PORTARIA Nº 4.772, DE 23 DE SETEMBRO DE 2008.

(Republicação)

(Texto compilado com as alterações promovidas pelas Portarias nºs 4.145/2016, 2.050/2016, 1.063/2016, 8.736/2015, 7.966/2015, 7.791/2015, 1.409/2015, 7.138/2014, 6.137/2014, 2.937/2014, 8.604/2013 e 8.605/2013)

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 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 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;

CONSIDERANDO o parecer favorável da Comissão de Informática deste Tribunal, no desempenho de suas atribuições regimentais,

RESOLVE:

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 Política 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 8.112/90.

(dispositivo alterado pela Portaria nº 8.604/2013)

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

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

II – Integridade: salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

III – Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

IV – Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infra-estrutura ou sistema de processamento da informação, instalações físicas que os abriguem.

V – Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

VI – Plano de Continuidade da Prestação dos Serviços: 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.

Art. 3º As disposições deste Ato aplicam-se a todos os usuários de recursos de tecnologia da informação do Tribunal Regional do Trabalho da 4ª Região.

Parágrafo único. Os convênios e os contratos firmados pelo Tribunal que envolvam utilização de recursos de tecnologia da informação devem observar as disposições deste Ato.

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

Parágrafo único. Os recursos de tecnologia da informação pertencentes ao Tribunal Regional do Trabalho da 4ª Região, disponíveis para o usuário, serão utilizados em atividades relacionadas às suas funções institucionais.

Art. 5º A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

§ 1º Serão realizadas auditorias ordinárias periódicas, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.

§ 2º As auditorias extraordinárias serão realizadas com o intuito de apurar eventos que deponham contra a segurança e as boas práticas no uso dos recursos de tecnologia da informação.

Art. 6º Toda informação gerada no Tribunal será classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

Parágrafo único. O Tribunal providenciará dispositivos de proteção proporcionais ao grau de confidencialidade e de criticidade da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculada, capazes de assegurar a sua autenticidade, integridade e disponibilidade.

Art. 7º As informações, sistemas e métodos gerados ou criados pelos usuários, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são propriedade do Tribunal e serão utilizadas exclusivamente para fins relacionados às atividades a ele afetas.

Parágrafo único. Quando as informações, sistemas e métodos forem gerados ou criados por terceiros para uso exclusivo do Tribunal, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

Art. 8º É criado o Comitê de Segurança da Informação, composto por sete membros:

I – o Desembargador-Presidente da Comissão de Informática, que o presidirá;
II – um magistrado de 1º Grau, indicado pela Comissão de Informática;
III – o Juiz Auxiliar da Presidência;
IV – o Juiz Auxiliar da Corregedoria Regional;
V – o Diretor-Geral;
VI – o Secretário-Geral Judiciário;
VII – o Diretor da Secretaria de Tecnologia da Informação e Comunicações.
(dispositivo alterado pela Portaria nº 2.937/2014)

Art. 9º As competências do Comitê de Segurança da Informação, seu funcionamento, bem como a designação de seus integrantes são regulados no Anexo 5 desta Portaria. (dispositivo alterado pela Portaria nº 2.937/2014)

Art. 10. O Escritório de Segurança da Informação, vinculado à Secretaria de Tecnologia da Informação e Comunicações, tem por objetivo prover soluções de

segurança que agreguem valor aos serviços prestados pelo Tribunal Regional do Trabalho da 4ª Região, pautadas na conscientização e no comprometimento de seus servidores para a preservação da confidencialidade, da integridade e da disponibilidade das informações, a segurança nas operações e a excelente imagem perante a sociedade. (dispositivo alterado pela Portaria nº 2.937/2014)

Art. 11. Compete ao Escritório de Segurança da Informação:

I – elaborar um Plano Diretor de Segurança da Informação, com base nas definições estratégicas estabelecidas pelo Comitê de Segurança da Informação;

II – a gestão da Política de Segurança da Informação e do Plano de Continuidade do Negócio;

III – fornecer subsídios para as atividades do Comitê de Segurança da Informação;

IV – coordenar as ações do Plano Diretor de Segurança da Informação e dos projetos a ele relacionados;

V – promover palestras e treinamentos para conscientização dos usuários e atualização das ações de segurança;

VI – realizar análises de risco periódicas no que tange à tecnologia, ambientes, processos e pessoas;

VII – manter os registros de monitoramento sobre o uso dos recursos de tecnologia;

VIII – realizar auditorias ordinárias e extraordinárias, com emissão de relatórios sobre o uso dos recursos de tecnologia, apontando, quando existentes, irregularidades e não-conformidades na utilização;

IX – coordenar as ações necessárias na ocorrência de incidentes de segurança da informação;

X – atuar de forma coordenada com outras áreas nos assuntos de Segurança da Informação;

XI – informar ao Comitê de Segurança da Informação:

a) nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de risco;

b) incidentes de segurança tecnológica.

Art. 12. Incumbe à chefia imediata e superior do usuário verificar a observância da Política de Segurança no âmbito de sua unidade, comunicando, de imediato, ao Comitê de Segurança da Informação, as irregularidades constatadas, para as providências cabíveis.

Art. 13. O descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 14. As normas complementares às diretrizes gerais definidas na Política de Segurança da Informação deste Tribunal serão editadas sob a forma de Anexos, que integrarão a presente Portaria. (dispositivo alterado pela Portaria nº 6.137/2014)

Art. 14-A. É criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI, subordinada à Secretaria de Tecnologia da Informação e Comunicações e coordenada pelo Escritório de Segurança da Informação. (dispositivo alterado pela Portaria nº 6.137/2014)

Art. 14-B. As atribuições da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI, sua estrutura, bem como a designação de seus integrantes são regulados no Anexo 7 desta Portaria. (dispositivo alterado pela Portaria nº 6.137/2014)

Art. 15. O presente Ato entra em vigor a partir da data de sua publicação.

Art. 16. Fica revogada a Portaria nº 2.316, de 04.7.2001 (DOE 05.7.2001).

CLEUSA REGINA HALFEN
Presidente do TRT da 4ª Região/RS

ANEXO 1

NSI001 – Controle de Acesso à Internet

(Anexo alterado pela Portaria n° 1.063/2016)

1. **Objetivos**

   1.1. Estabelecer diretrizes e padrões para o acesso à internet no âmbito do TRT da 4ª Região.

2. Motivações

   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 o serviço de acesso à internet.

3. **Referências normativas**

   3.1. 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.

   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.

   3.3. 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.

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

4. **Conceitos e definições**

   4.1. Arquivo de registro de mensagens (*logs*) - registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

   4.2. Código malicioso - termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*.

4.3. *Proxy* - também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede.

4.4. *Proxy* externo - são servidores não administrados pelo TRT4, responsáveis por intermediar o acesso à internet, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o proxy administrado pelo TRT4.

4.5. Sítio - É um conjunto de páginas *web* organizadas a partir de um URL básico, onde fica a página principal, e geralmente são armazenadas numa única pasta ou subpastas relacionadas no mesmo diretório de um servidor.

4.6. Situação de contingência - estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.

5. **Diretrizes**

5.1. O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela Secretaria de Tecnologia da Informação e Comunicações.

5.1.1. É expressamente proibido o uso de proxies externos ou similares.

5.2. O acesso à internet é disponibilizado pelo TRT4 para uso nas atividades relacionadas ao trabalho, observado o disposto nesta norma.

5.3. Constitui acesso indevido à internet qualquer das seguintes ações:

5.3.1. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança da informação, tais como pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software.

5.3.2. Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*), exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Tecnologia da Informação e Comunicações.

5.3.3. Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto as definidas como ferramenta de trabalho.

5.3.4. Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do TRT.

5.3.5. Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

5.4. O acesso à internet será controlado, de forma automática, pela ferramenta de proxy (filtro de conteúdo), configurada de acordo com os termos desta norma.

5.4.1. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, do magistrado ou gestor da unidade à Secretaria de Tecnologia da Informação e Comunicações, que a submeterá,

quando for o caso, ao Comitê de Segurança da Informação, para deliberação.

5.5. Cabe ao gestor da unidade orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de internet, conforme as regras estabelecidas nesta norma, bem como reportar ao Escritório de Segurança da Informação ou Comitê de Segurança da Informação o seu descumprimento.

5.6. A critério da Administração, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

5.6.1. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

5.6.2. Limitação de banda de tráfego de dados.

5.7. As medidas identificadas no item anterior, sempre que implementadas, serão precedidas de comunicação aos usuários interessados.

6. Monitoramento e Auditorias

6.1. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pelo Escritório de Segurança da Informação.

6.2. Em caso de indícios de descumprimento das diretrizes previstas nesta norma, a chefia imediata ou superior solicitará, justificadamente, ao Comitê de Segurança da Informação a realização de auditoria extraordinária.

6.3. Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Escritório de Segurança da Informação serão encaminhados ao Comitê de Segurança da Informação, para os devidos fins.

7. Atualização da Norma

7.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO 2
NSI002 – Do Serviço de Correio Eletrônico Institucional
(Anexo alterado pelas Portarias nº 1.409/2015 e 7.138/2014)

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

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

2.1 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.

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

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

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

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

2.3 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.

2.4 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 (@).

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

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

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

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

2.7 *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.

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

2.9 *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).*

2.10 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*).

2.11 *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.

3. Referências Normativas

3.1 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.

3.2 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.

3.3 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.

3.4 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.

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

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

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

4.2 No âmbito deste Tribunal, o domínio do endereço eletrônico é "trt4.jus.br".

4.3 As caixas postais têm capacidade de armazenamento limitada a 25 gigabytes (GB).

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

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

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

4.7 **Caixa Postal Institucional Pessoal**

4.7.1 Magistrados e Servidores

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

4.7.1.2 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. (alterado pela Portaria nº 1.409/2015)

4.7.1.3 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.

4.7.1.4 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.

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

4.7.1.6 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. (alterado pela Portaria nº 1.409/2015)

4.7.1.7 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. (incluído pela Portaria nº 1.409/2015)

4.7.1.8 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.

(incluído pela Portaria nº 1.409/2015)

4.7.2 Estagiários

4.7.2.1 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.

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

4.7.2.3 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.

4.7.2.4 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.

4.8 **Caixa Postal Institucional da Unidade**

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

4.8.2 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.

4.8.3 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.

4.8.4 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.

4.8.5 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.

4.9 **Caixa Postal de Sistema**

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

4.9.2 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.

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

5. **Lista de distribuição** (criação, alteração e exclusão)

5.1 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.

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

5.3 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.

5.4 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.

5.5 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.

5.6 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).

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

6. **Utilização dos recursos do sistema de correio eletrônico**

6.1 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.

6.2 O acesso ao correio eletrônico, a partir de estações de trabalho fornecidas pelo Tribunal, será feito apenas a partir do navegador de internet.

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

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

6.5 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.

6.6 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.

6.7 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.

7. **Monitoramento e Auditoria**

7.1 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.

7.2 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. (alterado pela Portaria nº 1.409/2015)

7.3 As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação. (alterado pela Portaria nº 1.409/2015)

7.4 (revogado pela Portaria nº 1.409/2015)

7.5 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.

7.6 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.

7.7 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. (alterado pela Portaria nº 1.409/2015)

ANEXO 3

NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso

(Anexo incluído pela Portaria n° 8.604/2013 e alterado pela Portaria n° 1.063/2016)

1. Objetivos

1.1. Estabelecer diretrizes e padrões para a utilização dos recursos de tecnologia da informação e para o controle de acesso, no âmbito do Tribunal Regional do Trabalho da 4ª Região (TRT4).

2. Motivações

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

2.2. Garantia de que os acessos aos recursos tecnológicos sejam feitos de forma segura e controlada.

2.3. Necessidade de um processo sistemático para gerenciar o uso de recursos de tecnologia da informação, visando garantir a segurança e continuidade das atividades deste Tribunal.

