PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO
SECRETARIA DO TRIBUNAL PLENO

ATO GP Nº45, DE 21 DE MAIO DE 2018

Estabelece nova Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª Região.

O **DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro, de forma a oferecer todas as informações necessárias aos processos deste Tribunal com integridade, confidencialidade e disponibilidade;

CONSIDERANDO as melhores práticas para a proteção e controle da informação referenciadas na família de normas NBR ISO/IEC 27000, seguidas pelas principais organizações e órgãos governamentais;

CONSIDERANDO as diretrizes gerais para a implantação da Gestão de Segurança da Informação no Poder Judiciário publicadas pelo CNJ;

CONSIDERANDO que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade,

RESOLVE, *ad referendum* do Tribunal Pleno:

CAPÍTULO I

Art 1º Estabelecer, através deste Ato, nova Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª Região (TRT19) e dos órgãos que integram a sua estrutura.

DAS DISPOSIÇÕES PRELIMINARES

Art 2º Para efeitos deste Ato aplicam-se as seguintes definições:

I – Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

II – Disponibilidade: Garantia de que usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

III – Integridade: Salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

IV – Segurança da informação: Preservação da confidencialidade, da integridade e da disponibilidade da informação;

V – Política de Segurança da Informação (PSI): Conjunto de intenções e diretrizes globais, formalmente expressas com o objetivo de garantir a segurança da informação no âmbito da instituição;

VI – Recurso de Tecnologia da Informação e Comunicações (TIC): qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

VII – Hardware é a parte física do computador ou dispositivo de TIC, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placa;

VIII – Software é qualquer programa, aplicativo ou sistema desenvolvido para utilização em computadores ou em outros dispositivos eletroeletrônicos;

IX – Ativo de informação: patrimônio composto por pessoas, por elementos de infraestrutura tecnológica (hardware e software), bem como pelos dados e informações gerados e manipulados nos processos de trabalho do Tribunal;

X – Ambiente tecnológico: conjunto de recursos que utilizam ou disponibilizam serviços de tecnologia da informação e sistemas de informação do Tribunal;

XI – Análise de risco e vulnerabilidades: avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação e da probabilidade de sua ocorrência;

XII – Usuários: conjunto composto por magistrados, servidores, prestadores de serviços e estagiários no exercício de suas funções públicas como também usuários externos, para fins de segurança da informação, que tenham acesso aos

recursos de Tecnologia da Informação sob responsabilidade da Secretaria de Tecnologia da Informação e Comunicações (SETIC), divididos da seguinte forma:

a) Usuário interno: magistrados e servidores ativos do quadro efetivo, servidores cedidos ou removidos deste ou para este tribunal, ou ainda unidade do Tribunal;

b) Usuário especial: magistrados e servidores aposentados e pensionistas;

c) Usuário colaborador: prestador de serviço terceirizado, estagiário, consultor ou outro colaborador do Tribunal;

d) Usuário externo: pessoa física ou jurídica;

XIII – Proprietário da informação: pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade cada uma se enquadra.

Art 3º As disposições desta Política de Segurança da Informação, normas e procedimentos relacionados aplicam-se a todos os usuários do Tribunal.

Art 4º As informações geradas no âmbito deste Tribunal são de sua propriedade, independente da forma de apresentação ou armazenamento, de modo que essas informações devem ser adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades desenvolvidas neste Tribunal.

Parágrafo Único. Toda informação gerada no Tribunal deverá ser classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

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

§ 1° Os recursos de TIC, pertencentes ao TRT19 e que estão disponíveis para os usuários, devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2° A utilização dos recursos de TIC será monitorada pela instituição.

Art 6º Deverá ser elaborado um Modelo de Gestão que permita a criação e a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI),

em conformidade com as diretrizes para a Gestão de Segurança da Informação publicadas pelo CNJ.

