PORTARIA Nº 7.628, DE 21 DE DEZEMBRO DE 2016.

Altera a Portaria nº 4.772/2008, a qual institui 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 adequação da periodicidade da revisão das normas, bem como dos processos de trabalho de segurança da informação, em virtude de orientação do Conselho Nacional de Justiça, a partir do levantamento de governança e infraestrutura de TIC do Poder Judiciário – iGovTIC 2016;

CONSIDERANDO a importância de revisão e atualização da Política de Segurança da Informação, instituída pela Portaria n° 4.772/2008 da Presidência deste Tribunal, a fim de adequá-la à realidade da Justiça do Trabalho da 4ª Região e às melhores práticas preconizadas pelos padrões nacionais e internacionais;

CONSIDERANDO o que consta no Processo Administrativo n° 0003728-96.2012.5.04.0000,

RESOLVE:

Art. 1º Alterar os artigos 1º e 11 da Portaria 4.772/2008, que passam a ter 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.
>
> § 1º A Política de Segurança da Informação será revista anualmente, ou quando necessário, em menor prazo.
>
> § 2º 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 Política de Segurança da Informação nos Órgãos e entidades da Administração Pública Federal;

II – Instrução Normativa GSI/PR nº 1, de 13 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 198, de 01 de julho de 2014, 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 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

VII – Norma ABNT NBR ISO/IEC 27001:2013, que normatiza o Sistema de Gestão da Segurança da Informação;

VIII - Norma ABNT NBR ISO/IEC 27002:2013, que normatiza o Código de Prática para Controles da Segurança da Informação;

XI – Código Penal Brasileiro;

XII – Lei 8.112/90, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

Art. 11 - As atribuições do Escritório de Segurança da Informação serão definidas pela norma que regulamenta as atribuições e responsabilidades da Secretaria de Tecnologia da Informação e Comunicações.”

Art. 2º Alterar o item 5.4 do Anexo 1 (NSI001 – Controle de Acesso à Internet) da Portaria 4.772/2008, que passa a vigorar com a seguinte redação:

> "5.4 - Todo tráfego de internet será controlado e inspecionado, de forma automática, pela ferramenta de proxy (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta norma ou definidos pela Administração do Tribunal."

Art. 3º Alterar o Anexo 2 (NSI002 – Do Serviço de Correio Eletrônico Institucional) da Portaria nº 4.772/2008, que passa a vigorar com a seguinte redação:

"**ANEXO 2**

NSI002 – Do Serviço de Correio Eletrônico Institucional

1. Objetivo

Esta norma estabelece regras e padrões para a utilização do serviço de correio eletrônico no âmbito do TRT da 4ª Região.

2. Motivação

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Proteção do ambiente tecnológico do Tribunal.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover e controlar o serviço de correio eletrônico.

3. Conceitos

Para efeitos desta norma são estabelecidos os seguintes conceitos e definições:

3.1. Serviço de correio eletrônico institucional – serviço de envio e recebimento de mensagens eletrônicas (também conhecidas por "*e-mails*") no âmbito do TRT da 4ª Região.

3.2. Caixa postal – conta de correio eletrônico onde são armazenadas as mensagens recebidas e/ou enviadas.

3.2.1. Caixa postal institucional pessoal – conta de correio eletrônico de um único usuário (magistrado, servidor ou estagiário).

3.2.2. Caixa postal institucional da unidade – conta de correio eletrônico de uma unidade administrativa ou judiciária, constante da estrutura organizacional do

Tribunal.

3.2.3. Caixa postal de sistema – conta de correio eletrônico de um sistema informatizado que necessite esse recurso para o seu funcionamento.

3.3. Lista de distribuição – agrupamento de diversos endereços eletrônicos, que permite a distribuição conjunta de uma mensagem eletrônica a todos os seus integrantes, sem caixa postal específica.

3.4. Endereço eletrônico – conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo arroba (@).

3.4.1. Identificador – parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@).

3.4.2. Domínio – parte final do endereço eletrônico, localizada após o símbolo arroba (@).

3.5. Arquivo de registro de mensagens (logs) – compila registros de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas, ou realizar auditorias.

3.6. Usuário de correio eletrônico – magistrado, servidor e estagiário.

3.7. *Spam* – mensagem enviada a um grande número de endereços eletrônicos, que não possua caráter institucional e/ou cujo objeto não seja inerente à atividade funcional do usuário ou da unidade.

3.8. *Phishing* – fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais com o uso de meios técnicos e de engenharia social.

3.9. *Malware* – programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: *worm*, *bot*, *spyware*, *backdoor*, cavalo de tróia e *rootkit).*

3.10. Material criptografado – dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: *token*, *smart card*).

3.11. *Hoax* – mensagem eletrônica encaminhada a muitos destinatários e de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.

