Processo Administrativo: 00223.00.80.2014.5.13.0000

RESOLUÇÃO ADMINISTRATIVA Nº 133/2014

O Egrégio **TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO**, em Sessão Administrativa realizada em 20.11.2014, sob a Presidência de Sua Excelência o Senhor Desembargador **CARLOS COELHO DE MIRANDA FREIRE**, com a presença do Representante da Procuradoria Regional do Trabalho, Sua Excelência o Senhor Procurador **FLÁVIO HENRIQUE EVANGELISTA FREITAS GONDIM**, presentes Suas Excelências os Senhores Desembargadores **UBIRATAN MOREIRA DELGADO**, **ANA MARIA FERREIRA MADRUGA**, **FRANCISCO DE ASSIS CARVALHO E SILVA**, **EDVALDO DE ANDRADE**, **EDUARDO SÉRGIO DE ALMEIDA**, **WOLNEY DE MACEDO CORDEIRO** e **LEONARDO JOSÉ VIDERES TRAJANO**,

CONSIDERANDO a importância da Segurança da Informação para o processo judicial eletrônico, em um cenário onde incidentes são cada vez mais frequentes;

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

CONSIDERANDO a necessidade de atualizar a Política de Segurança da Informação e Comunicações da instituição;

CONSIDERANDO a necessidade de rever a estrutura, diretrizes e responsabilidades referentes à Segurança da Informação, visando garantir a integridade, confidencialidade e disponibilidade das informações;

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:

Art. 1° Estabelecer, através desta RA, a nova Política de Segurança da Informação e Comunicações do Tribunal Regional do Trabalho da 13ª Região.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

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

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

II- Política de Segurança da Informação e Comunicações (POSIC): conjunto de intenções e diretrizes globais formalmente expressas com o objetivo de garantir a Segurança da Informação no âmbito da instituição;

III- Confidencialidade: garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;
IV- Integridade: garantia de que a informação esteja inalterada desde sua geração ou alteração autorizada;

V- Disponibilidade: garantia de que a informação esteja sempre disponível às pessoas autorizadas;

VI- Recurso de tecnologia da informação e comunicações (TIC): qualquer equipamento, dispositivo, serviço, infra-estrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

VII- Usuário: qualquer pessoa que utilize

sistemas e/ou demais recursos de TIC da instituição;

VIII- Plano de Continuidade do Negócio: conjunto de ações de prevenção e procedimentos de recuperação 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;

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

Art. 3° As disposições desta Política de Segurança da Informação e Comunicações, normas e procedimentos relacionados aplicam-se a todos os usuários: magistrados; servidores efetivos, requisitados e cedidos; terceirizados; consultores; estagiários; pensionistas; jurisdicionados e inativos.

Parágrafo Único. As disposições são válidas para outras pessoas que se encontrem a serviço do Tribunal Regional do Trabalho da 13ª Região, autorizadas a utilizar temporariamente os recursos de tecnologia da informação e comunicações da instituição.

Art. 4° O uso adequado dos recursos de tecnologia da informação e comunicações visa garantir a continuidade da prestação jurisdicional deste Tribunal.

§ 1° Os recursos de tecnologia da informação e comunicações, pertencentes ao Tribunal Regional do Trabalho da 13ª Região e que estão disponíveis para os usuários, devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2° A utilização dos recursos de tecnologia da informação e comunicações será monitorada pela instituição.