3. Referências normativas

3.1. Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 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 a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.2. Norma Complementar 07/IN01/DISC/GSIPR, de 06 de maio de 2010, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.3. Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.4. Norma Complementar 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.5. Norma Complementar 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes relacionadas à Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos órgãos e entidades da Administração Pública Federal.

3.6. 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.

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

4. Conceitos e definições

4.1. Arquivo de registro de mensagens (*logs*) - registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

4.2. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.3. Dispositivo móvel: equipamento portátil dotado de capacidade computacional, que permite conexão à rede cabeada ou à rede sem-fio, podendo acessar recursos de rede e internet. São exemplos: *smartphones*, *notebooks* e *tablets*, dentre outros.

4.4. *Malwares*: 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 troia e *rootkit*).

4.5. Proprietário do ativo de informação: pessoa ou outra entidade que tem a responsabilidade (aprovada pela administração) para qualificar o ciclo de vida de um ativo.

4.6. Rede cabeada: corresponde ao acesso aos recursos tecnológicos e à transmissão de dados através da utilização de meios físicos (ativos de distribuição de dados, cabos e pontos de rede).

4.7. Rede lógica: é a rede de dados utilizada pelo Tribunal, abrangendo serviços e sistemas de tecnologia da informação, rede cabeada, rede sem-fio, ativos de distribuição de dados e equipamentos conectados nessa rede.

4.8. Rede sem-fio: também conhecida como rede *wireless* ou *wi-fi*, corresponde ao acesso aos recursos tecnológicos e à transmissão de dados sem a utilização de meios físicos (cabeamento), através da utilização de pontos de acesso sem-fio.

4.9. Remoção de acesso: processo que tem por finalidade remover/excluir definitivamente ou parcialmente determinado(s) acesso(s).

4.10. Solução baseada em nuvem: modelo computacional que permite acesso por demanda e independente da localização a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

4.11. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do Tribunal Regional do Trabalho da 4ª Região.

5. Uso de Recursos de Tecnologia da Informação

5.1. Diretrizes gerais

5.1.1. O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade das atividades desenvolvidas neste Tribunal.

5.1.2. Os recursos de tecnologia da informação disponibilizados pelo Tribunal Regional do Trabalho da 4ª Região aos usuários serão utilizados em atividades relacionadas às 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) a rede lógica do TRT4 e os respectivos canais e pontos de distribuição;

III) as contas de acesso dos usuários, assim como os certificados digitais;

IV) os sistemas computacionais desenvolvidos com base nos recursos providos pelo TRT4;

V) os sistemas computacionais contratados de terceiros, sob licença ou na forma de *software* livre ou aberto, incluídas as soluções baseadas em nuvem.

5.1.3. O usuário é responsável por:

I) 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;

II) preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

III) preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados;

IV) atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

5.1.4. Os procedimentos de instalação, configuração e manutenção de equipamentos e softwares serão realizados pela Secretaria de Tecnologia da Informação e Comunicações ou por terceiros por ela autorizados, sob a supervisão do gestor da unidade, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade.

5.1.5. Não será fornecido suporte a equipamentos particulares (computadores, *notebooks*, *smartphones* e *tablets*), seja quanto à instalação e configuração

de sistemas ou aplicativos, ainda que disponibilizados pelo TRT4, seja quanto às questões relacionadas à conexão à rede sem-fio.

5.1.6. Os equipamentos servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra *malwares*.

5.2. Da Rede Lógica

5.2.1. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do TRT4 terão seus acessos monitorados por questões de segurança e para fins de auditoria.

5.2.2. A cada ponto de acesso à rede de dados do TRT4 poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da Secretaria de Tecnologia da Informação e Comunicações.

5.2.3. É proibida a conexão de qualquer dispositivo não fornecido pelo TRT4 na rede cabeada do Tribunal, sem a prévia anuência da Secretaria de Tecnologia da Informação e Comunicações.

5.2.3.1. A conexão de qualquer equipamento à rede cabeada do TRT4 será feita pela Secretaria de Tecnologia da Informação e Comunicações, ou por terceiros por ela autorizados.

5.2.4. O Tribunal disponibilizará acesso à rede sem-fio para usuários internos e externos.

5.2.4.1. A conexão, para os usuários internos, será feita por meio da credencial (nome de usuário e senha) utilizada para o acesso à rede, e, para os usuários externos, será feita mediante cadastramento prévio em sistema específico do TRT4.

5.2.4.2. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo TRT4.

5.2.4.3. O acesso à internet por meio das redes sem-fio observará as regras dispostas no Anexo 1 – Controle de Acesso à Internet, da Política de Segurança da Informação.

5.2.4.4. Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à internet via rede sem-fio.

5.2.4.5. Poderão ser bloqueados os acessos à rede sem-fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica.

5.2.5. Cada unidade do TRT4 terá disponível área de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

5.2.5.1. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas nesse item, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

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

a) fotos, músicas e filmes de qualquer formato;

b) programas não homologados ou não licenciados;

c) programas de conteúdo prejudicial à segurança do parque computacional deste Tribunal.

5.3. Nuvem corporativa

5.3.1. Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 5.2.5.2.

5.3.2. Os arquivos armazenados na nuvem corporativa poderão ser compartilhados exclusivamente com outros usuários do TRT4.

5.3.3. É vedado o armazenamento na nuvem corporativa de arquivos para cuja edição o TRT4 disponibilize sistemas próprios, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas.

5.4. Computadores portáteis fornecidos pelo TRT4

5.4.1. O fornecimento de computadores portáteis a magistrados e servidores está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e Recebimento.

5.4.2. Os computadores portáteis possuem instalação padrão desenvolvida pelo TRT4, composta por *softwares* e aplicativos necessários ao desempenho das funções de trabalho, além de *softwares* para proteção, monitoramento e auditoria do equipamento.

5.4.3. Os problemas de *software* serão solucionados pela reinstalação padrão desenvolvida pelo TRT4, que fica desobrigado de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados.

5.4.4. A instalação, manutenção e suporte de qualquer *software*/sistema não fornecido pelo Tribunal, bem como o backup de dados locais, é de exclusiva responsabilidade do usuário.

5.4.5. Em caso de exoneração, dispensa da função, cedência, remoção, aposentadoria ou término das atividades que ensejaram o fornecimento, o

equipamento deve ser devolvido ao TRT, com todos os acessórios que o acompanharam, no prazo de 20 dias.

5.5. Licenças de *software*

5.5.1. As licenças de *softwares*, de qualquer natureza, contratadas ou adquiridas pelo TRT4 são de uso institucional, privativo deste Tribunal.

5.5.2. O Tribunal utilizará, preferencialmente, em suas atividades, *Software* Livre ou de Código Aberto.

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

5.5.3. 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.

5.5.3.1. 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 TRT4.

5.5.3.2. As unidades organizacionais do Tribunal poderão encaminhar à Secretaria de Tecnologia da Informação e Comunicações pedido de homologação de *softwares*, para o 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.

5.6. Serviço de mensagem instantânea

5.6.1. O serviço de mensagem instantânea disponibilizado pelo TRT4 destina-se às comunicações internas.

5.6.1.1. Se necessário à execução das atividades institucionais, poderá ser solicitada à Secretaria de Tecnologia da Informação e Comunicações, com a devida justificativa, a liberação para comunicação externa.

6. Do controle do acesso

6.1. Do gerenciamento de acessos

6.1.1. O acesso à rede, serviços e aos sistemas computacionais disponibilizados pelo TRT4 serão solicitados à Secretaria de Tecnologia da Informação e Comunicações, por meio do sistema de atendimento, em que

definidos os níveis de acesso adequados às atividades desenvolvidas.

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

I) os acessos necessários ao desenvolvimento das atividades dos servidores e estagiários vinculados a sua unidade.

II) a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor ou estagiário da unidade, sempre que necessária sua adequação às atividades desenvolvidas.

III) a remoção dos acessos concedidos ao servidor ou estagiário, imediatamente após o afastamento ou desligamento da unidade.

6.1.2.1. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do servidor/estagiário a informações da unidade.

6.1.3. A Secretaria de Apoio aos Magistrados informará à Secretaria de Tecnologia da Informação e Comunicações da nomeação e posse de novos magistrados, a fim de agilizar o primeiro cadastro, e será a responsável pela administração dos acessos de magistrados no sistema PJe.

6.1.4. A Secretaria de Tecnologia da Informação e Comunicações comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a Política de Segurança da Informação, em formato eletrônico, para a caixa postal institucional pessoal do usuário, para ciência.

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

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

6.1.6. A Secretaria de Gestão de Pessoas comunicará à Secretaria de Tecnologia da Informação e Comunicações os casos de falecimento e os afastamentos em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, retorno à origem, ou término do estágio de estudantes, para remoção dos acessos concedidos aos usuários.

6.1.6.1. Os usuários aposentados, cedidos e removidos para outros órgãos, terão acesso aos serviços administrativos via extranet.

6.1.7. As solicitações de acessos de prestadores de serviço aos recursos tecnológicos do TRT4 terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto para a realização das atividades.

6.1.8. O privilégio de administrador na estação de trabalho é restrito aos técnicos de informática que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

6.1.9. Nos computadores portáteis disponibilizados pelo TRT4, também terão privilégio de administrador os magistrados e servidores destinatários dos equipamentos.

6.2. **Da conta de rede e respectiva senha para utilização**

6.2.1. Para ter acesso aos recursos de tecnologia da informação disponibilizados pelo TRT4 é necessário que o usuário possua uma conta de rede.

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

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

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

6.2.5. Na utilização das credenciais de acesso, 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 de tecnologia da informação a partir de sua conta de acesso:

I) não compartilhar a senha com outras pessoas;

II) não armazenar senhas em local acessível por terceiros;

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 de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão.

6.2.6. 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, no mínimo, três das quatro categorias a seguir:

a) caracteres maiúsculos (A-Z);

b) caracteres minúsculos (a-z);

c) dígitos de base (0 a 9);

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

6.2.6.1. Excetuam-se da regra do item 6.2.7 os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

6.2.7. 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.

6.2.8. A conta do usuário será bloqueada após 10 tentativas consecutivas de acesso não reconhecidas, considerando também as tentativas inválidas de acesso à rede sem-fio.

6.2.9. 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.

7. Registros (*log*) de Eventos

7.1. Serão mantidos, por um período mínimo de três (3) meses, os registros dos acessos dos usuários aos recursos tecnológicos disponibilizados pelo TRT4, inclusive para fins de apuração e comprovação de incidentes de segurança.

7.2. 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.

8. Atualização da Norma

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de uso de recursos de tecnologia da informação e de controle de acesso, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO 4
NSI004 – Procedimentos de backup e recuperação de dados
(Anexo alterado pelas Portarias nº 7.138/2014 e n° 4.145/2016)

1. Objetivo

Normatizar e dar publicidade aos procedimentos de backup, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicações.

2. Conceitos e definições

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

2.1 Backup tipo "*archive*" – é o utilizado pelos backups mensais e anuais, tem retenção maior, mas só contém a versão do arquivo no momento do *archive.*

2.2 Backup tipo "backup" – é o ordinário, utilizado nos backups diários, com retenção menor, mas que contém versões diárias dos arquivos (possibilita o backup de várias versões e a navegação por estas versões).

2.3 Backup completo – são transmitidos todos os arquivos existentes no momento do backup.

2.4 Backup incremental – somente os arquivos novos ou modificados desde o último backup são transmitidos.

2.5 RPO (*recovery-point objective*) – o quanto é necessário voltar no tempo para encontrar um backup dos dados, ou seja, o tempo máximo de perda de dados.

