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

PORTARIA Nº 4.772, DE 23 DE SETEMBRO DE 2008.

(Republicação)

(Texto compilado com as alterações promovidas pelas Portarias nº 988/2022, 299/2022 2.926/2021, 4.786/2020, 6.493/2019, 3.241/2019, 230/2019, 1.885/2018, 7.137/2017 7.628/2016, 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.

§ 1º A Política de Segurança da Informação será revista anualmente, ou quando necessário, em menor prazo. (parágrafo incluído pela Portaria nº 7.628/2016)

§ 2º A presente Política de Segurança da Informação tem por fundamento as seguintes referências legais e normativas: (parágrafo alterado pela Portaria nº 299/2022).

I - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação no âmbito da Administração Pública Federal;

II – Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

III – Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

IV - Instrução Normativa GSI/PR nº 5, de 31 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. (dispositivo inserido pela Portaria nº 299/2022)

V - Resolução CNJ nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

VI - Resolução CNJ nº 370 de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

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

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

IX – Código Penal Brasileiro;

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

XI - Decreto nº 10.222, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.

XII - ISO/IEC 27000:2018, que define uma visão geral sobre sistemas de gestão de segurança da informação e de termos e conceitos utilizados.

XIII - Lei nº 13.709/2018, Lei Geral de Proteção de Dados; (dispositivo inserido pela Portaria nº 299/2022)

Art. 2º Para os efeitos deste Ato aplicam-se as seguintes definições: (dispositivo alterado pela Portaria nº 299/2022)

I - Auditoria - processo sistemático, independente e documentado para obter evidências de auditoria e avaliá-las objetivamente para determinar em que medida os critérios de auditoria

são atendidos;

II - Confidencialidade: propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados;

III - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

IV - Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada;

V - Integridade: propriedade de precisão e completude;

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.

VII - Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, instalações físicas que os abriguem.

VIII - Segurança da Informação: conjunto de ações, controles e medidas para assegurar a preservação da confidencialidade, disponibilidade e integridade da informação

IX - 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.

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 Gestor de Segurança da Informação, composto por oito membros: (dispositivo alterado pela Portaria nº 299/2022)

I - Assessor-Jurídico da Presidência do Tribunal;

II - Diretor da Secretaria Administrativa;

III - Secretário-Geral Judiciário;

IV - Assessor Técnico-Operacional da Corregedoria;

V - Diretora da Secretaria de Gestão de Pessoas;

VI - Diretor da Secretaria de Tecnologia da Informação e Comunicações;

VII - Coordenador da Coordenadoria de Segurança Institucional;

VIII - Assistente-chefe do Escritório de Segurança da Informação, que coordenará o grupo;

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.

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. As atribuições do Escritório de Segurança da Informação são definidas pela Portaria nº 7.596/2014 e suas atualizações, que regulamenta as atribuições e responsabilidades da Secretaria de Tecnologia da Informação e Comunicações. (dispositivo alterado pela Portaria nº 4.786/2020)

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. 14-C. O tratamento de dados pessoais no âmbito deste Tribunal é regido pela Política de Proteção e Privacidade de Dados Pessoais do TRT-4. (dispositivo inserido pela Portaria nº 299/2022)

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 pelas Portarias n°s 1.063/2016, 7.628/2016, 7.137/2017, 6.493/2019, 4.786/2020, 2.926/2021 e 299/2022)

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. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal; (item alterado pela Portaria nº 299/2022)

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 - também conhecido por *malware*, 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, *ransomware* e *rootkit*. (item alterado pela Portaria nº 299/2022)

4.3. *Proxy* web - 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. (item alterado pela Portaria nº 299/2022)

4.4. *Proxy web* 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. (item alterado pela Portaria nº 299/2022)

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 no ambiente tecnológico do TRT dar-se-á, exclusivamente, pelos meios autorizados, configurados pela Secretaria de Tecnologia da Informação e Comunicações. (item alterado pela Portaria nº 299/2022)

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

5.2. O acesso à internet nas dependências da Justiça do Trabalho é disponibilizado para uso nas atividades relacionadas ao trabalho, observado o disposto nesta norma. (item alterado pela Portaria nº 299/2022)

5.2.1. Equipamentos do TRT que estão fora das dependências (ex.: teletrabalho, *home-office, etc)* da Justiça do Trabalho poderão ser configurados para utilizar os mecanismos de controle de acesso à internet estabelecidos pela SETIC.

