RESOLUÇÃO ADMINISTRATIVA TRT13 N.º 070/2023

Processo: 0004783-47.2023.5.13.0000
Proad: 12347/2022)

O Egrégio **TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO**, em Sessão Administrativa Telepresencial Ordinária realizada no dia 07/12/2023, sob a Presidência de Sua Excelência ao Senhor Desembargador **THIAGO DE OLIVEIRA ANDRADE**, com a presença do Representante da Procuradoria Regional do Trabalho, Sua Excelência o Senhor Procurador **MÁRCIO ROBERTO DE FREITAS EVANGELISTA,** presentes Suas Excelências os Senhores Desembargadores **MARGARIDA ALVES DE ARAÚJO SILVA, FRANCISCO DE ASSIS CARVALHO E SILVA, UBIRATAN MOREIRA DELGADO, EDUARDO SÉRGIO DE ALMEIDA, WOLNEY DE MACEDO CORDEIRO, HERMINEGILDA LEITE MACHADO,**

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 a importância de promover a governança da Segurança da Informação na instituição, alinhada ao Planejamento Estratégico Institucional;

CONSIDERANDO a importância de estabelecer objetivos, princípios e diretrizes de Segurança da Informação, alinhadas às recomendações e boas práticas relacionadas ao tema;

CONSIDERANDO a importância da Segurança da Informação para a continuidade da prestação jurisdicional;

CONSIDERANDO que a Segurança da Informação é uma área sistêmica e mais abrangente, englobando a proteção de dados pessoais e a Segurança Cibernética;

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:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer 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.

Art. 2º São princípios básicos da POSIC e do SGSI:

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

II - privacidade e a proteção de dados pessoais;

III - continuidade da prestação jurisdicional;

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

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

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

Art. 3º Para efeitos deste normativo, aplicam-se as seguintes definições:

I - 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; e

XIII - Segurança Cibernética: segmento da Segurança da Informação que visa proteger as informações armazenadas nos computadores e aparelhos de computação, e transmitidas através das redes de comunicação, incluindo a Internet.

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

Parágrafo único. As informações produzidas no âmbito do Tribunal são patrimônio intelectual da instituição, não cabendo a seus criadores qualquer forma de direito autoral.

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 passível de monitoramento e controle pela instituição.

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

Art. 7º A segurança física e patrimonial deve observar, no que couber, as disposições deste normativo, 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 as diretrizes fundamentais e os princípios basilares relacionados à Segurança da Informação que devem ser incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico Institucional;

II - Normas de Segurança da Informação (nível tático): complementares à POSIC e instituídas por Atos da Presidência do Tribunal, especificam as obrigações a serem seguidas de acordo com as diretrizes estabelecidas na POSIC; e

III - Procedimentos de Segurança da Informação (nível operacional): contemplam regras operacionais, roteiros e manuais com informações técnicas que instrumentalizam o disposto 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 no site institucional em portal destinado ao tema, 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 organizacional da Segurança da Informação na instituição é disposta conforme segue:

I - Comitê Gestor de Segurança da Informação (CGSI): regulamentado por Ato da Presidência do Tribunal, com a seguinte composição:

a) Juiz(a) Auxiliar da Presidência, coordenador(a);

b) Juiz(a) Auxiliar da Vice-Presidência, vice-coordenador(a);

c) magistrado(a) indicado pela Presidência;

d) Secretário(a)-Geral da Presidência;

e) Diretor(a) Geral da Secretaria;

f) Diretor(a) da Secretaria de Governança e Gestão Estratégica;

g) Diretor(a) da Secretaria de Tecnologia da Informação e Comunicação;

h) Assessor(a) Jurídico(a) da Presidência;

i) Assessor(a) de Governança de Segurança da Informação;

j) Assessor(a) de Governança de Tecnologia da Informação e Comunicação; e

k) Agente responsável pela Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética.

II - Assessoria de Governança de Segurança da Informação (AGSI): conforme disposto no Manual de Organização da instituição, subordinada à Secretaria de Governança e Gestão Estratégica, composta por servidores efetivos;

III - Unidade de Segurança Cibernética: conforme disposto no Manual de Organização da instituição, subordinada à Secretaria de Tecnologia da Informação e Comunicação, composta por servidores efetivos do quadro de TIC; e

IV - Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR): 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. O Sistema de Gestão de Segurança da Informação (SGSI) consiste em uma uma abordagem sistemática para a gestão e proteção das informações no âmbito da instituição, abrangendo a gestão da Segurança da Informação relacionada a ativos de TIC (Segurança Cibernética), a pessoas (Segurança da Informação em Recursos Humanos), a contratos e documentos (Segurança da Informação Documental), a dados pessoais (Privacidade e Proteção de Dados Pessoais), dentre outros, integrada aos demais processos e áreas estratégicas da instituição.

Art. 11. 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; e

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

Art. 12. 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; e

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.

Art. 13. Os processos do SGSI são interdependentes e devem ser estruturados, monitorados e revisados de forma a permitir sua melhoria contínua.

Art. 14. O escopo e os processos do SGSI serão formalizados por meio de Atos da Presidência do Tribunal, devendo ser revisados sempre que necessária a atualização.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 15. Compete ao Tribunal Pleno:

I - aprovar a POSIC e a PPDP e suas revisões; e

II - aprovar a estrutura organizacional adequada à gestão do SGSI.

Art. 16. 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 dos colegiados estratégicos nas áreas de Segurança da Informação e de Proteção de Dados Pessoais;

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; e

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

Art. 17. 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; e

IX - manifestar-se sobre matérias atinentes à Segurança da Informação que lhe sejam submetidas.

Art. 18. Compete à Assessoria de Governança de Segurança da Informação (AGSI) coordenar o Sistema de Gestão de Segurança da Informação (SGSI), conforme atribuições definidas no Manual de Organização da instituição.

Art. 19. Compete à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) as ações necessárias para tratar e responder a incidentes de Segurança Cibernética na instituição, conforme atribuições definidas em seu Ato constitutivo.

Art. 20. Compete à unidade de Segurança Cibernética operacionalizar os normativos de Segurança da Informação relacionados à Segurança Cibernética, conforme atribuições definidas no Manual de Organização da instituição.

Art. 21. Compete aos(às) gestores(as) das 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; e

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

Art. 22. Compete aos magistrados(as), servidores(as), estagiários (as), aprendizes, prestadores(as) de serviços e demais usuários da instituição:

I - observar as disposições da POSIC e normas relacionadas no desempenho de suas atividades;

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

III - participar das campanhas de conscientização e dos treinamentos institucionais pertinentes aos tema Segurança da Informação e proteção de dados pessoais; e

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

Art. 23. 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. 24. São consideradas violações, exemplificativamente:

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 institucionais 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; e

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. 25. O descumprimento das disposições deste normativo 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. 26. As disposições deste normativo aplicam-se a todos os usuários internos e externos da instituição.

Art. 27. Revoga-se a Resolução Administrativa TRT13 n.º 104/2021.

Art. 28. A presente Resolução entra em vigor a partir da data de sua publicação.

MARIA CARDOSO BORGES
Chefe do Núcleo de Gestão Judiciária