2.6 RTO (*recovery-time objective*) – tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente.

2.7 Tivoli Storage Manager (TSM) Server – é o equipamento servidor de backup, que gerencia todos os backups realizados.

2.8 Versão ativa – é a última versão do arquivo no backup.

2.9 Versão de arquivos – no TSM, sempre que um arquivo for criado/alterado/apagado, é criada uma nova versão deste arquivo no backup.

2.10 Versão(ões) inativa(s) – versão(ões) anterior(es) à última versão do arquivo no backup.

3. Referências Normativas

3.1 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.

3.2 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.

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

4. Procedimentos de backup

4.1 Os procedimentos de backup realizados pela SETIC serão executados de forma automática e abrangem os dados gravados nos diretórios de rede privativos de cada unidade judiciária e administrativa do Tribunal e nos sistemas computacionais disponibilizados pelo TRT.

4.1.1 O backup dos dados das unidades do interior do Estado será realizado a partir do repositório centralizado em Porto Alegre, após a sincronização dos equipamentos-servidores de cada Foro, realizada ao final de cada dia.

4.1.2 Os dados armazenados em discos rígidos locais não serão copiados e não será garantida sua recuperação em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional instalado na máquina.

4.2 Os dados objeto de backup serão armazenados, ao final do processo, em dois locais: uma cópia no conjunto de fitas primárias, disponíveis para restaurações, e a outra cópia no conjunto de fitas secundárias, armazenadas no cofre.

4.3 A periodicidade, o tempo de retenção, o RPO e o RTO dos backups observarão as seguintes regras (excetuados os dados do PJe-JT, que possui regramento próprio): (alterado pela Portaria n° 4.145/2016)

				Arquivos armazenados em diretórios de rede na Capital
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 arquivos deletados, a última versão será mantida pelo prazo de 60 dias.	A versão objeto de backup tem retenção de quinze (15) dias.
Backup semanal	**Dias e horários**	N/A	N/A	N/A

				Arquivos armazenados em diretórios de rede na Capital
(tipo archive)	**Retenção**	N/A	N/A	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 archive)	**Dias e horários**	Durante o recesso	Durante o recesso	Durante o recesso
	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

4.4 A periodicidade, o tempo de retenção, o RPO e o RTO dos backups dos dados relativos ao PJe-JT observarão as seguintes regras:

		RQUIVOS DE CONFIGURAÇÃO DO APACHE (Interno e Externo)	**ARQUIVOS DE CONFIGURAÇÃO DO JBOSS**	**BANCO DE DADOS POSTGRES**
Backup diário	Dias e horários	Incremental, de segunda a sexta-feira, com início às 21h.	Incremental, de segunda a sexta-feira, com início às 21h.	Completo, todos os dias.
	Retenção	A versão objeto do backup será retida pelo período de trinta (30) dias.	A versão objeto do backup será retida pelo período de trinta (30) dias.	A versão objeto do backup será retida pelo período de quinze (15) dias.
Backup mensal (tipo archive)	Dia	Segundo domingo do mês	Segundo domingo do mês	Segundo domingo do mês
	Retenção	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano
Backup anual (tipo archive)	Dia	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.

		RQUIVOS DE CONFIGURAÇÃO DO APACHE (Interno e Externo)	ARQUIVOS DE CONFIGURAÇÃO DO JBOSS	BANCO DE DADOS POSTGRES
	Retenção	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.
RPO (tempo máximo de perda dos dados)		24 horas	24 horas	02 horas
RTO (tempo estimado para a restauração)		1 hora	4 horas	19 horas

4.5 No caso de serviços armazenados em nuvem (e-mail), a responsabilidade pelo backup será da prestadora de serviços, assegurado um prazo de retenção de, no mínimo, 30 dias.

5. Recuperação de dados

A recuperação de dados e arquivos, sempre que não puder ser realizada pelo próprio usuário, será solicitada à Secretaria de Tecnologia da Informação e Comunicações, por meio da Seção de Atendimento ao Usuário.

6. Testes de recuperação de dados

6.1 Periodicamente serão realizados testes de recuperação de dados.

6.2 Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, na periodicidade e forma estabelecidas no quadro que segue:

Grupo de backup	Equipes responsáveis pela recuperação	Periodicidade	Recuperação	Equipe responsável pela validação	Validação
Arquivos armazenados em diretórios de rede na Capital	SST/SGBD	Mensal	Restaurar versão do dia anterior de alguns arquivos do volume lógico (drive) sendo testado.	SST	Por amostragem, verificar a integridade de alguns arquivos recuperados.

Grupo de backup	Equipes responsáveis pela recuperação	Periodicidade	Recuperação	Equipe responsável pela validação	Validação
Arquivos armazenados em diretórios de rede do interior	SRT/SGBD	Mensal	Restaurar a versão mais recente de alguns arquivos de uma localidade do interior. Alternar localidade a cada teste.	SRT	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Dados do inFOR do interior	SGBD	Semestral	Restaurar versão do dia anterior da base de dados do inFOR de uma das localidades do interior. Alternar localidade a cada teste.	CDS	Testar, por amostragem, o funcionamento adequado do sistema em relação a determinado processo em uma unidade do interior.
Dados dos sistemas armazenados no Banco de Dados da Capital	SGBD	Bimestral	Restaurar versão do dia anterior de uma das tablespaces da base de produção, alternando a cada teste o sistema (inFOR, NovaJus4, Folha, RH, PJ4, System) envolvido.	CDS	Testar, por amostragem, o funcionamento adequado do sistema cujas tablespaces foram recuperadas. Testar inFOR, NovaJus4 e ADMEletrônico em relação a determinado processo. Testar sistemas RH e Folha em relação a determinado servidor.

Grupo de backup	Equipes responsáveis pela recuperação	Periodicidade	Recuperação	Equipe responsável pela validação	Validação
PJe	SGDB	Mensal	Restaurar para base de BUGFIX e para a base de testes (TST) ou de Treinamento (TRN) do PJe a base de produção.	SGBD/ Equipe de apoio do PJe	Testar a integridade dos dados e funcionamento da base restaurada, mediante sua utilização para homologação de novas versões do PJe.

6.3 Os resultados dos testes serão validados, de forma documentada, pelas equipes identificadas no quadro anterior.

6.4 Se restaurações de dados forem realizadas em períodos iguais ou menores que os definidos para os testes, a equipe responsável pela execução dos testes poderá, a partir dos resultados obtidos, considerar que tais ações têm validade como teste naquele período.

7. Revisão e atualização das normas

7.1 As normas previstas no presente anexo serão atualizadas sempre que alterados os procedimentos de backup.

7.2 A revisão das normas observará a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO 5
NSI005 – Comitê de Segurança da Informação
(Anexo incluído pela Portaria nº 2.937/2014 e alterado pela Portaria n° 8.736/2015)

1. Integrantes do Comitê

Observado o disposto no art. 8º da Portaria nº 4.772/2008, o Comitê de Segurança da Informação será composto pelos seguintes integrantes:

– JOÃO PEDRO SILVESTRIN, Desembargador-Presidente da Comissão de Informática;
– RODRIGO DE ALMEIDA TONON, magistrado de 1º Grau, indicado pela Comissão de Informática;
– ANDREA SAINT PASTOUS NOCCHI, Juiz Auxiliar da Presidência;
– CLOCEMAR LEMES SILVA, Juiz Auxiliar da Corregedoria Regional;
– BÁRBARA BURGARDT CASALETTI, Diretora-Geral;
– ONÉLIO LUIS SOARES DOS SANTOS, Secretário-Geral Judiciário;
– NATACHA MORAES DE OLIVEIRA, Diretora da Secretaria de Tecnologia da Informação e Comunicações.

2. Competências do Comitê

Compete ao Comitê de Segurança da Informação:

I – elaborar e submeter à Presidência do Tribunal, ouvida a Comissão de Informática, propostas de normas e políticas de uso dos recursos de informação, tais como:

a) classificação das informações;
b) gerenciamento de identidade e controle de acesso lógico;
c) controle de acesso físico;
d) controle de acesso à *internet*;
e) utilização do correio eletrônico;
f) utilização de equipamentos de tecnologia da informação;
g) utilização de programas e aplicativos;
h) utilização de armazenamento lógico;
i) contingência e continuidade do negócio.

II – rever a Política de Segurança da Informação e normas relacionadas, no período máximo de dois anos, e sugerir alterações;

III – estabelecer diretrizes e definições estratégicas para a elaboração do Plano Diretor de Segurança da Informação;

IV – dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação e em normas relacionadas;

V – propor e acompanhar planos de ação para aplicação da Política de Segurança da Informação, assim como campanhas de conscientização dos usuários;

VI – receber comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal, instruí-las com os elementos necessários à sua análise e apresentar parecer ao órgão ou autoridade competente a apreciá-las;

VII – solicitar ao Escritório de Segurança da Informação, quando necessário, a realização de auditorias extraordinárias, relativamente ao uso dos recursos de tecnologia da informação no âmbito do Tribunal;

VIII – avaliar relatórios e resultados de auditorias apresentados pelo Escritório de Segurança da Informação;

IX – apresentar à Presidência do Tribunal os resultados da Política de Segurança da Informação;

X – elaborar relatório anual de suas atividades, a ser encaminhado no último trimestre de cada ano à Presidência do Tribunal.

3. Funcionamento do Comitê

3.1 Nos impedimentos ou afastamentos do Presidente da Comissão de Informática, o Comitê de Segurança da Informação será presidido pelo Juiz Auxiliar da Presidência.

3.2 O *quorum* para funcionamento e deliberação do Comitê de Segurança da Informação é de três magistrados e dois servidores.

3.3 As deliberações do Comitê de Segurança da Informação poderão ser feitas em reunião ou por meio eletrônico, a critério do Presidente do Comitê.

3.4 Compete ao Presidente do Comitê convocar seus integrantes para participarem de reunião.

3.4.1 Poderão ser convidados para as reuniões magistrados e/ou servidores não integrantes do Comitê, para esclarecimentos porventura necessários.

3.4.2 A pauta da reunião e os respectivos documentos serão previamente encaminhados aos integrantes do Comitê e aos demais convidados para a reunião.

3.4.3 A reunião será registrada em ata, a qual deve ser aprovada e assinada por todos os integrantes do Comitê presentes na reunião, em expediente administrativo eletrônico classificado como sigiloso.

3.5 As deliberações do Comitê de Segurança da Informação por meio eletrônico devem ser registradas e mantidas, em caráter permanente, pelo Escritório de Segurança da Informação.

ANEXO 6
NSI006 – Gestão de Riscos de Tecnologia da Informação e Comunicações
(Anexo incluído pela Portaria nº 6.137/2014)

8. Objetivos

Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações (TIC), e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TRT da 4ª Região (GRSIC-TRT4).

9. Aplicabilidade

Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TRT da 4ª Região.

10. Motivações
- 10.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.
- 10.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.
- 10.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

11. Referências normativas
- 11.1. Decreto nº 3.505/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- 11.2. Resolução CNJ nº 90/2009, que dispõe sobre os requisitos de nivelamento de Tecnologia da Informação no âmbito do Poder Judiciário.
- 11.3. 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.
- 11.4. 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.
- 11.5. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.
- 11.6. Norma Técnica ABNT NBR ISO 31000:2009, que fornece princípios e diretrizes genéricas para a gestão de riscos.
- 11.7. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.
- 11.8. 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.

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

12. Conceitos e definições

12.1. **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;

12.2. **Análise de riscos** – uso sistemático de informações para identificar fontes e estimar o risco;

12.3. **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos;

12.4. **Ativos de Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

12.5. **Avaliação de riscos** – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

12.6. **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas;

12.7. **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

12.8. **Evitar risco** – forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

12.9. **Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC–TRT4)** – conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

12.10. **Gestão de Riscos em Projetos de TIC** – conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

12.11. **Gestão de Riscos em Processos de TIC** – conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

12.12. **Identificação de riscos** – processo para localizar, listar e caracterizar elementos do risco.