4. Referências Normativas

4.1. Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de

Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

4.2. Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15.10.2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

4.3. Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15.07.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

4.4. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

4.5. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

5. Caixas postais de correio eletrônico (criação, alteração e exclusão)

5.1. As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.

5.2. No âmbito deste Tribunal, o domínio do endereço eletrônico é “trt4.jus.br”.

5.3. A capacidade mínima de armazenamento das caixas postais será de 25 gigabytes (GB).

5.4. Somente será criada caixa postal institucional pessoal, caixa postal institucional da unidade ou caixa postal de sistema.

5.5. As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à Secretaria de Tecnologia da Informação e Comunicações.

5.6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido apenas pelo período de três meses, a contar da alteração.

5.7. Caixa Postal Institucional Pessoal

5.7.1. Magistrados e Servidores

5.7.1.1. Todo magistrado e servidor terá uma caixa postal institucional pessoal.

5.7.1.2. A solicitação de caixa postal institucional pessoal para magistrado de primeiro grau incumbe à Secretaria de Apoio aos Magistrados e, para servidor e desembargador (quando for o caso), à Secretaria de Gestão de Pessoas.

5.7.1.3. O identificador do endereço de correio eletrônico será formado pelo primeiro nome e pelo último sobrenome do magistrado ou servidor, separados pelo sinal de ponto.

5.7.1.4. O identificador do endereço de correio eletrônico poderá, em situações excepcionais, a critério da Secretaria de Tecnologia da Informação e Comunicações, ser a primeira letra do nome do usuário, seguida do sobrenome.

5.7.1.5. A adequação dos endereços de correio eletrônico ao padrão ora estabelecido deve ser solicitada pelo próprio interessado.

5.7.1.6. A caixa postal institucional pessoal de magistrados e/ou servidores será excluída definitivamente nos casos de falecimento ou afastamentos em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, ou retorno à origem.

5.7.1.7. Ocorridos os fatos descritos no item anterior, incumbe à Secretaria de Gestão de Pessoas comunicá-los à Secretaria de Tecnologia da Informação e Comunicações, no prazo de 5 dias.

5.7.1.8. Recebida a comunicação de que trata o item anterior, incumbe à Secretaria de Tecnologia da Informação e Comunicações:

a) no prazo de 5 dias, informar ao magistrado e ao servidor a data da exclusão definitiva da respectiva caixa postal;

b) no prazo de 20 dias, excluir definitivamente a caixa postal.

5.7.2. Estagiários

5.7.2.1. O gestor da unidade poderá solicitar, por escrito, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado.

5.7.2.2. O envio de mensagem por estagiário será restrito aos endereços eletrônicos mantidos pelo Tribunal.

5.7.2.3. O identificador do endereço eletrônico do estagiário será formado pela primeira letra do seu nome seguida do último sobrenome, acrescido pela palavra “estagiário”, separados pelo sinal de ponto.

5.7.2.4. O uso do correio eletrônico pelo estagiário será de total responsabilidade do gestor da unidade, a quem incumbirá solicitar, por escrito, a exclusão dessa caixa postal imediatamente após o desligamento do estagiário da respectiva unidade administrativa ou judiciária.

5.8. Caixa Postal Institucional da Unidade

5.8.1. As unidades administrativas e judiciárias previstas na estrutura organizacional do Tribunal poderão ter caixa postal institucional da unidade.

5.8.2. O gestor da unidade será também o gestor da respectiva caixa postal, competindo-lhe:

a) solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade;

b) autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.

5.8.3. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.

5.8.4. As comissões, os grupos de trabalho e outros núcleos formalmente constituídos, ainda que não constantes na estrutura organizacional do Tribunal, poderão, em caráter excepcional, ter caixa postal institucional quando o desempenho das atividades que lhes são afetas necessitar a troca de mensagens eletrônicas com o público externo.

5.8.5. A caixa postal referida no item acima fica a critério da Presidência, a quem compete solicitar a sua criação, indicar o magistrado, o servidor ou a unidade que será responsável pelo respectivo gerenciamento, bem como, se for o caso, estabelecer o período de duração dessa caixa.

5.9. Caixa Postal de Sistema

5.9.1. A caixa postal de sistema será criada quando houver essa necessidade para o funcionamento de um sistema informatizado.

5.9.2. O gestor da unidade responsável pelo desenvolvimento ou manutenção do sistema informatizado será também o gestor da respectiva caixa postal, competindo-lhe:

a) solicitar a criação, alteração e exclusão da caixa postal de sistema;

b) autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.

5.9.3. O identificador do endereço de correio eletrônico será formado pela denominação ou sigla que permita a identificação do respectivo sistema informatizado.

