RESOLUÇÃO ADMINISTRATIVA Nº 145/2019

PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO
TRIBUNAL PLENO

** Texto compilado até as alterações promovidas pela Portaria SGP/CSIN nº 382/2023.*

Institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região.

CERTIFICO que o Pleno do Egrégio Tribunal Regional do Trabalho da 18ª Região, em sessão administrativa ordinária hoje realizada, sob a Presidência do Excelentíssimo Desembargador Paulo Pimenta (Presidente do Tribunal), com a participação dos Excelentíssimos Desembargadores Daniel Viana Júnior (Vice-Presidente e Corregedor), Elvecio Moura dos Santos, Mário Sérgio Bottazzo, Geraldo Rodrigues do Nascimento, Iara Teixeira Rios, Silene Aparecida Coelho e Rosa Nair da Silva Nogueira Reis, e do Excelentíssimo Procurador-Chefe da Procuradoria Regional do Trabalho da 18ª Região, Tiago Ranieri de Oliveira, consignadas as ausências justificadas dos Excelentíssimos Desembargadores Platon Teixeira de Azevedo Filho, Kathia Maria Bomtempo de Albuquerque, Gentil Pio de Oliveira, Eugênio José Cesário Rosa e Welington Luis Peixoto, em virtude de férias, tendo em vista o que consta do Processo Administrativo Sisdoc nº 4001/2014 (MA-131/2019);

CONSIDERANDO os princípios constitucionais elencados no *caput* do artigo 37 da Constituição Federal;

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias e deveres para o uso da internet no Brasil (Marco Civil da Internet);

CONSIDERANDO a Lei nº 13.709, de 23 de abril de 2014 – Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Resolução CNJ Nº 211/2015, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o Decreto Nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dentre outras providências, no âmbito da administração pública federal (PNSI);

CONSIDERANDO a Resolução Administrativa TRT 18ª Nº 129/2016, que Regulamenta a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), no âmbito do Tribunal Regional do Trabalho da 18ª Região e dá outras providências;

CONSIDERANDO a Resolução Administrativa TRT 18ª Nº 69/2017, que aprova o Regulamento Geral de Secretaria do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Resolução Administrativa TRT 18ª Nº 83/2018, que institui o Sistema de Governança Institucional do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Resolução Administrativa TRT 18ª Nº 93/2018, que estabelece disciplinas gerais para o funcionamento das comissões e demais colegiados afins no âmbito do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO as políticas do Tribunal Regional do Trabalho da 18ª Região para Gestão de Riscos, Gestão de Continuidade de Negócios e Governança e Gestão de Tecnologia da Informação e Comunicação instituídas por Resoluções Administrativas;

CONSIDERANDO a norma brasileira NBR ISO/IEC 27014:2013, que fornece orientações sobre a governança de segurança da informação;

CONSIDERANDO a norma ISO/IEC 27000:2018, que fornece a visão geral dos sistemas de gestão de segurança da informação (SGSI) e também fornece termos e definições comumente usados na família de normas associadas a esses sistemas;

CONSIDERANDO a necessidade de revisão da Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região, até então regulamentada pela norma intitulada PO01;

CONSIDERANDO o estabelecimento de que as políticas no âmbito do Tribunal devem ser instituídas por resoluções administrativas,

RESOLVEU, por unanimidade:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art.1º Fica instituída a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região.

Art. 2º Para os fins desta Resolução, considera-se:

I – ativo: algo que tem valor e necessita ser devidamente protegido, referindo-se, no contexto desta política, à informação em seus diversos suportes e formatos, assim como aos recursos de tecnologia da informação e comunicação associados;

II – autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por um determinado indivíduo, entidade ou processo;

III – disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduo, entidades ou processos;

IV – evento de segurança da informação: ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação ou falhas de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

V – gestão de continuidade de negócios – GCN: processo abrangente de gestão que identifica ameaças potenciais para a organização e os possíveis impactos nas operações de negócios caso elas se concretizem;

VI – gestor de ativo: refere-se à unidade ou indivíduo formalmente designado para controlar o ciclo de vida de um ou mais ativos;

VII – incidente de segurança da informação: ocorrência de um único evento ou uma série de eventos de segurança da informação indesejados ou inesperados que têm uma probabilidade significativa de ameaçar a segurança da informação e comprometer as operações de negócios;

VIII – integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

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

X – segurança da Informação: preservação da integridade, da disponibilidade, da autenticidade e, quando necessário e previsto em lei ou regulamento, do sigilo da informação;

XI – sigilo ou confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

XII – usuários: magistrados, servidores e demais indivíduos, organizações e sistemas previamente autorizados a acessar e/ou utilizar recursos de TIC do Tribunal.