12.13. **Reduzir risco** – forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

12.14. **Reter risco** – forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

12.15. **Riscos de Segurança da Informação e Comunicações** – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais

ameaças, com impacto negativo no negócio da organização;

12.16. **Transferir risco** – uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

12.17. **Tratamento dos riscos** – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

12.18. **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

13. Escopo

A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação, bem como dos projetos e processos relacionados à área de TIC, que suportam os principais processos de negócio do TRT da 4ª Região.

14. Diretrizes

14.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação deste Tribunal.

14.2. A Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

14.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e são tratados de forma a assegurar respostas tempestivas e efetivas.

15. Gestão de riscos em projetos de TIC

15.1. A gestão e comunicação de riscos em projetos de TIC são definidas na metodologia de gerenciamento de projetos adotada e têm como objetivo aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

15.2. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada.

15.3. A gestão de riscos em projetos é monitorada pelo Escritório de Projetos da Secretaria de Tecnologia da Informação e Comunicações.

16. Gestão de riscos em processos de TIC

16.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

16.2. As atividades inerentes à gestão de riscos nos processos de TIC (por exemplo: contratação, desenvolvimento, etc.) devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.

16.3. A gestão de riscos em processos de TIC é monitorada pela Seção de Governança de TIC.

17. Gestão de riscos em Segurança da Informação e Comunicações (GRSIC-TRT4)

17.1. O processo de GRSIC-TRT4 é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação e da Gestão de Continuidade de Negócios.

17.2. O processo de GRSIC-TRT4 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011 e ABNT NBR ISO/IEC 31000:2009 e na Norma Complementar nº 04/IN01/DSIC/GSIPR.

17.3. Os critérios para avaliação do risco levam em consideração o "PSR": a) **Probabilidade**, que é a possibilidade de uma vulnerabilidade ser explorada, ocasionando um incidente de segurança; b) **Severidade**, que é a consequência para o ativo de informação caso um incidente ocorra; e c) **Relevância**, que é a importância do ativo de informação para os processos de negócio aos quais ele está relacionado. Considera-se como **Impacto**, o produto da Severidade e da Relevância. Desta forma, a avaliação de riscos é realizada através do produto de três variáveis (probabilidade, severidade e relevância). A partir do valor obtido, o risco é classificado de acordo com a tabela a seguir:

Classificação do Risco	Valores do "PSR"
Muito baixo	1 a 6
Baixo	8 a 16
Médio	18 a 30
Alto	32 a 50
Muito alto	60 a 125

17.4. Os riscos classificados como "Baixo" ou "Muito Baixo" são aceitos pela Presidência do TRT da 4ª Região (conforme item 10.7.2).

17.4.1. A aceitação do risco, neste caso, não significa negligenciá-lo, mas reconhecer sua existência e acompanhá-lo, de forma a evitar ser surpreendido por sua concretização.

17.4.2. Os demais riscos serão tratados de acordo com as necessidades levantadas pelas partes interessadas, pelas regulamentações e legislações vigentes e pela análise custo/benefício.

17.5. Considerando as políticas praticadas pelo TRT da 4ª Região, não há riscos passíveis de serem tratados através da estratégia de transferência de riscos.

17.6. O processo de GRSIC-TRT4 é composto pelas etapas descritas a seguir:

17.6.1. Definições preliminares – compreende a definição do escopo da avaliação de riscos a ser executada e a identificação das partes interessadas, considerando os critérios para classificação e aceitação de riscos definidos nos itens 10.3 e 10.4, respectivamente.

17.6.1.1. O escopo pode abranger o Tribunal como um todo, um segmento, um processo, um sistema, um recurso ou um ativo

de informação.

17.6.1.2. O escopo é definido considerando-se prioritariamente os principais serviços que suportam os processos de negócio do TRT da 4ª Região.

17.6.2. Análise/Avaliação dos riscos – compreende:

17.6.2.1. Mapeamento dos ativos de informação no âmbito do escopo definido;

17.6.2.2. Identificação dos riscos: identificação de ameaças, vulnerabilidades e dos controles de SIC já existentes, relacionados aos ativos mapeados;

17.6.2.3. Análise dos riscos: informar valores para probabilidade, severidade e relevância de cada risco para o escopo analisado;

17.6.2.4. Avaliação dos riscos: determinar, considerando os itens 10.3 e 10.4, se os riscos são aceitáveis ou se requerem tratamento, comparando-se a estimativa de riscos com os critérios estabelecidos na fase anterior; e

17.6.2.5. Relação dos riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na fase anterior.

17.6.3. Plano de Tratamento de Riscos – compreende a elaboração de plano visando à definição das formas de tratamento dos riscos, de implantação de controles e dos responsáveis por sua implementação, considerando as restrições organizacionais, estruturais, tecnológicas e técnicas, os requisitos normativos e/ou legais, os controles de SIC existentes e implementados e a análise custo/benefício.

17.6.3.1. Para cada risco levantado, deve ser definida a estratégia de tratamento: mitigar (reduzir), evitar ou reter.

17.6.3.2. Para cada tratamento, devem ser definidas as tarefas a serem realizadas, o responsável pela execução do tratamento e o prazo de execução;

17.6.3.3. Considerando a definição da estratégia de tratamento e do(s) controle(s) a ser(em) implementado(s), deve ser informado, para cada risco levantado, o risco residual.

17.6.4. Aceitação de riscos – nesta fase, são verificados os resultados do processo executado, considerando o Plano de Tratamento de Riscos aprovado, e os riscos residuais, aceitando-os formalmente ou submetendo-os a nova avaliação.

17.6.5. Implementação do Plano de Tratamento de Riscos: após a aceitação dos riscos, as ações de SIC contidas no Plano aprovado devem ser executadas e implantadas.

17.6.6. Monitoramento e análise crítica: esta fase tem por objetivo monitorar os riscos levantados e detectar possíveis falhas nos resultados, nos controles implementados e na eficácia da GRSIC-TRT4.

17.6.6.1. Monitoramento dos riscos: os riscos devem ser regularmente monitorados e analisados criticamente, a fim de verificar mudanças relativas aos critérios de avaliação e de aceitação dos riscos, aos processos/fluxos suportados pela área de TIC, aos ativos de informação, às ações de segurança da informação e aos fatores do risco (ameça, vulnerabilidade, probabilidade e impacto);

17.6.6.2. Monitoramento do processo de GRSIC-TRT4: o processo deve ser monitorado e analisado criticamente, com o objetivo de mantê-lo alinhado às normas relacionadas à matéria e às necessidades do TRT da 4ª Região.

17.6.7. Melhoria do processo de GRSI-TRT4 – a cada dois anos ou sempre que necessário, o processo deverá ser revisto, e, se for o caso, encaminhada proposta à Presidência, após parecer do Comitê de Segurança da Informação, a fim de implementar eventuais melhorias identificadas, executando-se as ações corretivas ou preventivas aprovadas, assegurando que as melhorias atinjam os objetivos pretendidos.

17.6.8. Comunicação do Risco: as unidades da Secretaria de Tecnologia da Informação e Comunicações, o Comitê de Segurança e a Presidência devem ser consultados ou informados nas diversas fases da gestão de riscos.

17.7. Responsabilidades da GRSIC-TRT4

17.7.1. O Escritório de Segurança da Informação, em conjunto com a Diretoria da Secretaria de Tecnologia da Informação e Comunicações, é responsável por gerenciar e coordenar as atividades inerentes ao processo de GRSIC no âmbito do TRT da 4ª Região especificadas no item 10.6.

17.7.2. Cabe à Presidência do TRT da 4ª Região, após manifestação do Comitê de Segurança da Informação, aprovar formalmente os seguintes documentos: definições preliminares da análise de GRSIC-TRT4 (subitem 10.6.1), o documento de aceitação de riscos (subitem 10.6.4) e o relatório de melhorias a serem implantadas/executadas (subitem 10.6.7).

ANEXO 7
NSI007 – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI

(Anexo incluído pela Portaria nº 6.137/2014)

1. Missão

Apoiar as atividades de tratamento e resposta a incidentes em redes computacionais, a fim de contribuir para a garantia da disponibilidade e da segurança na prestação de serviços do Tribunal.

2. Referências Normativas

2.1 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.

2.2 Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2.3 Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2.4 Portaria nº 4.772/2008, da Presidência do TRT da 4ª Região, que institui a Política de Segurança da Informação no âmbito deste Tribunal.

3. Público-alvo

O público-alvo da ETRI é formado por todos os usuários da rede de computadores e sistemas deste Tribunal.

A ETRI relaciona-se, internamente, com as diversas unidades da Secretaria de Tecnologia da Informação e Comunicações e com o Comitê de Segurança da Informação.

Externamente, a ETRI se relaciona com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – Cert.br e outros órgãos do Poder Judiciário Federal.

4. Modelo de Implementação

A ETRI será composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e à resposta a incidentes em redes computacionais.

5. Estrutura Organizacional e Composição

A ETRI é subordinada à Secretaria de Tecnologia da Informação e Comunicações e é coordenada pelo Escritório de Segurança da Informação.

A ETRI é composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, sendo: um administrador de redes, um administrador de banco de dados, um analista de suporte (atendimento) e um analista de sistemas.
Para cada uma das posições será designado um suplente.

Caso necessário, poderão ser convocados servidores de outras áreas do Tribunal (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades.

6. Integrantes

A ETRI é composta pelos seguintes integrantes:
Membros Titulares:
– ANDRÉ SOARES FARIAS, analista de sistemas;
– FELIPE BOHM DA CUNHA, administrador de redes;
– ERIC GUATIMOZIN SILVA, administrador de banco de dados;
– DENILSON RIBEIRO DE QUADROS, analista de suporte (atendimento).
Membros Suplentes:
– FÁBIO DE OLIVEIRA GARCIA, suplente do analista de sistemas;
– ANDRÉ LUIZ LIVI, suplente do administrador de redes;
– EVANDRO BASSANESI, suplente do administrador de banco de dados;
– DIEGO FRAGA CONTESSA, suplente do analista de suporte (atendimento).

7. Autonomia

A autonomia da ETRI é compartilhada. A equipe recomendará, no mínimo, aos Coordenadores das áreas técnicas envolvidas, à Diretoria da Secretaria de Tecnologia da Informação e Comunicações e ao Escritório de Segurança da Informação, os procedimentos a serem executados ou as medidas de recuperação durante um ataque e apresentará as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas). De acordo com a gravidade do incidente, a proposição deverá, ainda, ser submetida à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

8. Atribuições

São atribuições da ETRI:

I – opinar sobre assuntos relacionados a tratamento e resposta a incidentes em redes computacionais;

II – propor as metodologias e os 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.

ANEXO 8
NSI008 – Gestão de Incidentes de Segurança da Informação
(Anexo incluído pela Portaria nº 7.791/2015)

1. Objetivos

Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito deste Tribunal.

2. Motivações

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

2.2. Necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade.

2.4. Formalização de um processo sistemático para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos futuros.

3. Referências normativas

3.1. 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 a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.4. 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.

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

4. Conceitos e definições

4.1. **Artefato malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. **Ativos de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3. **Usuários:** magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

4.4. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI:** Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

4.5. **Evento de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

4.6. **Incidente de segurança da informação:** é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

4.7. **Medida de contenção:** controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o reestabelecimento do sistema/serviço afetado, mesmo eu não seja em sua capacidade total.

4.8. **Medida de solução:** controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação.

4.9. **Tratamento de Incidentes de Segurança em Redes Computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4.10. **Vulnerabilidade**: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5. Escopo

A Gestão de Incidentes de Segurança da Informação, definida nesta norma, tem

seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC, que suportam os principais processos de negócio do TRT da 4ª Região.