Art. 5° As informações geradas no âmbito deste Tribunal são de sua propriedade,independente da forma de

apresentação ou armazenamento. Assim, 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. 6° 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. 7° A estrutura normativa da Segurança da Informação será organizada da seguinte forma:

I- Política de Segurança da Informação e Comunicações (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 (nível tático): contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações. 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 (Internet, redes sociais, correio eletrônico, equipamentos, softwares, armazenamento lógico, outros);

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

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

Art. 8° 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 Tribunal

· Periodicidade da revisão: bienal

III- Procedimentos

· Nível de aprovação: Diretoria da área/unidade envolvida

· Periodicidade da revisão: anual

Art. 9° A política e as normas integrantes da estrutura normativa devem ser divulgadas a todos os magistrados, servidores, estagiários e prestadores de serviços 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 de TIC, 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 Comunicações 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- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

VII- Receber e analisar as comunicações de descumprimento da política e normas de Segurança da Informação, apresentando parecer à autoridade/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 O Núcleo de Segurança da Informação (NSI), estrategicamente posicionado diretamente subordinado à diretoria da área gestora de TIC, composto por servidores efetivos do quadro de TIC, terá as seguintes responsabilidades:

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 e Comunicações;

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;

b) Incidentes de segurança tecnológica.

Art.12 O Grupo de Resposta a Incidentes de Segurança da Informação (GRISI), composto por servidores efetivos do quadro de TIC, terá as seguintes responsabilidades:

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

II- Comunicar ao NSI ocorrência de eventos de segurança para tratamento em tempo hábil.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art.13 Compete aos magistrados, servidores, estagiários, prestadores de serviços e demais 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 e Comunicações e/ou das normas e procedimentos relacionados.

Art.14 Compete ao Tribunal Pleno:

I- Aprovar a Política de Segurança da Informação e Comunicações 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, do NSI e do GRISI ;

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 e demais Gestores de áreas/unidades:

I- Verificar a observância das disposições desta política, normas e procedimentos de Segurança da Informação no âmbito de sua área/unidade, 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 áreas/unidades, quando solicitado pelo CGSI.

Art.17 Compete à unidade de assesoria jurídica da Presidência:

I- Informar ao CGSI e demais áreas/unidades envolvidas eventuais alterações legais e/ou regulatórias que impliquem responsabilidades e ações envolvendo a gestão da Segurança da Informação;

II- Recomendar, sempre que necessário, a inclusão de cláusulas específicas relacionadas à Segurança da Informação na análise e elaboração de contratos, visando proteger os interesses da instituição;

III- Avaliar, sempre que solicitado, os aspectos jurídicos inerentes à política, normas e procedimentos de Segurança da Informação.

Art.18 Compete à unidade gestora de recursos humanos:

I- Garantir que magistrados, servidores, estagiários, prestadores de serviços e demais usuários da instituição comprovem, mediante Termo de Responsabilidade, ciência da estrutura normativa da Segurança da Informação;

II- Informar às áreas/unidades envolvidas alterações no quadro funcional da instituição.

Art.19 Compete à unidade gestora de TIC:

I- Operacionalizar os normativos provenientes da Política de Segurança da Informação e Comunicações relacionados aos recursos de TIC;

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

Art.20 Compete à unidade de assessoria de comunicação social:

I- Executar as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação e Comunicações e documentos relacionados.

CAPÍTULO V

DAS VIOLAÇÕES E SANÇÕES

Art.21 São consideradas violações à política, às normas ou aos procedimentos de Segurança da Informação as seguintes situações, não se limitando às mesmas:

I- Quaisquer ações ou situações que possam expôr a instituição à perda financeira e/ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação e comunicações;

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.22 O descumprimento à política, às normas e aos procedimentos de Segurança da Informação 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.23 A presente RA entra em vigor a partir da data de sua publicação.

Art.24 Revogam-se as disposições em contrário, especialmente a RA nº 65/2007, de 18 de julho de 2007.

OBSERVAÇÕES: Suas Excelências os Senhores Desembargadores Ana Maria Ferreira Madruga e Francisco de Assis Carvalho e Silva participaram desta Sessão Administrativa nos termos do artigo 29 do Regimento Interno. Ausente, justificadamente, Sua Excelência o Senhor Desembargador Paulo Maia Filho, que se encontra afastado para atuar junto ao C. Tribunal Superior do Trabalho (Resolução Administrativa nº 48/2014).

MARIA CARDOSO BORGES
Secretária do Tribunal Pleno e de
Coordenação Judiciária - Substituta