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 tais como: pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software. (item alterado pela Portaria nº 4.786/2020)

5.3.1.1. A restrição de que trata o item 5.3.1 pode ser flexibilizada: por razão de trabalho, desde que, previamente, autorizada pelo Comitê de Segurança da Informação. (item incluído pela Portaria nº 4.786/2020)

5.3.2. Utilizar softwares para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*) e/ou realizar o *download* de softwares e arquivos piratas, exceto programas homologados pelo TRT4 ou autorizados pelo Comitê Gestor de Segurança da Informação. (item alterado pela Portaria nº 299/2022)

5.3.3. Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto programas homologados pelo TRT4 ou autorizados pelo Comitê de Segurança da Informação. (item alterado pela Portaria nº 4.786/2020)

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. Todo tráfego de internet será controlado, de forma automática, e poderá ser inspecionado, pela ferramenta de *proxy web* (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta norma ou definidos pela Administração do Tribunal. (item alterado pela Portaria nº 299/2022)

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, à Secretaria de Tecnologia da Informação e Comunicações, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação, para deliberação. (item alterado pela Portaria nº 7.137/2017)

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, quando implementadas, serão comunicadas à Seção Central de Serviços de Tecnologia da Informação e Comunicações, a fim de possibilitar o repasse de informações aos usuários interessados. (item alterado pela Portaria nº 2.926/2021)

6. Monitoramento e Auditorias

6.1. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicações. (item alterado pela Portaria nº 7.137/2017)

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

(Com a redação dada pelas Portarias nºs 7.138/2014, 1.409/2015 7.628/2016, 1.885/2018, 6.493/2019, 4.786/2020 e 299/2022)

1. Objetivo

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

2. Motivação

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

2.2. Proteção do ambiente tecnológico do Tribunal.

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

3. Conceitos e definições

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

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

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

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

do Tribunal, ou, em casos justificados, relacionada a atividades específicas ou eventos extraordinários temporários. (item alterado pela Portaria nº 1.885/2018)

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

3.3. Lista de distribuição – agrupamento de diversos endereços eletrônicos, representado por um endereço eletrônico específico, que permite a distribuição conjunta de uma mensagem eletrônica a todos os seus integrantes. (item alterado pela Portaria nº 4.786/2020)

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

3.5. Identificador – parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@), que o diferencia das demais caixas postais e identifica seu usuário, setor ou finalidade. (item alterado pela Portaria nº 4.786/2020)

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

3.7. Arquivo de registro de mensagens (*logs*) – registro de eventos, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias. (item alterado pela Portaria nº 299/2022)

3.8. Usuário de correio eletrônico – magistrado, servidor ou estagiário que utiliza alguma caixa postal eletrônica. (item alterado pela Portaria nº 4.786/2020)

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

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

3.11. *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, *ransomware* e *rootkit).* (item alterado pela Portaria nº 1.885/2018)

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

3.13. *Hoax* – mensagem eletrônica encaminhada a muitos destinatários, de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas. (item alterado pela Portaria nº 4.786/2020)

3.14. *Alias* - endereço eletrônico alternativo para uma conta de correio eletrônico. Pode ser usado para exibir um endereço genérico ou temporário para o público. (item incluído pela Portaria nº 4.786/2020)

4. Referências Normativas (item alterado pela Portaria nº 299/2022)

4.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

4.2. 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.

4.3. 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 da organização.