6. Diretrizes

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes em segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

6.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRT, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação deste Tribunal, e dos quais decorram interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

6.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

7. O processo de Gestão de Incidentes de Segurança da Informação

7.1. O processo de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI).

7.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

7.2.1. Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação.

7.2.2. Investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação ações de contenção, quando necessárias.

7.2.3. Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

7.2.4. Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

7.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7.3.1. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através do formulário de solicitação de atendimento da Central de Serviços ou diretamente ao Escritório de Segurança da Informação, pelo telefone ou pelo e-mail setic.esi@trt4.jus.br, que os reportarão à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

7.3.1.1. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (observada ou suspeita).

7.3.1.2. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou recursos tecnológicos.

7.3.2. As equipes da Secretaria de Tecnologia da Informação responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, para o devido registro e encaminhamento.

7.3.3. O Tribunal poderá receber notificações externas (CTIR.BR, CSIRT ou outras empresas) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, etc, que deverão ser remetidas ao Escritório de Segurança da Informação, para o devido encaminhamento.

7.4. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

7.4.1. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais deve, em conjunto com as outras áreas da Setic, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenções, comunicando as áreas afetadas e coletando os dados necessários.

7.4.2. A coleta de evidências dos incidentes de segurança da informação deve ser realizada por pessoal competente e autorizado designado pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ou por ela própria.

7.4.3. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

7.5. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e a Administração do TRT deverão ser comunicados, para avaliação das providências cabíveis.

7.6. O encerramento do incidente de segurança da informação será realizado pelo Escritório de Segurança da Informação, com comunicação a todas as áreas interessadas, bem como ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR), na forma e nos casos definidos pelo referido órgão.

7.7. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

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 encontram-se ao final deste Anexo e dele fazem parte integrante.

8. Atualização da Norma

As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada a

periodicidade prevista para a revisão da Política de Segurança da Informação.

9. Apêndices

9.1. Detalhamento dos Papéis e Responsabilidades dos envolvidos no Processo de Gestão de Incidentes de Segurança da Informação:

Papéis	
Escritório de Segurança da Informação (ESI)	Seção responsável pela área de segurança de TIC e que coordena a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI).
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	Equipe responsável pelas atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.
Comitê de Segurança da Informação	Comitê multidisciplinar responsável pela coordenação das ações e deliberações relacionadas à área de segurança da TIC.
Outras áreas da SETIC	Compreendem a Diretoria da SETIC, suas Coordenadorias e Seções. Atuam em conjunto na análise e resolução dos incidentes em redes quando acionados pela ETRI.
Presidência	Órgão diretivo do TRT a quem compete deliberar sobre as ações de contenção nos casos de incidentes graves.

Responsabilidades	
Escritório de Segurança da Informação (ESI)	Coordenar o cumprimento e evolução da maturidade do processo de Gestão de Incidentes de Segurança em Redes do Tribunal.
	Assessorar o Comitê de Segurança da Informação e a SETIC na análise e tomada de decisões a respeito de situações resultantes de incidentes de segurança da informação.
	Realizar a comunicação com o CTIR.BR.
	Coordenar as atividades da ETRI do Tribunal.
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	Monitorar o ambiente e recursos de TIC do TRT a fim de perceber quaisquer alteração negativa.
	Realizar a investigação do incidente de segurança da informação, de forma a propor medidas de contenção dos danos causados pelo incidente.
	Reestabelecer a operação normal do ambiente e/ou recurso de TIC após a ocorrência de um incidente de segurança da informação.
	Realizar a análise do incidente de segurança da informação, de forma a propor medidas para eliminar ou solucionar problemas que causaram o incidente de segurança da informação.
Comitê de Segurança da Informação	Analisar e deliberar sobre ações a serem realizadas para o tratamento de incidentes de segurança da informação.
Outras áreas da SETIC	Auxiliar a ETRI na proposição e execução de medidas para contenção e solução de incidentes de segurança da informação.

9.2. Detalhamento das Atividades previstas no Processo de Gestão de Incidentes de Segurança da Informação:

1. Registrar Incidente de Segurança		
Descrição	Comunicada a ocorrência ou suspeita de incidente, registrar de forma detalhada em formulário próprio no Google Drive – RISI, categorizando o incidente de segurança dentre os tipos constantes do formulário. Verificar a necessidade de autorização prévia do Comitê de Segurança de Informação para prosseguimento.	
	Atividade predecessora: não há	Atividades sucessoras: 2. Encaminhar pedido de autorização 3. Investigar o incidente
Considerações Importantes	Para o registro do incidente pode ser necessário o contato com o usuário ou equipe que o informou para esclarecimentos que permitam o registro e trâmite do incidente. Além disso, de acordo com o tipo de incidente pode ser necessária a autorização prévia do Comitê de Segurança da Informação para a realização dos procedimentos necessários à investigação.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	Comunicação de suspeita ou ocorrência de incidente de Segurança da Informação	
Saídas	Formulário RISI preenchido com informações iniciais	
Atividades	1.1 Receber a comunicação sobre o incidente	Receber e-mail, via encaminhamento do formulário de solicitação de atendimento da Central de Serviços, via formulário de registro de demanda da área técnica ou pelo envio de alertas emitidos pelos sistemas de monitoramento ou por qualquer outro meio a notificação de que ocorreu incidente de segurança ou que há suspeita de sua ocorrência.
	1.2 Solicitar esclarecimentos ao informante, quando necessário	Entrar em contato com o informante para obter informações necessárias ao registro e posterior encaminhamento das providências.
	1.3 Registrar o incidente	Preencher o Formulário RISI no Google Drive, descrevendo e categorizando o incidente.
	1.4 Verificar necessidade de autorização prévia do Comitê de Segurança da Informação	Após categorizar o incidente, verificar a necessidade de autorização do Comitê de Segurança da Informação para o prosseguimento. Em geral, são submetidas à prévia autorização do Comitê a emissão de relatórios de acesso de determinado servidor em sistemas e serviços disponibilizados, investigações de acessos não autorizados ou que exijam a verificação de dados dos usuários.
	1.5 Encaminhar para o Escritório de Segurança da Informação	Se necessária autorização do Comitê, encaminhar ao Escritório de Segurança da Informação para solicitar a autorização.
	1.6 Encaminhar incidente para investigação	Após autorização do Comitê ou quando desnecessária autorização, encaminhar o incidente para investigação pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI). Este encaminhamento poderá ser direcionado a apenas um dos integrantes da equipe, quando se trate de ação específica para cuja realização o integrante esteja habilitado.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

2. Encaminhar pedido de autorização

Descrição	Ao Escritório de Segurança da Informação incumbe solicitar autorização ao Comitê para o prosseguimento da investigação nos casos em que há necessidade de emissão de relatórios de acesso de determinado(s) servidor(es) em sistemas e serviços disponibilizados, investigação de acessos não autorizados ou que exijam a verificação de dados dos usuários.	
	Atividade predecessora: 1. Registrar o incidente de segurança	Atividades sucessoras: 3. Investigar o incidente 9. Cumprir providências/encerrar o incidente
Considerações Importantes	O funcionamento do Comitê de Segurança da Informação está regrado no Anexo 5 da Política de Segurança da Informação. Aspectos importantes: O quórum mínimo para deliberação no Comitê é de três magistrados e dois servidores. Nas ausências do Presidente do Comitê quem o substitui é o Juiz Auxiliar da Presidência. As deliberações podem ser feitas por meio eletrônico (e-mail).	
Papéis	Escritório de Segurança da Informação	
Entradas	Formulário RISI – com registro de incidente que necessita de relatórios de acesso de determinado servidor	
Saídas	Pedido de autorização ao Comitê de Segurança da Informação (por e-mail)	
Atividades	2.1. Coletar as informações necessárias ao encaminhamento do pedido de autorização para prosseguimento da investigação	Ao encaminhar o pedido de autorização para prosseguimento da investigação, o Escritório de Segurança da Informação deve fornecer ao Comitê de Segurança da Informação o máximo de informações possíveis que propiciem a deliberação de forma rápida.
	2.2. Encaminhar pedido de autorização ao Comitê	O pedido de autorização pode ser encaminhado via e-mail ou submetido para deliberação em reunião do Comitê de Segurança da Informação.
	2.3. Prestar os esclarecimentos, quando necessário	O Comitê de Segurança da Informação poderá solicitar esclarecimentos antes da autorização. Neste caso, o Escritório de Segurança da Informação é o responsável por coletar as informações e encaminhá-las ao Comitê.
	2.4. Encaminhar para investigação	Se autorizado, o Escritório de Segurança da Informação deve dar prosseguimento à investigação junto à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI).
	2.5 Encaminhar para finalização	Nos casos em que não houver autorização pelo Comitê de Segurança da Informação para a realização da investigação solicitada, encaminhar para finalização ou encerramento do incidente.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

3. Investigar o incidente		
Descrição	A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), com base nas informações registradas no RISI, deverá investigar as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento.	
	Atividades predecessoras: 1. Registrar incidente de segurança 2. Encaminhar incidente de segurança	Atividades sucessoras: 4. Propor ações de contenção 5. Comunicar as áreas afetadas 6. Realizar investigação de acessos Estas atividades poderão ocorrer de forma concomitante ou não.

Considerações Importantes	Para esta atividade a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) poderá solicitar informações às áreas técnicas responsáveis, a fim de elucidar a extensão e o impacto do problema, quais ativos e sistemas estão sendo afetados e começar a definir uma ação para conter o incidente. A identificação do tipo e impacto do incidente é muito importante nesta etapa, pois ela definirá o encaminhamento a ser dado quanto à necessidade de ações de contenção, de comunicação a outras áreas sobre a ocorrência do incidente e de realização de investigação de acessos.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	Autorização do Comitê de Segurança da Informação ou Formulário RISI preenchido com as informações iniciais	
Saídas	Formulário RISI preenchido com as informações do incidente investigado	
Atividades	3.1 Verificar o tipo de incidente	Verificar se é uma investigação de acesso indevido, descumprimento da Política de Segurança da Informação, indisponibilidade de um serviço ou sistema por falha de segurança, invasão, propagação de vírus, vazamento de dados etc.
	3.2 Analisar a extensão e o impacto causado pelo incidente	Analisar quais serviços, sistemas e ativos foram afetados e qual foi o dano causado pelo impacto. Se necessário, envolver outras equipes.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

4. Propor ações de contenção		
Descrição	Com base nas informações levantadas na investigação do incidente, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá propor ações para conter o incidente, que podem ser soluções de contorno ou de resolução do problema.	
	Atividades predecessoras: 3. Investigar o incidente 7. Aplicar medidas aprovadas	Atividade sucessora: 7. Aplicar medidas aprovadas
Considerações Importantes	Dependendo do tipo de incidente e de sua extensão, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) poderá envolver outras áreas da Setic para definir as ações de contenção. Dependendo da ação que for definida e da gravidade do incidente, poderá ser necessária a aprovação da chefia de uma ou mais áreas envolvidas ou mesmo da Presidência do Tribunal. Se as medidas não forem autorizadas, novas medidas deverão ser propostas. Assim também se o incidente não for contido, novas medidas deverão ser propostas.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI preenchido com as informações sobre o incidente/ ou não aprovação das medidas anteriores/ ou informação de que as medidas não foram suficientes a conter o incidente	
Saídas	RISI preenchido com as ações de contenção propostas	
Atividades	4.1 Propor ações de contenção	A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá propor ações que contenham o incidente, de forma a evitar que os danos e impactos aumentem com o passar do tempo. Além disso, a ação de contenção deve reestabelecer o sistema ou serviço, ainda que parcialmente, via solução de contorno ou resolução da causa do incidente.
	4.2 Encaminhar solução para aprovação das chefias	Dependendo do teor da ação proposta, será necessária a aprovação da chefia das áreas afetadas e/ou envolvidas no incidente e na sua resolução.