6. Lista de distribuição (criação, alteração e exclusão)

6.1. É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do Tribunal.

6.2. A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina ou pela Presidência.

6.3. A solicitação deve ser encaminhada, por escrito, à Secretaria de Tecnologia da Informação e Comunicações, acompanhada de justificativa e, quando destinada à atividade temporária, do período de sua duração.

6.4. Cada lista de distribuição terá um gestor, a quem incumbe:

a) manter permanentemente atualizado o rol de integrantes da lista de distribuição;

b) solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição;

c) solicitar exclusão da lista de distribuição, quando esta não for mais necessária.

6.5. O identificador do endereço eletrônico será formado pela denominação ou sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos, seguido da palavra “lista”, separados por hífen.

6.6. A lista de distribuição será composta exclusivamente por endereços eletrônicos do Tribunal e será bloqueada para o recebimento de mensagem eletrônica enviada pelo público externo, excepcionando-se, a critério da Presidência, aquelas integradas por representantes externos (ex.: Comitê Gestor Regional do Sistema Processo Judicial Eletrônico da Justiça do Trabalho – PJe-JT e Conselho Consultivo da Escola Judicial).

6.7. A Secretaria de Tecnologia da Informação e Comunicações deve manter, permanentemente, tabela atualizada com as listas de distribuição do Tribunal e seus respectivos gestores.

7. Utilização dos recursos do sistema de correio eletrônico

7.1. O uso do correio eletrônico institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou da unidade, sendo vedado o uso para fins particulares.

7.2. O acesso ao correio eletrônico, a partir de estações de trabalho

fornecidas pelo Tribunal, será feito apenas a partir do navegador de internet.

7.3. É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

7.4. O tamanho máximo da mensagem eletrônica, incluindo os anexos, não pode exceder 20 megabytes (MB).

7.5. O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos somente é permitido em caráter excepcional e por aquelas unidades administrativas autorizadas pela Presidência.

7.6. É de responsabilidade do usuário:

a) utilizar o correio eletrônico institucional de acordo com os preceitos desta Norma;
b) eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;
c) manter apenas o seu acesso à conta institucional pessoal de correio eletrônico, sendo vedada a disponibilização desse acesso a terceiros;
d) informar ao Escritório de Segurança da Informação o recebimento de mensagem que contrarie o disposto no item.

7.7. É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

a) informações privilegiadas, confidenciais e/ou de propriedade do Tribunal para destinatários não autorizados;

b) materiais obscenos, ilegais ou antiéticos;

c) materiais preconceituosos ou discriminatórios;

d) materiais caluniosos ou difamatórios;

e) propaganda com objetivo comercial;

f) listagem com endereços eletrônicos institucionais;

g) *malwares* (item 2.8)*;*

h) material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;

i) material protegido por lei de propriedade intelectual;

j) entretenimentos e “correntes”;

l) assuntos ofensivos;

m) músicas, vídeos ou animações que não sejam de interesse

específico do trabalho;

n) *Spam, phishing e hoax* (itens 2.7, 2.8 e 2.11);

o) materiais criptografados.

8. Monitoramento e Auditoria

8.1. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos, que coloquem em risco a segurança da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio.

8.2. As auditorias ordinárias ou extraordinárias serão coordenadas pelo Escritório de Segurança da Informação (Setic) e os relatórios serão encaminhados ao Comitê de Segurança da Informação.

8.3. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

8.4. A eliminação dos arquivos de registro de mensagens eletrônicas (logs) e de caixas postais será adiada em caso de auditoria, bem como de notificação administrativa ou judicial.

8.5. A Secretaria de Tecnologia da Informação e Comunicações encaminhará, até o dia 5 de dezembro de cada ano, relatório às unidades e aos respectivos gestores, com o rol das listas de distribuição e caixas postais a elas vinculadas, bem como a lista de eventuais caixas postais de estagiários lotados na respectiva unidade.

8.6. Cabe ao gestor conferir os dados do relatório referido no item anterior e, até o dia 15 de dezembro do mesmo ano, fazer os ajustes necessários.

9. Atualização da Norma

9.1. O disposto na presente norma será atualizado sempre que houver alterações significantes na arquitetura e/ou tecnologia referente ao serviço de correio eletrônico, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação."

Art. 4º Alterar o subitem 3.2 do Anexo 3 (NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso) da Portaria nº 4.772/2008, que passa a vigorar com a seguinte redação:

> "3.2. Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15.07.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes

para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta."

