PORTARIA N. 8.604, de 05 de novembro de 2013.

Altera a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de revisar e aprimorar a atual Política de Segurança da Informação, instituída pela Portaria 4772/2008 da Presidência deste Tribunal, com a normatização de situações ainda não regradas e atualização das normas já existentes para que estejam adequadas à atual realidade da Justiça do Trabalho da 4ª Região;

CONSIDERANDO a recomendação do Tribunal de Contas da União, no sentido de alinhamento da Política de Segurança às diretrizes nacionais, contemplando itens não normatizados (item 9.1.1 do Acórdão 381/11);

CONSIDERANDO o parecer favorável da Comissão de Informática deste Tribunal à proposta apresentada pelo Comitê de Segurança da Informação;

RESOLVE:

Art. 1º Alterar os artigos 1º e 9º, inciso II, da Portaria 4772/08, que passam a vigorar com a seguinte redação:

Art. 1º Estabelecer a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região, da qual são parte integrante todas as normas e procedimentos complementares e afins editados pelo Tribunal, e que tem como objetivo garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal, com integridade, confidencialidade e disponibilidade.

Parágrafo único. A presente Política de Segurança da Informação tem por fundamento as seguintes referências legais e normativas:

I- Decreto nº 3.505, de 13 de junho de 2000, que institui a Politica de Segurança da Informação nos Órgãos e entidades da Administração Pública Federal;

II - Instrução Normativa GSI/PR nº 1, de junho de 2008, que disciplina

a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta , e dá outras providências;
III - Norma 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que cria metodologia de gestão de segurança da informação e comunicações;
IV - Norma 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que cria diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;
V - Resolução nº 70, de 18 de março de 2009, do Conselho Nacional de Justiça, que dispõe sobre o Planejamento e a gestão Estratégica no âmbito do Poder Judiciário e dá outras providências;
VI - Resolução nº 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário;
VII- "Control Objectives for Information and related Technology 4.1 – COBIT 4.1", modelo de gestão de Governança em TI;
VIII - Norma NBR ISO/IEC 27001:2006, que normatiza o sistema de gestão da segurança da informação;
IX - Norma NBR ISO/IEC 27002:2005, que normatiza a prática para gestão da segurança da informação;
X - Norma NBR 15999-1:2007, que normatiza a prática para gestão de continuidade de negócios.
XI - Código Penal Brasileiro
XII - Lei 8112/90

Art. 9º (…)
II - Rever, no período máximo de dois anos, essa Política de Segurança e normas relacionadas sugerindo possíveis alterações.

Art. 2º Alterar a Portaria 4772/2008 da Presidência deste Tribunal, que passa a vigorar acrescida dos artigos 14-A e 14-B:

Art. 14-A - Será criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, sob a coordenação do Escritório de Segurança da Informação.

Art. 14-B – Compete a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:

I. Opinar sobre assuntos relacionados a tratamento e resposta a incidentes em redes computacionais;
II. propor as metodologias e processos específicos para tratamento e resposta a incidentes em redes computacionais, tais como análise, avaliação de riscos e vulnerabilidades;
III. prover ações de monitoria, auditoria e registro de dados em redes computacionais;
IV. participar na elaboração de planos de continuidade;
V. analisar tecnicamente e monitorar incidentes de segurança da informação;
VI. realizar testes e verificações em sistemas e serviços de redes computacionais;
VII. participar de investigações de incidentes de segurança da informação;
VIII. identificar e avaliar os riscos decorrentes da implementação de mudanças no ambiental computacional.

Art. 3º Alterar os itens 1.1.3, 1.1.6., 1.2.1, 1.2.2, 1.2.4, 1.2.5, 1.2.6, 1.2.7 e 1.3.1 do Anexo 2 (NSI002 – Controle de Uso do Correio Eletrônico), integrante da Portaria 4772/2008, que passam a vigorar com a seguinte redação:

1.1.3. As contas de que trata o subitem 1.1.2 serão de uso dos responsáveis pelas unidades, que poderão autorizar o acesso a outros servidores, mediante delegação expressa no sistema de correio eletrônico.

1.1.3.1. Cabe ao responsável pela caixa postal da unidade excluir o acesso de servidor anteriormente designado, nos casos em que houver afastamento ou desligamento da unidade ou sempre que entender necessário.

1.1.6. As mensagens de correio eletrônico de terceirizados e estagiários só poderão ser enviadas para endereços dentro do âmbito do TRT. Caso seja necessário, para interesse do serviço, o envio de mensagens para endereço externo, o responsável pela unidade administrativa deverá solicitar o acesso à Seção de Atendimento ao Usuário, com a respectiva justificativa.

1.2.1. As solicitações de novas caixas postais deverão ser encaminhadas à Secretaria de Tecnologia da Informação e Comunicações, pela chefia imediata ou superior, com os respectivos dados cadastrais.

1.2.2. Cabe à chefia imediata ou superior comunicar à Secretaria de Tecnologia da Informação e Comunicações o desligamento de empregados terceirizados, temporários e estagiários sob sua

responsabilidade para a exclusão definitiva da caixa postal.