CAPÍTULO II
DA ESTRUTURA NORMATIVA

Art 7º A estrutura normativa da Segurança da Informação será organizada da seguinte forma:

I – Política de Segurança da Informação em nível estratégico: constituída pelo presente documento, define as regras de alto nível que representam os princípios básicos incorporados pela instituição à sua gestão, 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 em nível tático: contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas na PSI. Especificam, no plano tático, os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política. As normas devem abranger, no mínimo:

a) Tratamento e classificação da informação;

b) Tratamento de incidentes;

c) Tratamento de códigos maliciosos;

d) Controle de acesso lógico e físico;

e) Contingência e continuidade do negócio;

f) Monitoração e auditoria de recursos de TIC;

g) Utilização de recursos de TIC;

h) Geração e restauração de cópias de segurança - backup.

III – Procedimentos de Segurança da Informação em nível operacional: instrumentalizam o disposto na política e nas normas, permitindo a direta aplicação nas atividades da instituição.

Art 8º Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser aprovados e revisados conforme os critérios a seguir:

I – Política

- Nível de aprovação: Tribunal Pleno
- Periodicidade da revisão: bienal

II – Normas

- Nível de aprovação: Presidência do Tribunal
- Periodicidade da revisão: bienal

III – Procedimentos

- Nível de aprovação: Diretoria da área ou unidade envolvida
- Periodicidade da revisão: anual

Art 9º A política e as normas integrantes da estrutura normativa devem ser divulgadas a todos os usuários quando de sua posse/admissão, bem como através dos meios oficiais de divulgação interna da instituição e, também, publicadas na Intranet institucional, de maneira que seu conteúdo possa ser consultado a qualquer momento.

CAPÍTULO III
DA ESTRUTURA FUNCIONAL

Art 10. O Comitê Gestor de Segurança da Informação (CGSI), composto por representantes das áreas Jurídica, Administrativa e TIC, instituído em Ato da Presidência, terá as seguintes responsabilidades:

I – Propor à Presidência do Tribunal normas de Segurança da Informação;

II – Rever periodicamente a Política de Segurança da Informação e normas relacionadas, sugerindo possíveis alterações;

III – Dirimir dúvidas e deliberar sobre questões não contempladas na política e normas de Segurança da Informação;

IV – Propor e acompanhar planos de ação para aplicação da política e normas de Segurança da Informação;

V – Promover a cultura de Segurança da Informação na instituição;

VI – Propor a criação de grupos de trabalho para tratar de temas e soluções específicas sobre Segurança da Informação;

VII – Receber e analisar as comunicações de descumprimento da política e normas de Segurança da Informação e apresentar parecer à autoridade ou ao órgão competente à sua apreciação;

VIII – Solicitar, sempre que necessário, a realização de auditorias pela área de Segurança da Informação, relacionadas ao uso dos recursos de TIC no âmbito do Tribunal;

IX – Apoiar as ações estratégicas para a implantação dos processos mínimos especificados para o Modelo de Gestão da Segurança da Informação.

Art 11. A unidade responsável pelo Macroprocesso de Segurança da Informação de que trata a Resolução Nº 211/2015 do CNJ, estrategicamente subordinada à diretoria da área gestora de TIC, será composta por servidores efetivos do quadro de TIC e terá as seguintes atribuições:

I – Coordenar o Sistema de Gestão de Segurança da Informação (SGSI), em conformidade com as diretrizes para a Gestão de Segurança da Informação publicadas pelo CNJ;

II – Elaborar o Plano Diretor de Segurança da Informação, a partir das definições estratégicas estabelecidas pelo CGSI;

III – Coordenar as ações do Plano Diretor de Segurança da Informação e dos projetos relacionados;

IV – Coordenar a Gestão da Política de Segurança da Informação;

V – Coordenar a Gestão do Plano de Continuidade do Negócio;

VI – Coordenar a Gestão de Riscos em Segurança da Informação, visando minimizar os riscos associados à informação, apresentando as medidas de segurança necessárias;

VII – Coordenar a Gestão de Vulnerabilidades em TIC, visando a detecção, remoção e controle de vulnerabilidades;

VIII – Gerenciar as ações necessárias na ocorrência de incidentes de Segurança da Informação, coordenando o Grupo de Resposta a Incidentes de Segurança da Informação (GRISI);

IX – Fornecer subsídios para as atividades do CGSI;

X – Promover palestras e treinamentos para conscientização dos usuários e atualização das ações de Segurança da Informação;

XI – Emitir relatórios sobre o uso dos recursos de tecnologia, apontando irregularidades e não-conformidades na utilização;

XII – Atuar de forma coordenada com outras áreas nos assuntos de Segurança da Informação;

XIII – Informar ao CGSI:

a) Nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de riscos e vulnerabilidades;

b) Incidentes de segurança tecnológica.