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

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

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

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

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

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

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

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

5.7. Caixa Postal Institucional Pessoal

5.7.1. Magistrados e Servidores (item alterado pela Portaria nº 1.885/2018)

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

5.7.1.2. A criação de caixa postal institucional pessoal de servidor ou magistrado será feita pela SETIC após a notificação de seu ingresso pela SEGESP. (item alterado pela Portaria nº 4.786/2020)

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

5.7.1.4. Em situações justificadas, o identificador dos endereços de correio eletrônico poderá ser formado segundo outra ordem ou abreviação do nome do usuário.

5.7.1.5. A adequação dos endereços de correio eletrônico que não correspondam ao padrão estabelecido nesta norma será solicitada à SETIC pelo usuário interessado.

5.7.1.6. A caixa postal institucional pessoal de magistrados e/ou servidores será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta de magistrado, vacância por posse em outro cargo inacumulável e cedência permanente a outro órgão ou retorno à origem. (item alterado pela Portaria nº 4.786/2020)

5.7.1.6.1. Não ocorrerá a exclusão da caixa postal institucional pessoal nos casos de licenças. (item incluído pela Portaria nº 4.786/2020)

5.7.1.7. Ocorridos os fatos descritos no item anterior, incumbe à Secretaria de Gestão de Pessoas comunicá-los à Secretaria de Tecnologia da Informação e Comunicações, no prazo de até 5 dias da publicação do Ato respectivo, exceto nos casos de demissão, quando a comunicação deverá ocorrer de imediato à ciência do afastamento pela Secretaria de Gestão de Pessoas. (item alterado pela Portaria nº 4.786/2020)

5.7.1.8. Nos casos de demissão haverá suspensão imediata da caixa postal institucional, a partir da comunicação da Secretaria de Gestão de Pessoas. (item alterado pela Portaria nº 4.786/2020)

5.7.1.8.1. A exclusão da caixa postal será realizada somente após comunicada pela Secretaria de Gestão de Pessoas a decisão administrativa definitiva (que equivale ao trânsito em julgado). (item alterado pela Portaria nº 4.786/2020)

5.7.1.9. Nos demais casos de que trata o item 5.7.1.7, incumbe à Secretaria de Tecnologia da Informação e Comunicações:

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

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

5.7.2. Estagiários (item alterado pela Portaria nº 1.885/2018)

5.7.2.1. O gestor da unidade poderá solicitar, por escrito, à SETIC, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado. (item alterado pela Portaria nº 4.786/2020)

5.7.2.2. O envio de mensagens por estagiários será restrito a endereços eletrônicos mantidos pelo TRT. Quando for expressamente solicitado, com a devida justificativa pelo gestor da unidade a que vinculados, será permitido o envio a endereços externos. (item alterado pela Portaria nº 4.786/2020)

5.7.2.3. O uso do correio eletrônico pelo estagiário autorizado será de responsabilidade do gestor da unidade a que vinculado.

5.7.2.4. O identificador do endereço eletrônico do estagiário será formado pela primeira letra do seu nome seguida do último sobrenome, acrescido pela palavra “estagiario”, separados pelo sinal de ponto. (item alterado pela Portaria nº 299/2022)

5.7.2.5. A caixa postal institucional pessoal de estagiários será excluída definitivamente quando da comunicação da Secretaria de Gestão de Pessoas sobre o término do estágio.

5.8. Caixa Postal Institucional da Unidade

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

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

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

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

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

5.8.4. Em casos excepcionais, devidamente justificados, e a critério da Presidência, poderão ser criadas caixas postais institucionais a fim de atender comissões, grupos de trabalho ou núcleos formalmente constituídos, bem como demandas de trabalho específicas e eventos temporários. (item alterado pela Portaria nº 4.786/2020)

5.8.4.1. Nessa hipótese, quando da solicitação de criação da caixa postal, deverão ser indicados o magistrado, servidor ou unidade que será responsável pelo respectivo gerenciamento, bem como, se for o caso, o

período em que a caixa postal deverá ser mantida. (item incluído pela Portaria nº 1.885/2018)

5.8.4.2. Findada a necessidade para a qual a caixa postal institucional da unidade foi criada, o responsável pelo gerenciamento deverá informar à SETIC para a exclusão da caixa postal. (item incluído pela Portaria nº 4.786/2020)