CAPÍTULO II

DOS OBJETIVOS

Art. 3º São objetivos da Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região:

I – estabelecer princípios de governança e gestão de segurança da informação;

II – estabelecer diretrizes para a proteção das informações, produzidas ou custodiadas pelo Tribunal Regional do Trabalho da 18ª Região, no nível adequado às obrigações e propósitos estratégicos do órgão;

III – dotar o Sistema de Governança Institucional de instância interna de apoio para tratar das questões de segurança das informações;

IV – atribuir responsabilidades para a efetiva segurança das informações.

Art. 3º-A O Tribunal Regional do Trabalho da 18ª Região observará também diretrizes, objetivos, princípios e ações da Estratégia Nacional de Segurança Cibernética - ENSEC-PJ (Res. CNJ nº 396/2021), visando a contribuir com a concretização dos objetivos da Política de Segurança Cibernética do Poder Judiciário. ***(Artigo incluído pela Portaria GP/GSI nº 304/2022)***

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º São princípios de governança e gestão da segurança da informação do Tribunal Regional do Trabalho da 18ª Região:

I – **ser integrada**:

a) atribuir responsabilidade e prestação de contas sobre segurança da informação em todos os níveis de atividades da organização;

b) integrar a segurança da informação aos processos de planejamento estratégico, orçamentário e de ações do Tribunal; e

c) incorporar a segurança da informação como elemento essencial na concepção, desenho, aquisição ou desenvolvimento, gerência, operação, suporte e manutenção de processos e projetos organizacionais, sistemas de informação, serviços e infraestrutura de tecnologia da informação;

II – **ser eficaz**:

a) propor e decidir a segurança com base na gestão corporativa de riscos em ativos de informação, visando a determinar os controles apropriados para alcançar os níveis adequados de riscos aos propósitos organizacionais; e

b) prevenir, detectar e responder efetivamente aos incidentes de segurança da informação;

III – **estar em conformidade**: atender aos requisitos internos e externos originados de legislação e regulamentações pertinentes obrigatórias e de exigências do próprio negócio e de relações contratuais;

IV – **ser positiva**: promover ambiente positivo de segurança mediante:

a) conscientização da necessidade da segurança da informação;

b) incorporação do comprometimento da gestão;

c) atenção às expectativas e exigências das partes interessadas; e

d) aprimoramento dos valores sociais;

V – **ser continuamente melhorada**: avaliar continuamente a segurança da informação com base nos resultados da organização e promover modificações necessárias.

CAPÍTULO IV

DAS DIRETRIZES

Art. 5º Os objetivos de segurança da informação serão desenvolvidos e acompanhados em conformidade com o Modelo de Gestão Estratégica do Tribunal.

Art. 6º O Tribunal Regional do Trabalho da 18ª Região manterá e aprimorará continuamente, dentro do contexto do órgão, o sistema de gestão de segurança da informação – SGSI, previamente estabelecido e implementado com base nos requisitos da norma brasileira ABNT NBR ISO/IEC 27001:2013.

Art. 7º O SGSI deve operar em abrangência e limites previamente determinados e considerar o contexto organizacional, ou seja, o ambiente de ameaça às informações, os objetivos estratégicos do órgão e as exigências legais, regulamentares e contratuais.

Art. 8º Por meio do SGSI, o Tribunal estabelecerá, implementará, manterá e aprimorará continuamente os controles internos aplicáveis à manutenção dos riscos de segurança da informação em níveis adequados aos propósitos organizacionais.

Art. 9º As informações produzidas ou custodiadas pelos usuários do Tribunal, no desempenho de suas funções, ainda que fora das dependências físicas do órgão, devem ser adequadamente protegidas por todo o ciclo vital, independentemente do meio, suporte ou formato em que se apresentem, e utilizadas exclusivamente para os fins relacionados às atividades institucionais.

Art. 10. O Tribunal adotará controles administrativos e tecnológicos para assegurar a integridade, a disponibilidade, a autenticidade e, quando necessário e previsto por lei ou regulamento, o sigilo da informação e a proteção de dados pessoais, em conformidade com os critérios de risco ou de classificação. ***(Artigo alterado pela Portaria GP/GSI nº 304/2022)***

Art. 11. Os contratos e convênios celebrados pelo Tribunal, cujo objeto envolva a utilização de ativos de informação, deverão conter cláusula exigindo a observância desta Política e das normas correlatas, que estarão disponíveis no sítio eletrônico do Tribunal na Internet.