1.2.4. As caixas postais de servidores e magistrados falecidos ou afastados em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão ou retorno à origem serão desativadas 48 horas após a comunicação pela Secretaria de Gestão de Pessoas à Secretaria de Tecnologia da Informação e Comunicações das situações referidas anteriormente.

1.2.5. As caixas postais deste Tribunal são limitadas a 25 gigabytes (GB).

1.2.6. A Secretaria de Tecnologia de Informação e Comunicações manterá um processo sistemático para armazenamento dos arquivos de registro de mensagens (logs) de correio eletrônico.

1.2.7. Os arquivos de registro de mensagens (logs) de correio eletrônico serão mantidos pelo período de 30 dias, pelo menos.

1.3.1. O tamanho máximo da mensagem enviada ou recebida, incluindo todos os seus anexos, não excederá 20 megabytes (MB).

Art. 4º – Suprimir os itens 1.3.2.1, 1.3.4., 1.4, 1.4.1, 1.5 e 1.5.1, do Anexo 2 (NSI002 – Controle de Uso do Correio Eletrônico), integrante da Portaria 4772/2008.

Art. 5º. Alterar a Portaria 4772/2008 da Presidência deste Tribunal para incluir o Anexo 3 (NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso), com a seguinte redação:

ANEXO 3

NSI 003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso

1.Utilização dos recursos de tecnologia da informação

1.1. O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade da prestação jurisdicional deste Tribunal.

1.2. Os recursos de tecnologia da informação disponibilizados pelo Tribunal Regional do Trabalho da 4ª Região ao usuário, serão utilizados em atividades relacionadas às suas funções institucionais, e abrangem os

seguintes elementos:

I - Os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios.

II - As contas de acesso dos usuários e os canais e pontos de distribuição e acesso à rede de dados do TRT e a redes externas, assim como os certificados digitais.

III - Os sistemas computacionais desenvolvidos com base nos recursos providos pelo TRT

IV - Os sistemas computacionais contratados de terceiros, sob licença ou na forma de software livre ou aberto, incluídas as soluções baseadas em nuvem.

1.3. É de responsabilidade do usuário zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização pessoal, tais como computadores, impressoras, dispositivos móveis e demais equipamentos.

1.4. As licenças de softwares, de qualquer natureza, contratadas ou adquiridas pelo TRT são de uso institucional, privativo deste Tribunal.

1.5. Este Tribunal utilizará, preferencialmente, em suas atividades, Software Livre ou de Código Aberto.

1.5.1. Fica definida como padrão a suíte de escritório LibreOffice desenvolvida pela Associação Civil sem Fins Lucrativos BrOffice.org Projeto Brasil.

1.6. É proibida a instalação de softwares não licenciados ou não homologados pela Secretaria de Tecnologia da Informação e Comunicações nos equipamentos conectados à rede do Tribunal.

1.6.1. A instalação de softwares não homologados poderá ser autorizada excepcionalmente pelo Comitê de Segurança da Informação desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança e proteção estabelecidas, bem como a compatibilidade e adequação aos recursos computacionais disponibilizados pelo TRT.

1.6.2. As unidades organizacionais do Tribunal poderão encaminhar à Secretaria de Tecnologia da Informação e Comunicações pedido de homologação de softwares para uso em suas atividades. Homologado o uso, o software passará a integrar o padrão utilizado

na configuração dos novos equipamentos. Quando necessário, o pedido, acompanhado de parecer técnico, será submetido ao Comitê de Segurança da Informação.

1.7. É proibido o armazenamento em qualquer diretório na rede do Tribunal ou nas soluções baseadas em nuvem de arquivos não relacionados ao trabalho, que ficam sujeitos à exclusão, sem prévio aviso, pela Secretaria de Tecnologia da Informação e Comunicações, tais como:

I – fotos, músicas e filmes de qualquer formato;

II – programas não homologados ou não licenciados;

III – programas de conteúdo prejudicial à segurança do parque computacional deste Tribunal.

1.7.1. Os arquivos armazenados na nuvem corporativa poderão ser compartilhados exclusivamente com outros usuários do TRT.

1.7.2. É vedado o armazenamento na nuvem corporativa de arquivos para cuja edição o TRT disponibilize sistemas próprios, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas.

1.8. A cada ponto de acesso à rede de dados do TRT poderá ser conectado apenas um equipamento, vedando-se a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da Secretaria de Tecnologia da Informação e Comunicações.

1.9. É proibida a conexão de qualquer dispositivo não fornecido pelo TRT na rede de computadores sem a prévia anuência da Secretaria de Tecnologia da Informação e Comunicações.

1.9.1. A conexão de qualquer equipamento à rede de dados do TRT será feita pela Secretaria de Tecnologia da Informação e Comunicações, ou por terceiros por ela autorizados.

1.10. Os procedimentos de manutenção dos equipamentos de informática serão realizados pela Secretaria de Tecnologia da Informação e Comunicações, ou por terceiros por ela autorizados.