5.9. Caixa Postal de Sistema

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

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

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

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

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

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

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

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

6.3. A solicitação deve ser encaminhada, por escrito, à Secretaria de Tecnologia da Informação e Comunicações, acompanhada de justificativa e de informações sobre a finalidade da lista, nome do gestor da lista, e, quando destinada à atividade temporária, do período de sua duração. (item alterado pela Portaria nº 1.885/2018)

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

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

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

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

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

6.6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido pelo período máximo de três meses, a contar da alteração. (item alterado pela Portaria nº 1.885/2018)

7. Utilização dos recursos do sistema de correio eletrônico

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

7.2. O acesso ao correio eletrônico a partir de estações de trabalho fornecidas pelo Tribunal será feito apenas a partir do navegador de internet. (item alterado pela Portaria nº 4.786/2020)

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

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

7.5. O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos é permitido em caráter excepcional ou a unidades administrativas, autorizado pela Presidência. (item alterado pela Portaria nº 4.786/2020)

7.6. É de responsabilidade do usuário: (item alterado pela Portaria nº 4.786/2020)

a) eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;

b) manter exclusivo o acesso à sua caixa postal institucional pessoal, não compartilhando a respectiva senha e/ou delegando o acesso a terceiros.

c) informar ao Escritório de Segurança da Informação o recebimento de mensagens que contrarie o disposto no item 7.7.

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

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

b) materiais obscenos, ilegais ou antiéticos;

c) materiais preconceituosos ou discriminatórios;

d) materiais caluniosos ou difamatórios;

e) propaganda com objetivo comercial;

f) listagem com endereços eletrônicos institucionais, exceto nos casos em que a atividade funcional demande tal ação; (item alterado pela Portaria nº 299/2022)

g) *malwares*; (item alterado pela Portaria nº 4.786/2020)

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*; (item alterado pela Portaria nº 4.786/2020)

o) materiais criptografados, exceto nos casos em que as informações da mensagem necessitem proteção quanto ao sigilo. (item alterado pela Portaria nº 4.786/2020)

7.8. A recuperação de mensagens de caixas postais institucionais de unidade poderá ser solicitada pelo respectivo responsável desde que seja formalizado e justificado por meio de sistema de atendimento de TI.

7.8.1. A SETIC não garante a recuperação de mensagens de e-mails ou de caixas postais excluídos há mais de 20 dias. (item alterado pela Portaria nº 4.786/2020)

7.8.2. Recuperada(s) a(s) mensagem(ns) de e-mail, a SETIC verificará com o solicitante a melhor forma de disponibilizá-la(s) novamente; (item incluído pela Portaria nº 6.493/2019)

7.8.3. Casos omissos serão tratados pela SETIC pontualmente. (item incluído pela Portaria nº 6.493/2019)

8. Monitoramento e Auditoria

8.1. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio. (item alterado pela Portaria nº 4.786/2020)

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

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

8.4. Os arquivos de registro de mensagens eletrônicas (logs) serão mantidos pelo prazo de 30 dias, exceto nos casos de auditoria ou notificação administrativa ou judicial, em que serão devidamente armazenados pelo Escritório de Segurança da Informação, a fim de salvaguardar os dados respectivos. (item alterado pela Portaria nº 1.885/2018)

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

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

9. Atualização da Norma

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

ANEXO 3

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

(Anexo incluído pela Portaria n° 8.604/2013 e alterado pelas Portarias n° 1.063/2016, 7.628/2016, 1.885/2018, 6.493/2019, 4.786/2020 e 299/2022)

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 (item alterado pela Portaria nº 299/2022)

3.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

3.2. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

3.3. Instrução Normativa GSI/PR nº 5, de 31 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

3.4. 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.

3.5. 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.

3.6. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.7. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação.

3.8. 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.

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

3.10. Portaria GP nº 3.244/2021, de 25 de novembro de 2021, que estabelece normas gerais sobre administração de materiais de consumo e bens permanentes no âmbito do Tribunal Regional do Trabalho da 4ª Região.