	4.3. Proposição de novas medidas, caso o incidente não seja contido	Se o incidente não for contido pelas medidas inicialmente propostas, novas medidas deverão ser estudadas e aplicadas.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

5. Comunicar as áreas afetadas		
Descrição	Se o incidente de segurança afetar um ou mais grupos de serviço/sistemas ou usuários (por exemplo, investigação de acesso por descumprimento da Política de Segurança da Informação), a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), de posse da extensão e do impacto do incidente, deverá comunicar as áreas da Setic sobre a ocorrência e, em conjunto com o Escritório de Segurança da Informação, deliberar se é necessário informar outras áreas do TRT sobre o incidente.	
	Atividade predecessora: 3. Investigar o incidente	Atividade sucessora: 4. Propor ações de contenção
Considerações Importantes	É de suma importância informar outras áreas da Setic para que estas possam agir para ajudar na proposição de medidas para conter e/ou resolver o incidente. Além disso, a área de Atendimento aos Usuários deve ser informada principalmente quando o incidente afetar sistemas e serviços utilizados diretamente pelos usuários, de forma a repassar orientações e informações sobre o incidente e seu tratamento, prazo de retorno do serviço, etc. Se necessário, uma comunicação ostensiva pode ser divulgada, informando que a Setic está ciente do problema e está trabalhando para resolvê-lo, estimando o tempo para tratá-lo.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI preenchido com as informações sobre o incidente investigado	
Saídas	Pedido à Direção da Setic para comunicar áreas afetadas (se externo à Setic) ou comunicação interna, com as informações necessárias + RISI preenchido com as informações sobre o plano de comunicações.	
Atividades	5.1. Informar a extensão do impacto e quais sistemas/ serviços foram afetados	De posse dessas informações, será possível avaliar a quem e como a comunicação será realizada, bem como o teor da mensagem.
	5.2. Definir como e a quem a comunicação será realizada	Definir, em conjunto com o Escritório de Segurança da Informação, como a mensagem será divulgada, a quem será divulgada e o que ela conterá.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

6. Coletar dados (relatório de acessos)		
Descrição	Se o incidente disser respeito à investigação sobre acessos de determinado(s) servidor(es) em sistemas e serviços disponibilizados, investigação de acessos não autorizados ou que exijam a verificação de dados dos usuários, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) realizará a auditoria necessária e compilará os dados em relatório a ser encaminhado ao Comitê de Segurança da Informação.	
	Atividade predecessora: 3. Investigar o incidente	Atividade sucessora: 8. Analisar incidente
Considerações Importantes	Nestes casos a documentação gerada deverá ser armazenada em local de acesso restrito (os relatórios não deverão ser inseridos no sistema utilizado para o registro dos incidentes e demandas em geral).	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI + Autorização do Comitê de Segurança da Informação	
Saídas	Relatório de acessos	
Atividades	6.1. Identificação dos dados necessários à elucidação do incidente	De acordo com as informações recebidas os dados podem ser coletados de sistemas de monitoramento diversos. Assim é importante que sejam identificados quais os dados que melhor podem elucidar a questão noticiada.
	6.2. Realizar a coleta e compilação de dados	Realizar a coleta e a compilação de dados necessários à elaboração de relatório ao Comitê de Segurança da Informação. Estes dados deverão ser armazenados em local de acesso restrito ao Escritório de Segurança da Informação ou ao Comitê.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação.	

7. Aplicar medidas aprovadas		
Descrição	Executar as ações propostas na fase anterior, visando conter o incidente, e verificar se o resultado esperado foi alcançado.	
	Atividade predecessora: 4. Propor ações de contenção (caso as medidas aplicadas não tenham sido suficientes a conter o incidente de forma adequada).	Atividade sucessora: 8. Analisar incidente
Considerações Importantes	Após aplicar as medidas, a equipe deverá avaliar se o incidente foi contido e, em caso negativo, deverá propor/realizar novas ações que contenham o incidente.	
Papéis	Outras áreas da Setic e Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI com autorização da aplicação da medida de contenção proposta	
Saídas	RISI com resultados das medidas aplicadas	
Atividades	7.1 Aplicar as medidas necessárias	Realizar as configurações e/ou modificações necessárias para conter o incidente.
	7.2 Avaliar medidas aplicadas	Verificar se medidas aplicadas obtiveram o resultado esperado e, em caso negativo, propor novas medidas de contenção.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

8. Analisar incidente		
Descrição	Esta atividade tem por objetivo analisar o incidente como um todo (causa raiz identificada, ações de contenção aplicadas, resultados dos relatórios elaborados etc), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução). Se for o caso de uma investigação (suspeita de violação da Política de Segurança da Informação), a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá elaborar relatórios de acesso com base na análise de ferramentas e logs disponíveis a fim de elucidar a suspeita, apresentando suas conclusões ao Comitê de Segurança da Informação.	
	Atividades predecessoras: 6. Coletar dados (relatórios de acesso) 7. Aplicar medidas aprovadas	Atividades sucessoras: 9. Analisar proposições ESI 10. Cumprir providências/encerrar o incidente
Considerações Importantes	O estudo poderá ser realizado em conjunto com outras áreas dependendo do tipo de incidente. De acordo com o teor da proposição, poderá ser necessário o encaminhamento para deliberação por parte do Comitê de Segurança da Informação ou comunicação a outras áreas (internas e externas).	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI preenchido com todas as informações	
Saídas	Solicitação de manifestação do Comitê de Segurança da Informação // Proposição de ações à Direção da Setic.	
Atividades	8.1 Analisar causa-raiz do incidente	Analisar o cenário do incidente, identificando a causa-raiz, quais as vulnerabilidades exploradas, quais as ameaças envolvidas, etc;
	8.2 Propor melhorias no cenário investigado	De posse da análise realizada, propor ações de melhoria para o cenário analisado, de forma a evitar (ou diminuir o risco de) que o incidente volte a ocorrer.
	8.3 Redigir relatório	No caso de ser uma investigação de acessos, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá analisar logs e utilizar as ferramentas de auditoria disponíveis para elucidar a suspeita informada no RISI e encaminhar o relatório à apreciação do Comitê de Segurança da Informação.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

9. Analisar proposições ETRI		
Descrição	Avaliar as soluções propostas ou analisar o relatório de auditoria enviado pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), deliberando a respeito ou simplesmente tomando ciência acerca do incidente, quando for o caso.	
	Atividade predecessora: 8. Analisar incidente	Atividade sucessora: 10. Cumprir providências/encerrar o incidente

Considerações Importantes	Nos casos de auditoria de logs de determinado usuário, o Comitê de Segurança da Informação analisará o teor do relatório e deliberará sobre o encaminhamento assunto do qual o mesmo trata. Outras questões também podem ser submetidas ao Comitê, considerando o impacto e abrangência do incidente.	
Papéis	Comitê de Segurança da Informação	
Entradas	Proposição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Saídas	Deliberação do Comitê de Segurança da Informação	
Atividades	9.1. Tomar ciência do incidente e medidas aplicadas	Tomar ciência do incidente e das medidas aplicadas.
	9.2 Avaliar soluções propostas	Ao Comitê de Segurança da Informação cabe deliberar sobre a proposição de novas ações pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), sempre que necessária sua intervenção.
	9.3. Analisar relatório de investigação/auditoria	Analisar o relatório e deliberar sobre o encaminhamento a ser dado.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

10. Cumprir providências/encerrar o incidente		
Descrição	O Escritório de Segurança da Informação deverá encaminhar para a equipe responsável as ações de melhorias levantadas e aprovadas, de forma a contribuir para que o problema seja resolvido. Além disso, caso haja alguma ação a ser tomada, informada pelo Comitê de Segurança da Informação na fase anterior, o Escritório de Segurança da Informação deverá executar durante esta fase. Depois, o incidente de segurança da informação será considerado como encerrado.	
	Atividades predecessoras: 8. Analisar incidente 9. Analisar proposições ESI	Atividade sucessora: 11. Analisar e consolidar informações (alimentar indicadores)
Papéis	Escritório de Segurança da Informação	
Entradas	Deliberação do comitê // RISI com providências	
Saídas	RISI preenchido e encerrado // Notificação ao CTIR.BR	
Atividades	10.1 Cumprir providências	O Escritório de Segurança da Informação deverá dar prosseguimento nas deliberações e ações definidas pelo Comitê de Segurança da Informação ou pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)
	10.2 Encerrar o incidente	Nesta fase, o incidente deve ser encerrado, uma vez que ele foi analisado e tratado corretamente.
	10.3 Notificar o incidente ao CTIR.BR	O incidente deverá ser informado ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR.BR (ver documento NOTIFICAÇÃO CTIR-Procedimentos)
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

11. Avaliar histórico de incidentes e consolidar informações (alimentar indicadores)	
Descrição	Analisar o tipo e histórico de incidentes, com o intuito de estudar o cenário "macro", de forma a perceber alguma oportunidade de melhoria no processo de gestão de riscos, bem como sistema ou serviço afetado por um ou mais incidentes.

	Atividade predecessora: 10. Cumprir providências/encerrar o incidente	Atividade sucessora: 12. Verificar oportunidades de melhoria e lições aprendidas
Considerações Importantes	É importante que os RISIs sejam preenchidos de forma completa e precisa, pois serão utilizados para alimentar os indicadores do processo de gestão de riscos.	
Papéis	Escritório de Segurança da Informação	
Entradas	RISI encerrado	
Saídas	Registro de indicadores	
Atividades	11.1 Avaliar histórico de incidentes	Verificar os RISIs anteriores e outras bases (TraceGP, por exemplo) a fim de fazer alguma correlação de incidentes e verificar possíveis *gaps* em algum processo, sistema ou infraestrutura.
	11.2 Alimentar indicadores estabelecidos	Atualizar as informações dos indicadores definidos para o processo.

12. Verificar oportunidades de melhoria e lições aprendidas		
Descrição	Com base na análise e consolidação de informações dos indicadores, deve-se buscar *gaps* no processo de gestão de incidentes e serviços/sistemas afetados pelos incidentes, para então sugerir melhoria nos mesmos.	
	Atividade predecessora: 11. Avaliar histórico de incidentes e consolidar informações	Atividade sucessora: Não há
Papéis	Escritório de Segurança da Informação	
Entradas	Registro de indicadores	
Saídas	Relatório de melhorias	
Atividades	12.1 Analisar indicadores	Com base nos indicadores e avaliação junto às outras áreas, o Escritório de Segurança da Informação deve avaliar se o processo está eficaz.
	12.2 Propor melhorias no processo	De acordo com a avaliação do processo e análise dos indicadores, o Escritório de Segurança da Informação deverá propor melhorias para tornar o processo mais eficaz e objetivo.

