nuvem: tem por objetivo garantir a Segurança da Informação nos serviços de TIC que utilizam computação em nuvem;

**V-** Classificação da informação eletrônica: tem por objetivo definir o grau de sigilo da informação eletrônica a fim de assegurar que a mesma receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a instituição.

**Art. 12** Os processos do SGSI são interdependentes e devem ser estruturados, monitorados e revisados de forma a permitir sua melhoria contínua.

**Art. 13** O escopo e os processos do SGSI serão formalizados por meio de Atos da Presidência do Tribunal, devendo ser revisados sempre que alguma atualização for necessária.

## **CAPÍTULO IV**

### **DAS RESPONSABILIDADES**

**Art. 14** Compete ao Tribunal Pleno:

- I- Aprovar a POSIC e a PPDP e suas revisões;
- II- Contribuir para a implementação e continuidade do SGSI;
- III- Aprovar estrutura organizacional adequada à gestão do SGSI.

**Art. 15** Compete à Presidência do Tribunal:

- I- Aprovar as normas de Segurança da Informação e suas revisões;
- II- Aprovar o escopo e processos do SGSI, e suas revisões;
- III- Aprovar a criação e composição do CGSI, CGPD e do GRISI;
- IV- Aprovar critérios para a avaliação de riscos de Segurança da Informação, definindo o nível de risco aceitável;

V- Garantir os recursos necessários ao funcionamento contínuo do SGSI;

VI- Deliberar sobre os casos de descumprimento da POSIC e da PPDP e das normas correlatas, mediante recomendações do CGSI e do CGPD.

**Art. 16** Compete ao Comitê Gestor de Segurança da Informação (CGSI):

I- Formular e conduzir diretrizes para a POSIC e o SGSI, bem como analisar periodicamente sua efetividade;

II- Propor a elaboração e a revisão de normas e de procedimentos inerentes à Segurança da Informação;

III- Manifestar-se sobre propostas de alteração ou de revisão da POSIC, bem como sobre minutas de normativo e iniciativas de natureza estratégica ou que necessitem de cooperação entre unidades, que versem sobre Segurança da Informação;

IV- Submeter minuta da POSIC e suas revisões ao Tribunal Pleno para aprovação; V- Submeter minutas das normas de Segurança da Informação e suas revisões à Presidência do Tribunal para aprovação; VI- Submeter minutas do escopo e dos processos do SGSI e suas revisões à Presidência do Tribunal para aprovação;

VII- Promover a cultura de Segurança da Informação na instituição, apoiando programas contínuos destinados à conscientização e capacitação dos usuários;

VIII- Analisar as comunicações de descumprimento da POSIC e normas de Segurança da Informação, apresentando, se for o caso, parecer à autoridade ou órgão competente;

IX- Solicitar a realização de auditorias pela unidade de Segurança da Informação, relacionadas ao uso de ativos de TIC na instituição; X- Manifestar-se sobre matérias atinentes à Segurança da Informação que lhe sejam submetidas.

**Art. 17** Compete à unidade de Segurança da Informação:

I- Coordenar o SGSI;

II- Gerenciar e manter os processos do SGSI;

III- Elaborar e revisar a POSIC e a PPDP;

IV- Elaborar e revisar normas, procedimentos e demais documentos relacionados à Segurança da Informação;

V- Assessorar o CGSI e o CGPD;

VI- Atuar de forma integrada com outras áreas nos assuntos relacionados à Segurança da Informação;

VII- Elaborar relatórios sobre o uso de recursos de tecnologia, apontando irregularidades e não conformidades na utilização.

**Art. 18** Compete ao Grupo de Resposta a Incidentes de Segurança da Informação (GRISI):

I- Avaliar incidentes de Segurança da Informação associados, principalmente, aos ativos críticos de TIC;

II- Promover o tratamento adequado às ocorrências de incidentes de Segurança da Informação.

**Art. 19** Compete à unidade gestora de TIC:

I- Operacionalizar os normativos de Segurança da Informação relacionados aos ativos de TIC;

II- Implementar e gerenciar os controles de Segurança da Informação inerentes aos ativos de TIC;

III- Monitorar a utilização dos ativos de TIC, mantendo seus registros.

**Art. 20** Compete aos diretores e demais gestores de unidades:

I- Verificar a observância das disposições da Política, normas e procedimentos de Segurança da Informação no âmbito de suas unidades, comunicando ao CGSI eventuais irregularidades;

II- Assegurar que seus subordinados possuam acesso e entendimento da estrutura normativa da Segurança da Informação;

III- Elaborar os procedimentos de Segurança da Informação relacionados às suas unidades.

**Art. 21** Compete aos magistrados, servidores, estagiários, prestadores de serviços e demais usuários da instituição:

I- Zelar continuamente pela proteção das informações produzidas ou custodiadas pela instituição contra acesso, modificação, destruição ou divulgação não autorizada;

II- Comunicar imediatamente ao CGSI qualquer descumprimento da Política e normas de Segurança da Informação de que tenham ciência ou suspeita.

**Art. 22** Compete ao Comitê Gestor de Proteção de Dados Pessoais (CGPD) as responsabilidades definidas na Política de Proteção de Dados Pessoais (PPDP).

## **CAPÍTULO V**

### **DAS VIOLAÇÕES E SANÇÕES**

**Art. 23** São consideradas violações, não se limitando às mesmas:



I- Quaisquer ações ou situações que possam expor a instituição à perda financeira e/ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo suas informações;

II- Utilização indevida de dados institucionais e divulgação não autorizada de informações, sem a permissão expressa de autoridade competente;

III- Uso de dados, informações ou ativos de TIC para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da instituição;

IV- A não comunicação imediata ao CGSI de quaisquer descumprimentos da estrutura normativa de Segurança da Informação, que porventura um usuário venha a tomar conhecimento.

**Art. 24** O descumprimento das disposições desta RA será apurado mediante sindicância ou processo administrativo disciplinar, estando sujeito às penalidades previstas em legislação vigente, sem prejuízo das responsabilidades civis e penais inerentes ao ato praticado.

## **CAPÍTULO VI**

### **DAS DISPOSIÇÕES FINAIS**

**Art. 25** A presente RA entra em vigor a partir da data de sua publicação.

**Art. 26** Fica revogada a RA nº 052/2019.

**RENAN CARTAXO MAQUES DUARTE**  
Secretário Geral Judiciário