CAPÍTULO V

DAS ESTRUTURAS DE GOVERNANÇA E GESTÃO

Art. 12. Compõem a estrutura de governança de segurança da informação:

I – Comitê de governança e estratégia; ***(Inciso alterado pela Portaria SGP/CSIN nº 382/2023)***

II – Colegiado temático de riscos institucionais; ***(Inciso alterado pela Portaria SGP/CSIN nº 382/2023)***

III – Comitê de segurança da informação e proteção de dados - CSIPD; e ***(Inciso alterado pela Portaria SGP/CSIN nº 382/2023)***

IV – ***(Revogado pela Portaria GP/GSI nº 304/2022)***

V – unidade responsável pela gestão da segurança da informação. ***(Inciso alterado pela Portaria GP/GSI nº 304/2022)***

§ 1º As competências e composições das instâncias internas de apoio à governança anunciadas nos incisos I, II e III são regulamentadas em atos normativos próprios. ***(Parágrafo alterado pela Portaria SGP/CSIN nº 382/2023)***

§ 2º As atribuições da unidade administrativa descrita no inciso V estão elencadas no Regulamento Geral de Secretaria do Tribunal Regional do Trabalho da 18ª Região.

Art. 13. Compõem a estrutura de gestão de segurança da informação:

I – unidade responsável pela gestão de segurança da informação; ***(Inciso alterado pela Portaria GP/GSI nº 304/2022)***

II – Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR; ***(Inciso alterado pela Portaria GP/GSI nº 304/2022)***

III – gestores de ativos.

§ 1º ***(Revogado pela Portaria GP/GSI nº 304/2022)***

§ 2º ***(Revogado pela Portaria GP/GSI nº 304/2022)***

Art. 14. ***(Revogado pela Portaria SGP/CSIN nº 382/2023)***

Art. 15. Compete à ETIR prestar prioritariamente o serviço de tratamento e resposta a incidentes de segurança cibernética.

Parágrafo único. A ETIR, com sua missão, público-alvo, modelo de implementação, estrutura de organização, autonomia e serviços disponibilizados, é instituída por ato normativo da Presidência. ***(Artigo alterado pela Portaria GP/GSI nº 304/2022)***

Art. 16. Compete ao Gestor de Ativo:

I – estabelecer o valor dos ativos por ele gerenciados, em escala que seja adequada aos processos de avaliação de riscos e de análise de impacto ao negócio;

II – registrar em inventário específico:

a) detalhes sobre o ativo;

b) valor;

c) requisitos de proteção;

d) custodiantes por ele indicados, se for o caso;

III – comunicar aos custodiantes e aos usuários as exigências de segurança da informação e monitorar periodicamente os controles e os riscos dos ativos sob sua responsabilidade, tomando as providências corretivas necessárias.

Parágrafo único. O processo de inventário e detalhamento dos ativos de informação, dentre outras providências, é editado por meio de ato normativo da Presidência. ***(Primitivo § 1º renumerado pela Portaria GP/GSI nº 304/2022)***

§ 2º ***(Revogado pela Portaria GP/GSI nº 304/2022)***

§ 3º ***(Revogado pela Portaria GP/GSI nº 304/2022)***

CAPÍTULO VI

DAS RESPONSABILIDADES GERAIS

Art. 17. Compete ao usuário zelar, no âmbito de sua unidade, pela observância das disposições constantes desta Política, bem como pelas normas relativas à segurança da informação que vierem a ser editadas, comunicando à autoridade superior as eventuais irregularidades.

Parágrafo único. A inobservância das diretrizes previstas nesta Política, assim como das normas e procedimentos a ela associadas, será devidamente apurada, podendo ensejar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa. ***(Parágrafo alterado pela Portaria GP/GSI nº 304/2022)***

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 18. A presente Resolução Administrativa substitui o conteúdo referenciado como documento “PO01” ou “Política de Segurança da Informação”, presente nos atos normativos de segurança da informação vigentes.

Art. 19. Esta Resolução Administrativa entra em vigor na data de sua publicação, revogando-se a Portaria TRT 18ª GP/NGTIC nº 001/2016.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

Goiânia, 17 de dezembro de 2019.

(*assinado eletronicamente*)
Thiago Domiciano de Almeida
Secretário-Geral da Presidência
Tribunal Regional do Trabalho da 18ª Região