9.3. Modelos de Documentos a serem utilizados nas atividades previstas no Processo de Gestão de Incidentes de Segurança da Informação:

9.3.1. RISI – Relatório de Incidentes de Segurança da Informação

RISI – Relatório de Incidente de Segurança da Informação	
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – Tribunal Regional do Trabalho da 4ª Região	
1 – Informações do RISI	
Descrição do Incidente:	Data e Hora de abertura:

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

	Data e Hora de fechamento:

Severidade do Incidente:
☐ Alta
☐ Média
☐ Baixa

2 – Identificador do Incidente

Origem da Identificação: ☐ Interna ☐ Externa
Nome Completo:
Área/Seção:
Telefone:
E-mail:
Empresa: N/A

3 – Detalhamento do Incidente

Tipo de Incidente	Descrição detalhada do incidente de Segurança
Não conformidade com a PSI ☐ Utilização da Internet ☐ Utilização do e-mail ☐ Utilização de Recurso Computacional	
Indisponibilidade de Serviço ou Sistema ☐ Rede ☐ E-mail ☐ Internet ☐ PJe-JT ☐ ADMEletrônico ☐ inFOR ☐ Link de dados ☐ Outros _____	
☐ **Ataque de força bruta a um sistema/página web**	
☐ **Alteração de sistema não planejada**	
☐ **Infecção por *malware***	
***Defacement* (alteração não autorizada de portal)** ☐ Internet ☐ Intranet ☐ Extranet	
DoS (Negação de Serviço) ☐ Portal de Internet ☐ Link de dados ☐ Sistemas	
☐ **Outros** Informar:	

Tipo de Impacto do Incidente	Grau de Impacto
☐ Confidencialidade	☐ Baixo ☐ Médio ☐ Alto
☐ Integridade	☐ Baixo ☐ Médio ☐ Alto

☐ Disponibilidade	☐ Baixo ☐ Médio ☐ Alto

4 – Investigação do Incidente

Equipe responsável pela investigação:	**Descrição detalhada da Investigação (causa raiz, o que ocasionou o incidente, etc.)**
Data de Entrega do Plano de Investigação:	

5 – Ação de Contenção

Equipe responsável pela execução da ação:	**Descrição da Ação de Contenção:**
Outras áreas envolvidas:	
Data e hora de proposição da ação:	
Data e hora de execução da ação proposta:	
Responsável(is) pela aprovação:	

6 – Comunicação a partes interessadas

Informar a quem o incidente foi comunicado	Data e hora da comunicação	Pessoa comunicada	Meio de comunicação
☐ SETIC			
☐ ESI			
☐ CPP			
☐ CDS			
☐ CIT			
☐ CAU			
☐ Partes interessadas ou afetadas. Informar:			
☐ Outros. Informar:			

7 – Análise e Encerramento do RISI

Outras ações necessárias? ☐ Sim ☐ Não	**Descrição Detalhada da(s) ação(ões) proposta(s)**
Responsável pela ação:	
Data de Proposição da Ação:	

9.3.2. Registro de Indicadores:

Registro de Indicadores		
Indicadores	**Ano 1**	**Ano 2**
Quantidade de incidentes registrados		
Quantidade de incidentes resolvidos		
Quantidade de incidentes em andamento		
Quantidade de incidentes registrados – por nível de severidade (alta, média e baixa)		
Quantidade de incidentes registrados – por categoria (não conformidade com a PSI, indisponibilidade de serviço/sistema, ataque de força bruta, infecção por *malware*, alteração não-autorizada de portal, negação de serviço)		

9.3.3. Notificação CTIR.BR – Procedimentos

NOTIFICAÇÃO CTIR.BR – PROCEDIMENTOS

1. A comunicação entre órgãos e instituições da APF e o CTIR Gov deve ocorrer por meio das ETIR, de forma centralizada, preferencialmente por meio de e-mail institucional relacionado a incidentes de segurança. No caso do TRT4 será utilizado o e-mail do Escritório de Segurança da Informação (posteriormente, poderá ser implementada nova conta específica abuse@orgao.gov.br, como sugerido nos padrões do CTIR).

2. O ponto único de contato para as notificações de incidentes de segurança ao CTIR Gov é o endereço eletrônico: ctir@ctir.gov.br.

1. Para comunicação através de um canal seguro, deverá ser utilizada a seguinte chave PGP:
PGP Key ID: 0xAFBEDFCF
Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF
2. O CTIR Gov atende ainda pelo telefone INOC-DBA: 10954*810.

3. As questões gerenciais ou relacionadas à Coordenação-Geral de Tratamento de Incidentes de Rede (CGTIR) serão tratadas por meio do correio eletrônico: cgtir@planalto.gov.br.

4. A notificação deverá conter os seguintes dados:

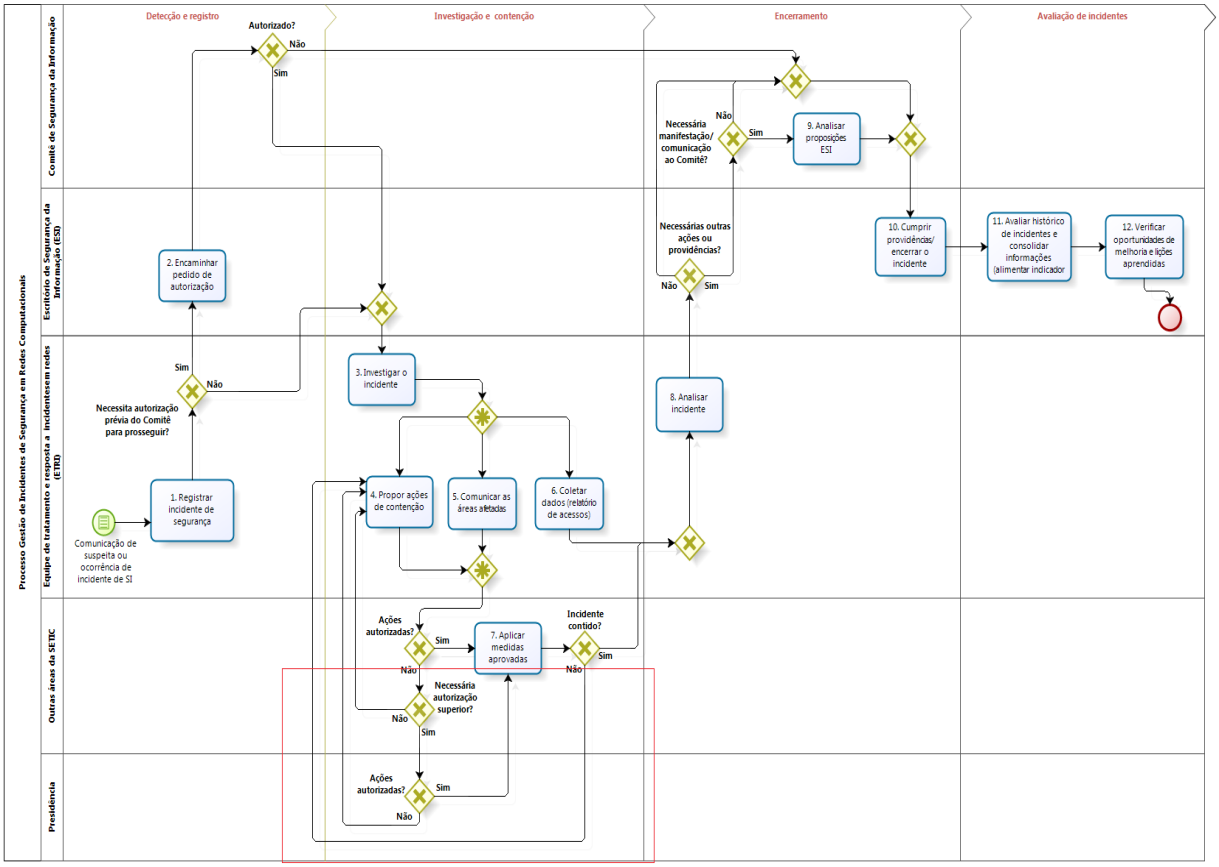
1. Assunto: fazer constar o "*nome do órgão*" e o "*tipo do incidente*".
2. Destinatário: ctir@ctir.gov.br.
3. CC: eventualmente, podem ser copiados outros envolvidos no incidente.
4. Corpo da Notificação: descrever sucintamente o incidente ocorrido, atentando para a correção das informações, tais como: organizações, pessoas ou serviços de rede envolvidos; time zone; registros de log; cronologia dos acontecimentos; ações adotadas; outros detalhes técnicos e incidentes correlacionados.
5. Anexos: Deverão ser anexadas as informações que facilitem a análise e a resposta ao incidente, tais como: logs de servidores e/ou serviços, cabeçalho de mensagens, código malicioso, etc.

5. No caso de recebimento de uma notificação ou resposta do CTIR, nas Comunicações que se seguirem deve sempre ser referenciado no campo "*Assunto*" o número de identificação fornecido no formato [CTIR Gov BR #XXXXX].

6. Principais tipos de incidentes de segurança possíveis de serem notificados:

1. abuso de sítios (desfiguração, injeção de links/código – *spamdexing*, erros de código, *cross site scripting*, abuso de fórum ou livros de visita, etc.);
2. inclusão remota de arquivos (*remote file inclusion* – RFI) em servidores web;
3. uso abusivo de servidores de e-mail;
4. hospedagem ou redirecionamento de artefatos ou código malicioso;
5. ataques de negação de serviço;
6. uso ou acesso não autorizado a sistemas ou dados;
7. varredura de portas;
8. comprometimento de computadores ou redes;
9. desrespeito à política de segurança ou uso inadequado dos recursos de Tecnologia;
10. ataques de engenharia social – *phishing*; (no caso de *phishing* recebido por e-mail, solicita-se que, além do texto da mensagem, sejam enviados os cabeçalhos completos para que se proceda, dentre outras coisas, à notificação do servidor de e-mail comprometido);
11. cópia e distribuição não autorizada de material protegido por direitos autorais;
12. uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

9.4. Desenho do Processo de Gestão de Incidentes de Segurança da Informação:



PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS
TRT DA 4ª REGIÃO

Powered by bizagi Modeler

ANEXO 9
NSI009 – Classificação da Informação
(Anexo incluído pela Portaria nº 7.966/2015)

1. Objetivos

Definir as diretrizes básicas e a classificação das informações do Tribunal Regional do Trabalho da 4ª Região, doravante denominado "*instituição*", com a finalidade de manter a proteção adequada à informação.

2. Abrangência

Esta norma se aplica a todas as informações do Tribunal Regional do Trabalho da 4ª Região independente do recurso usado para seu suporte.

3. Conceitos e Definições

3.1. **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto.

3.2. **Segurança da informação**: proteção da informação contra ameaças para garantir a continuidade do negócio, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio.

3.3 **Confidencialidade**: princípio de segurança da informação que garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para tal.

3.4. **Rótulo**: identificação física ou eletrônica da classificação atribuída à informação.

3.5. **Ciclo de vida da informação**: compreende etapas e eventos de produção, recebimento ou alteração, acesso, armazenamento, divulgação, transferência física ou em redes eletrônicas, cópia, impressão ou qualquer outra forma de reprodução, destruição e descarte.

3.6. **Proprietário da informação**: aquele que produz a informação ou a recebe em nome da instituição.

3.7. **Criptografia:** técnica de transformar uma informação legível em informação incompreensível por meio de procedimentos matemáticos.

4. Princípios e Diretrizes

4.1. É assegurado o direito de acesso pleno a documentos públicos, observado o disposto na legislação em vigor, em especial a Lei nº 12.527/2011.

4.2. A informação será usada apenas para os propósitos de interesse da instituição.

4.3. Cada usuário restringir-se-á apenas às informações e aos recursos de informação aos quais está autorizado.

4.4. As informações serão protegidas de acordo com o grau de confidencialidade estabelecido.

4.5. Toda informação possui um proprietário que é responsável por sua classificação no momento em que deu origem a ela.

4.6. A classificação inicial poderá ser revista, devendo ser identificado o momento em que tal ocorreu, bem como a autoridade que procedeu à reclassificação.

4.7. A classificação de uma informação deve ser preservada durante todo o seu ciclo de vida.

4.8. A classificação das informações deve observar as exigências e a finalidade das atividades da instituição e as implicações que trará para todos os seus usuários.

4.9. Na classificação das informações evitar-se-á o exagero, com a adoção, sempre que possível, de classificação de menor grau de restrição.

5. Classificação e Tratamento das informações

5.1. Uma informação é classificada de acordo com a sua exigência de confidencialidade como: secreta, restrita, interna e pública.