3.11. Resolução CSJT nº 164, de 18 de março de 2016, que disciplina o uso e a concessão de certificados digitais institucionais no âmbito da Justiça do Trabalho de primeiro e segundo graus.

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: métodos para garantir que o acesso aos ativos seja autorizado e restrito com base no negócio e em segurança. (item alterado pela Portaria nº 4.786/2020)

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, *ransomware* e *rootkit*). (item alterado pela Portaria nº 1.885/2018)

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.

4.12. Acesso privilegiado - nível de acesso restrito onde uma pessoa tem permissão para gerenciar um sistema e/ou serviço. (item incluído pela Portaria nº 1.885/2018)

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, os dispositivos móveis, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios; (item alterado pela Portaria nº 1.885/2018)

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 e serviços tecnológicos desenvolvidos com base nos recursos providos pelo TRT4; (item alterado pela Portaria nº 299/2022)

V) os sistemas e serviços tecnológicos contratados de terceiros, sob licença ou na forma de software livre ou aberto, incluídas as soluções baseadas em nuvem. (item alterado pela Portaria nº 299/2022)

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*.

5.1.7. O regramento de utilização dos certificados digitais fornecidos pelo Tribunal a magistrados e servidores, bem como a definição de responsabilidades, observarão o disposto nas Resoluções CSJT nº 164/2016 e nº 186/2017 e ao Manual de Instruções para Certificação Digital da SEGESP. (item alterado pela Portaria nº 299/2022)

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.

5.2.5. 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.

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

5.2.5.2. 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.

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

5.2.5.4. 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.

5.2.6. 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.

5.2.6.1. 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.

5.2.6.2. É proibido o armazenamento, em qualquer diretório na rede do Tribunal ou nas soluções baseadas em nuvem, de arquivos não

relacionados ao trabalho, tais como: (item alterado pela Portaria nº 1.885/2018)

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 (item alterado pela Portaria n° 1.885/2018)

5.3.1.Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 5.2.6.2.

5.3.2.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.

5.3.3.Os arquivos armazenados na nuvem corporativa deverão ser vinculados (ter como proprietário) à caixa postal institucional da unidade, quando existente, ou outra designada pelo gestor da unidade para tal fim.

5.3.4.Nos casos de relotação ou afastamentos previstos no Anexo 2 desta Política (casos de exclusão da caixa postal), o gestor deverá solicitar ao servidor ou estagiário, de forma antecipada, sempre que possível, a verificação da existência de arquivos que digam respeito às atividades da unidade e que permaneçam na propriedade do servidor/estagiário, para que sejam transferidos para a caixa postal institucional da unidade ou outra designada pelo gestor.

5.3.4.1.Caso persistam arquivos vinculados à caixa postal institucional do servidor/estagiário quando de sua exclusão, eles serão transferidos para a caixa postal institucional da unidade, ou outra designada pelo gestor, para triagem e definição da necessidade ou não de manutenção dos arquivos.

5.3.5.Nos casos de exclusão da caixa postal institucional de magistrados (exceto a hipótese de falecimento), será dada ciência, de forma antecipada, sobre a necessidade de transferência ou *download* dos arquivos armazenados na nuvem, sob pena de serem excluídos juntamente com a caixa postal.

5.3.6.Nos casos de exclusão da caixa postal institucional de unidade, os arquivos serão transferidos para a conta da unidade designada como nova responsável pelas atividades ou para servidor designado para tal fim.

5.3.7.A SETIC não garante a recuperação de caixas postais, mensagem de e-mails e arquivos armazenados na solução em nuvem excluídos há mais

de 30 dias. (item incluído pela Portaria nº 4.786/2020)

5.4.Equipamentos fornecidos pelo Tribunal (item alterado pela Portaria n° 1.885/2018)

5.4.1.O fornecimento de equipamentos a magistrados e servidores, quando autorizado, está condicionado às necessidades de trabalho e à responsabilização formal a partir de seu recebimento. (item alterado pela Portaria nº 4.786/2020)

5.4.2.Os computadores portáteis são fornecidos com 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. (item alterado pela Portaria nº 4.786/2020)

5.4.2.1.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.