Art 12. O Grupo de Resposta a Incidentes de Segurança da Informação, composto por servidores indicados pela área de TIC, terá as seguintes atribuições:

I – Avaliar fragilidades e eventos de segurança associados, principalmente, aos ativos críticos de TIC;

II – Comunicar à unidade responsável pelo Macroprocesso de Segurança da Informação a ocorrência de eventos de segurança para tratamento em tempo hábil.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art 13. Compete aos usuários da instituição:

I – Zelar continuamente pela proteção das informações institucionais contra acesso, modificação, destruição ou divulgação não autorizada;

II – Assegurar que os recursos, computacionais ou não, colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias da instituição;

III – Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

IV – Comunicar imediatamente ao CGSI qualquer descumprimento da Política de Segurança da Informação ou de normas e procedimentos relacionados.

Art 14. Compete ao Tribunal Pleno aprovar a Política de Segurança da Informação e suas revisões.

Art 15. Compete à Presidência do Tribunal:

I – Aprovar as normas de Segurança da Informação e suas revisões;

II – Aprovar a criação e composição do CGSI, da Unidade responsável pelo Macroprocesso de Segurança da Informação e do Grupo de Resposta a Incidentes de Segurança da Informação;

III – Receber, por intermédio do CGSI, relatórios de violações da política e das normas de Segurança da Informação, quando aplicável;

IV – Deliberar sobre os casos de descumprimento da política e das normas de Segurança da Informação, mediante recomendações do CGSI.

Art 16. Compete aos Diretores, Secretários e demais Gestores de unidades:

I – Verificar a observância das disposições desta política, normas e procedimentos de Segurança da Informação no âmbito de sua área, comunicando ao CGSI eventuais irregularidades;

II – Assegurar que suas equipes possuam acesso e entendimento da política, normas e procedimentos de Segurança da Informação;

III – Redigir e detalhar, técnica e operacionalmente, os procedimentos de Segurança da Informação relacionados às suas unidades, quando solicitado pelo CGSI.

Art 17. Compete à Secretaria Jurídico-Administrativa avaliar, sempre que solicitada, os aspectos jurídicos inerentes à política, às normas e aos procedimentos de Segurança da Informação.

Art 18. Compete à Secretaria de Tecnologia da Informação e Comunicações:

I – Operacionalizar os normativos provenientes da Política de Segurança da Informação relacionados aos recursos de TIC;

II – Monitorar a utilização dos recursos de TIC, mantendo seus registros.

Art 19. Compete à Coordenadoria de Comunicação Social executar as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação e documentos relacionados.

CAPÍTULO V
DAS VIOLAÇÕES E SANÇÕES

Art 20. São consideradas violações à política, às normas ou aos procedimentos de Segurança da Informação as seguintes situações:

I – Quaisquer ações ou situações que possam expor a instituição à perda financeira ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

II – Utilização indevida de dados institucionais e divulgação não autorizada de informações, sem a permissão expressa do proprietário da informação;

III – Uso de dados, informações ou recursos 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 política, de normas ou de procedimentos de Segurança da Informação, que porventura um usuário venha a tomar conhecimento.

Art 21. O descumprimento à política, às normas e aos procedimentos de Segurança da Informação será comunicado à autoridade competente para providências cabíveis.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art 22. O presente Ato entra em vigor a partir da data de sua publicação e revoga a **RESOLUÇÃO ADMINISTRATIVA N. 12/2008**.

Publique-se no D.E.J.T e no B.I.

Original assinado

PEDRO INÁCIO DA SILVA

Desembargador Presidente

Publicado no D.E.J.T e no BI nº 05 de 21/05/2018.