5.2. Informação Secreta

5.2.1. É toda informação imprescindível à segurança da sociedade e do Estado, bem como dos órgãos e instituições que o integram, e cuja divulgação ou acesso irrestrito possam, na forma prevista pelo art. 23 da Lei nº 11.527/2011:

a) pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

b) prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

c) pôr em risco a vida, a segurança ou a saúde da população;

d) oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

e) prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;

f) prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;

g) pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

h) comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

5.2.2. As informações secretas são restritas aos membros da Administração e magistrados e servidores previamente designados que, pela natureza da atividade que exercem, sejam obrigados a conhecê-las.

5.2.3. Toda informação secreta será controlada quanto a sua divulgação, mantidos registros históricos com a identificação inequívoca dos usuários que tiveram acesso a ela.

5.2.4. As cópias de documentos secretos serão pré-aprovadas, controladas e possuirão identificação única.

5.2.5. Toda informação secreta será guardada em local com acesso controlado, e medidas de segurança serão adotadas para sua guarda e seu transporte, que deverá ser expressamente autorizado quando for para fora da instituição.

5.2.6. Quando as informações secretas forem armazenadas eletronicamente, a Secretaria de Tecnologia da Informação e Comunicações será informada, a fim de verificar a segurança das condições de armazenamento.

5.2.7. O encaminhamento ou transporte em meio físico de informações secretas deverá ocorrer sempre por meio de mensageiro e sua entrega ao destinatário deve ser de forma pessoal; deverão estar acondicionadas em 2 (dois) envelopes de cor opaca, onde o envelope interno conterá a etiqueta de classificação apropriada e o externo não conterá qualquer indicação sobre a classificação da informação, apenas o destinatário, devidamente identificado.

5.2.8. É vedada a transmissão eletrônica de informações secretas, exceto se utilizada criptografia.

5.2.9. O prazo máximo de restrição de acesso da informação classificada como secreta é de quinze (15) anos, a contar de sua produção ou recepção (art. 24, § 1º, da Lei nº 12.527/2011).

5.3. Informação Restrita

5.3.1. É toda informação cujo conhecimento deve ficar limitado a um número reduzido de pessoas autorizadas e que, caso revelada a pessoas não autorizadas, pode acarretar dano à sociedade, pessoas físicas ou jurídicas, bem como comprometer serviços ou frustrar objetivos específicos da instituição.

5.3.2. Incluem-se nesta classificação os processos que tramitam em segredo de justiça, informações sobre sistemas informatizados, banco de dados e infraestrutura da instituição, cuja divulgação possa comprometer o adequado funcionamento dos serviços, credenciais de acesso a sistemas e banco de dados, bem como os expedientes e documentos anteriormente identificados como reservados ou confidenciais.

5.3.3. O acesso às informações restritas é limitado às autoridades envolvidas e servidores previamente designados que, pela natureza da função que exercem, sejam obrigados a conhecê-las.

5.3.4. A divulgação interna de uma informação restrita para autoridades e servidores que não pertencem à mesma função de quem a recebeu, bem como as cópias de documentos reservados, serão pré-aprovadas e devidamente registradas.

5.3.5. Toda informação restrita será guardada em local com acesso controlado, e medidas de segurança serão adotadas para o seu transporte, que deverá ser autorizado quando for para fora da instituição.

5.3.6. Sendo necessária a utilização de serviços de correio ou mensageiro interno, as informações restritas deverão estar acondicionadas em 2 (dois) envelopes de cor opaca, onde o envelope interno conterá a etiqueta de classificação apropriada e o externo não conterá qualquer indicação sobre a classificação da informação, apenas o destinatário, devidamente identificado.

5.3.7. A transmissão eletrônica de informações restritas deverá identificar obrigatoriamente os destinatários.

5.3.8. O prazo máximo de restrição de acesso da informação classificada como restrita é de cinco anos (5) anos, a contar de sua produção ou recepção (art. 24, § 1º, da Lei nº 12.527/2011).

5.4. Informação Interna

5.4.1. É toda informação cujo conhecimento e uso está restrito ao âmbito interno e propósitos da instituição.

5.4.2. Incluem-se nesta categoria as minutas de decisões, despachos, votos, sentenças e papéis de trabalho enquanto não firmados pela autoridade ou servidor responsável.

5.4.3. As informações internas só poderão ser reveladas ao público externo mediante autorização.

5.4.4. Para a transmissão eletrônica de informações de uso interno deverá haver a identificação dos envolvidos.

5.4.5. O prazo de restrição de acesso da informação classificada como interna se encerra com sua assinatura ou publicização, exceto se classificação mais restritiva for a ela atribuída.

5.5. Informação Pública

5.5.1. É toda informação que pode ou deve ser divulgada para o público externo da instituição.

5.5.2. Incluem-se nesta classificação as informações de caráter informativo ou promocional e aquelas cuja veiculação pública seja obrigatória por força legal ou normativa.

5.5.3. Na transmissão eletrônica ou física de informações públicas não deve sofrer qualquer restrição.

5.6. Informações classificadas como secreta e restrita não podem ser usadas como dados de teste nas atividades de desenvolvimento e manutenção de sistemas de informação sem autorização prévia do proprietário.

5.7. O descarte de informações secretas e restritas deve ser feito de forma que não seja possível recuperá-las.

5.8. Toda informação que não possuir uma classificação explícita quanto a sua confidencialidade e não estiver divulgada nos diversos meios de comunicação utilizados pela instituição será considerada como interna até ser classificada.

5.9. Toda informação classificada deverá ser rotulada, de forma a identificar a classificação realizada.

5.10. A classificação será realizada no momento em que a informação é gerada. Caso o gerador da informação não seja o proprietário, deverá consultar o proprietário a respeito da classificação.

5.11. Somente os membros da Administração da instituição podem classificar uma informação como secreta.

5.12. Somente os membros da Administração da instituição, magistrados e diretores de podem classificar uma informação como restrita.

5.13. Qualquer usuário pode classificar uma informação como interna, desde que restrito a sua área de atuação.

5.14. A reclassificação de uma informação só pode ser feita por quem a classificou originalmente e, na sua ausência, pela autoridade ou servidor que assumiu a sua função ou que possuir nível hierárquico superior ao exigido para a sua classificação.

6. Responsabilidades

6.1 Todos os usuários deverão acessar somente informações e recursos de informação para os quais estejam autorizado.

6.2 Os controles relativos à classificação das informações que lhe forem confiadas deverão ser observados por todos, principalmente no ambiente externo à instituição, com cuidados especiais para o uso de equipamentos portáteis, conversas e leituras de documentos em viagens ou locais públicos.

6.3 Qualquer exposição indevida e/ou riscos às informações classificadas como secreta e interna deverá ser reportada à chefia imediata.

6.4 Os usuários são responsáveis pelos atos praticados por meio de sua credencial de acesso aos recursos da área de tecnologia da informação.

6.5. O acesso à informação classificada como secreta, restrita ou interna cria a obrigação para aquele que a obteve de resguardar o sigilo.

7. Penalidades

O manuseio, divulgação ou uso indevido de informações importa na aplicação de sanções disciplinares, civis e penais previstas em lei.

ANEXO 10
NSI010 – Gestão de Continuidade de TIC

(Anexo incluído pela Portaria n° 2.050/2016)

1. Objetivos

Estabelecer as diretrizes e definir o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, aplicáveis ao ambiente tecnológico deste Tribunal.

2. Motivações

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

2.2 Correto direcionamento e dimensionamento de recursos tecnológicos para prover a Gestão de Continuidade de TIC.

2.3 Aumentar o nível de resiliência dos serviços e sistemas de TIC frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria da prestação jurisdicional.

2.4 Estabelecer procedimentos de gestão para assegurar a continuidade das operações de TIC.

3. Referências normativas

3.1 Norma Complementar nº 06/IN01/DSIC/GSIPR, de 11.11.2009, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.2 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.

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

3.4 Norma Técnica ABNT NBR ISO/IEC 22301:2013, que normatiza o sistema de gestão de continuidade de negócios e especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

4. Conceitos e definições

4.1 Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.

4.2 Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a

prestação jurisdicional do Tribunal, bem como técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

4.3 Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções dos negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

4.4 Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.

4.5 Estratégia de continuidade: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

4.6 Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

4.7 Plano de Continuidade: nome que se dá à documentação que abrange os procedimentos referentes à continuidade dos serviços de TIC e é composta por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.

4.8 Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade.

4.9 Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade.

4.10 Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

4.11 RPO (*Recovery Point Objective*) - Tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.

4.12 RTO (*Recovery Time Objective*) - Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

5. Diretrizes

5.1 A gestão de continuidade de TIC visa a:

5.1.1 Reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas do TRT4.

5.1.2 Manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação jurisdicional do TRT4.

5.1.3 Definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade.

5.2 A gestão de continuidade de TIC deve observar o resultado das análises de riscos de TIC e da análise de impacto de negócio realizadas, de forma a nortear as estratégias de continuidade.

5.3 Será elaborado Plano de Continuidade de TIC, com vistas a documentar os procedimentos necessários à operação em nível de contingência e comunicações necessárias, bem como o retorno à normalidade, quando da ocorrência de interrupções dos serviços e sistemas de TIC.

5.4 Devem ser fornecidos recursos humanos, tecnológicos e financeiros para a manutenção e melhoria contínua da gestão de continuidade de TIC.

6. Processo de Gestão de Continuidade de TIC

6.1 O processo de Gestão de Continuidade de TIC é composto pelas seguintes etapas:

6.1.1 Planejamento - compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades da SETIC são essenciais para prestação jurisdicional, quais deverão ser tratadas na Continuidade de TIC e quais estratégias serão utilizadas durante a ocorrência de um incidente. Compreende também a avaliação da necessidade de revisão dos planos já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças na infraestrutura, procedimentos ou testes realizados.

6.1.2 Execução - abrange a elaboração ou revisão dos planos pelas equipes técnicas, com a descrição dos cenários de falhas e os procedimentos técnicos para lidar com os problemas, a realização de testes (execução parcial ou integral dos procedimentos), a aprovação dos planos, seu armazenamento e divulgação.

6.1.3 Verificação - abrange a realização de testes periódicos dos Planos desenvolvidos e a análise dos incidentes críticos ocorridos (desastres) a fim de subsidiar a etapa de Melhoria.

6.1.4 Melhoria - compreende a identificação das oportunidades de melhoria e seu encaminhamento à consideração superior, com vistas a dar início a novo ciclo do processo.

6.2 O desenho do processo de Gestão de Continuidade de TIC, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos e indicadores definidos para o processo serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

6.2.1 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.

7. Plano de Continuidade de TIC

7.1 O Plano de Continuidade de TIC é composto pelos Planos de Continuidade Operacional e Planos de Recuperação de Desastres.

7.2 O Plano de Continuidade de TIC deve ser periodicamente testado, de forma a garantir sua efetividade.

7.3 O Plano de Continuidade de TIC deve ser revisado no mínimo uma vez por ano ou, ainda, em função dos resultados de testes realizados ou após mudança significativa nos ativos de informação (infraestrutura tecnológica, processo, atividades etc).

7.4 O Plano de Continuidade de TIC será acionado quando verificadas interrupções parciais ou totais que impactem nas atividades críticas do TRT.

7.4.1 Ocorrido o incidente, considerados os serviços, sistemas ou ativos afetados e a criticidade, as equipes técnicas responsáveis acionarão os Planos de Continuidade Operacional para a manutenção da continuidade das atividades, ainda que de forma contingencial, e os Planos de Recuperação de Desastre para retorno das atividades à normalidade.

7.4.2 A comunicação às partes interessadas observará as orientações contidas nos Planos de Continuidade Operacional.

7.4.3 Os ativos e serviços afetados pelo incidente serão monitorados pelas equipes responsáveis, a fim de subsidiar o fornecimento de informações à autoridade superior.

7.4.4 A ativação do Plano de Continuidade de TIC será encerrada quando da comunicação de retorno à normalidade dos serviços, sistemas ou ativos afetados.

8. Atualização da Norma

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