1.11. O serviço de mensageria instantânea disponibilizado pelo TRT destina-se exclusivamente às comunicações internas.

2. Acesso à rede e aos sistemas computacionais.

2.1. O acesso à rede, serviços e aos sistemas computacionais disponibilizados pelo TRT serão solicitados à Secretaria de Tecnologia da Informação e Comunicações, mediante o preenchimento de formulário eletrônico, disponível na Intranet, em que definidos os níveis de acesso adequados às atribuições desenvolvidas.

2.2. A solicitação deverá conter a autorização pela chefia imediata, responsável pelos acessos concedidos e pelas informações a que o servidor terá acesso.

2.3. Incumbe à chefia imediata solicitar à Secretaria de Tecnologia da Informação e Comunicações:

I - a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor da unidade, sempre que necessária sua adequação às atividades desenvolvidas;

II -a remoção dos acessos concedidos ao servidor, imediatamente após o afastamento ou desligamento da unidade.

2.4. Não solicitada a referida alteração/exclusão, a chefia poderá ser responsabilizada pelo acesso indevido do servidor a informações da unidade judiciária.

2.5. A Assessoria de Juízes informará à Secretaria de Tecnologia da Informação e Comunicações a nomeação/posse de novos magistrados, a fim de agilizar o primeiro cadastro.

2.6. Os usuários aposentados, cedidos e removidos, terão acesso aos serviços administrativos via extranet.

2.7. A Secretaria de Tecnologia da Informação e Comunicações comunicará à unidade judiciária a efetivação do cadastro e fornecerá as informações necessárias ao acesso, bem como orientação sobre a necessidade de ciência sobre a Política de Segurança da Informação.

2.7.1. As novas senhas solicitadas serão fornecidas por meio de comunicação eletrônica para a caixa da unidade judiciária ou caixa pessoal-funcional do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

2.8. O usuário é responsável pela preservação do sigilo das informações a

que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados.

3. Criação e utilização de senhas e recursos de autenticação

3.1. A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

3.2. É responsabilidade do usuário a alteração da senha inicial fornecida pela Secretaria de Tecnologia da Informação e Comunicações no primeiro acesso realizado.

3.3. A preservação e o sigilo da senha de acesso ou de outro mecanismo de autenticação que venha a ser utilizado, assim como os atos decorrentes de seu uso, são de responsabilidade do titular da credencial.

3.4. Na utilização das senhas de autenticação, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos computacionais a partir de sua senha de acesso:

I - não compartilhar a senha com outra pessoa;

II - não anotar a senha;

III – não utilizar senhas de fácil dedução como as que contém nomes próprios e de familiares, datas festivas e sequências numéricas;

IV - ao ausentar-se, ainda que temporariamente, durante a sessão de uso de determinado recurso de Tecnologia da Informação, o usuário deverá encerrar a sessão ou efetuar o bloqueio do acesso.

3.5. A senha deverá satisfazer os seguintes requisitos de complexidade:

I. não conter nome da conta do usuário (login) ou mais de dois caracteres consecutivos de partes de seu nome completo;

II. ter pelo menos seis caracteres

III. conter caracteres de três destas quatro categorias:

a. caracteres maiúsculos (A-Z)

b. caracteres minúsculos (a-z)

c. dígitos de base 10 (0 a 9)

d. caracteres não alfabéticos (como !, $, #, %)

3.5.1. Excetuam-se da regra do item 3.5. os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

3.6. A senha deverá ser alterada com uma periodicidade mínima de 1 (um) dia e máxima de 180 (cento e oitenta) dias desde a última modificação.

3.7. A conta do usuário será bloqueada após 10 tentativas consecutivas de acesso não reconhecidas.

3.8. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente ao Escritório de Segurança da Informação, que poderá, como medida preventiva, suspender temporariamente o acesso.

4. Criação de Identificação de Usuário

4.1. A identificação de usuários será composta pela primeira letra do prenome e o último sobrenome do servidor ou magistrado.

4.2. Em situações justificadas, poderá ser utilizado outro prenome ou sobrenome para a composição da identificação.

5. Registros (log) de Eventos

5.1. Serão mantidos, por um período mínimo de três (3) meses, os registros dos acessos dos usuários aos sistemas disponibilizados pelo TRT, inclusive para fins de apuração e comprovação de incidentes de segurança.

5.2. Serão registrados os seguintes dados:

I - Identificação de usuário de quem efetuou o acesso;

II - Data e hora de entrada e saída do sistema;

III - Origem do acesso;

IV - Erros ou falhas de conexão e acesso;

V - Troca de senhas de Serviços de Infraestrutura de TI;

VI - Outras informações que venham a ser necessárias para os controles de segurança.

Art. 6º. No prazo de 5 dias úteis a contar da publicação deste Ato será publicado na intranet texto compilado da Portaria 4772/08, com as alterações introduzidas por esta Portaria.

Art. 7º. A presente Portaria entra em vigor a partir da data de sua publicação.

Maria Helena Mallmann,
Presidente do TRT da 4ª Região