Art. 5º Alterar o item 4.3 do Anexo 4 (NSI004 - Procedimentos de backup e recuperação de dados) da Portaria nº 4.772/2008, que passa a vigorar com a seguinte redação:

"4.3. A periodicidade, tempo de retenção, RPO e RTO dos backups observarão as seguintes regras (excetuados os dados do PJe-JT, que possui regramento próprio):"

Tipo de Backup	Arquivos armazenados em diretórios de rede na Capital	Arquivos armazenados em diretórios de rede do interior e dados do inFOR do interior	Dados dos sistemas armazenados no Banco de Dados da Capital (NovaJus4, inFOR Capital, e-Revista e Sistemas Administrativos)	
Backup intradiário	**Dias e horários**	Todos os dias, às 10h, 13h, 15h e 18h.	N/A	Todos os dias, a cada duas horas.
	Retenção	Versões objeto do backup serão retidas por três (3) dias.	N/A	A versão objeto de backup tem retenção de quinze (15) dias.
Backup diário (tipo backup)	**Dias e horários**	Todos os dias, com início às 22h.	Todos os dias, com início às 5h.	Completo, todos os dias.
	Retenção	Quinze (15) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 dias. No caso de arquivos deletados, a última versão será mantida pelo prazo de 60 dias.	Trinta (30) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 dias. No caso de arquivo deletados, a última versão será mantida pelo prazo de 60 dias.	A versão objeto de backup tem retenção de quinze (15) dias.
Backup semanal (tipo archive)	**Dias e horários**	N/A	N/A	N/A
	Retenção	N/A	NA	N/A
Backup mensal (tipo archive)	**Dias e horários**	Terceiro final de semana de cada mês	Último final de semana de cada mês	Primeiro final de semana de cada mês
	Retenção	A versão dos arquivos objeto do backup será retida pelo período de seis (6) meses.	A versão dos arquivos objeto do backup será retida pelo período de seis (6) meses.	A versão objeto de backup será retida pelo período de quinze (15) meses.
Backup anual (tipo	**Dias e horários**	Durante o recesso	Durante o recesso	Durante o recesso

archive)	Retenção	A versão dos arquivos objeto do backup será retida pelo período de cinco (5) anos.	A versão dos arquivos objeto do backup será retida pelo período de seis (6) anos.	A versão objeto do backup será retida pelo período de dez (10) anos.
RPO (tempo máximo de perda dos dados)	10 horas	24 horas	2 horas	
RTO (tempo estimado para a restauração)	Imediato para restaurações pontuais. 30 horas para restauração completa.	2 horas	28 horas	

Art. 6º Alterar o inciso II, do item 2, do Anexo 5 (NSI005 – Comitê de Segurança da Informação) da Portaria nº 4.772/2008, que passa a vigorar com a seguinte redação:

> "II - rever a Política de Segurança da Informação e normas relacionadas e sugerir alterações;"

Art. 7º Alterar o item 4 e subitem 10.6.7 do Anexo 6 (NSI006 - Gestão de Riscos de Tecnologia da Informação e Comunicações), que passam a ter a seguinte redação:

> "4. Referências normativas
>
> 4.1. Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
>
> 4.2. Norma Complementar nº 04/IN01/DSIC/GSIPR (Revisão 01), de 15.02.2013, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal – APF, direta e indireta.
>
> 4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.
>
> 4.4. Norma Técnica ABNT NBR ISO 31000:2009, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.5. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.

4.6. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

4.7. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos."

"10.6.7. Melhoria do processo de GRSI-TRT4 – sempre que identificadas oportunidades de melhoria será encaminhada proposta à Presidência, após parecer do Comitê de Segurança da Informação, propondo sua implementação, executando-se as ações corretivas ou preventivas aprovadas."

Art. 7º Incluir os subitens 10.8 e 10.8.1 e item 11 no Anexo 6 (NSI006 - Gestão de Riscos de Tecnologia da Informação e Comunicações), com a seguinte redação:

"10.8. O desenho do processo de GRSI-TRT4, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como demais documentos relacionados, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

10.8.1. O processo será revisto periodicamente e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior."

"11. Atualização da Norma

11.1 As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação."

Art. 8º Alterar o item 7.8 do Anexo 8 (NSI008 – Gestão de Incidentes de Segurança da Informação), que passa a ter a seguinte redação:

"7.8. O desenho do processo de Gestão de Incidentes de Segurança da Informação, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do processo, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

7.8.1. O processo será revisto periodicamente e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior."

Art. 9º Excluir o item 9 Anexo 8 ((NSI008 – Gestão de Incidentes de Segurança da Informação).

Art 10. Republique-se a Portaria nº 4.772/2008, com as alterações ora efetuadas.

Art. 11. Esta Portaria entra em vigor na data de sua publicação.

BEATRIZ RENCK
Presidente do TRT da 4ª Região/RS