5.4.2.2.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.

5.4.3.Em caso de falecimento, aposentadoria, exoneração, demissão, cedência, remoção, redistribuição, dispensa da função 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, se outro prazo não houver sido estipulado em norma específica.

5.4.4.Nos casos de perda, furto ou roubo do equipamento, bem como nas hipóteses de ausência de devolução ou verificação de existência de avarias no equipamento devolvido, a Secretaria de Tecnologia da Informação e Comunicações informará à Diretoria-Geral a situação ocorrida, com a documentação respectiva, para as providências cabíveis.

5.4.4.1.Ocorrido um dos fatos acima, a reposição, quando autorizada pelo Comitê de Governança de TIC, dependerá da disponibilidade de equipamento para substituição.

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 poderá passar a integrar o padrão utilizado na configuração dos novos equipamentos. Quando necessário, o pedido, acompanhado de parecer técnico, será submetido ao Comitê Gestor de Segurança da Informação. (item alterado pela Portaria n° 299/2022)

6. Do controle do acesso

6.1. Do gerenciamento de acessos (item alterado pela Portaria n° 1.885/2018)

6.1.1. Os acessos 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 e a Secretaria de Gestão de Pessoas informarão à Secretaria de Tecnologia da Informação e Comunicações, respectivamente, a posse de novos juízes de primeiro grau e a de desembargadores, a fim de agilizar o primeiro cadastro.

6.1.4. A administração dos acessos dos magistrados no PJe é responsabilidade da Secretaria de Apoio aos Magistrados, relativamente aos juízes de primeiro grau, e da Secretaria-Geral Judiciária, relativamente aos desembargadores.

6.1.5. 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.

6.1.6. 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.

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

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

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

6.1.8. Nos casos em que autorizada a prestação de trabalho remoto, a Secretaria de Gestão de Pessoas comunicará à Secretaria de Tecnologia da Informação e Comunicações o término das atividades que o ensejaram para retirada dos acessos necessários ao trabalho à distância.

6.1.9. O privilégio de administrador na estação de trabalho é restrito aos membros da equipe técnica da SETIC que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

6.1.9.1. Nos computadores portáteis disponibilizados pelo Tribunal aos magistrados, estes terão privilégio de administrador local. (item alterado pela Portaria nº 299/2022)

6.1.10. Os acessos privilegiados aos sistemas e serviços de TIC serão concedidos aos membros da equipe técnica da SETIC, sempre que necessários ao desempenho das atividades funcionais, de modo a permitir a gestão e configuração do ambiente tecnológico.

6.1.10.1. É responsabilidade da chefia imediata solicitar a concessão, a alteração e a remoção dos acessos privilegiados dos seus subordinados.

6.1.10.2. Os acessos concedidos deverão ser revisados pelo menos uma vez ao ano.

6.1.11. 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. (item alterado pela Portaria nº 4.786/2020)

6.1.11.1. No caso do prestador de serviço necessitar de acesso privilegiado, as regras observarão o disposto no item 6.1.10.

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 contêm 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 de rede deverá contemplar os seguintes requisitos: (item alterado pela Portaria nº 299/2022)

I) ter, no mínimo, 08 (oito) caracteres;

II) não conter o nome de usuário (*login*) de rede;

III) conter ao menos três dos quatro tipos de caracteres listados a seguir: número (ex.: 1, 2, 3, 4…), maiúsculo (A, B, C, D..), minúsculo (a, b, c, d…) e especial (!,@, #, ?..);

6.2.7. Não poderão ser utilizadas as 02 (duas) últimas senhas de rede definidas pelo(a) usuário(a). (item alterado pela Portaria nº 6.493/2019)

6.2.8. A senha de rede deve ser alterada dentro de um período não maior do que 180 dias. (item alterado pela Portaria nº 299/2022)

6.2.9. Excetuam-se da regra dos itens 6.2.6 e 6.2.7 os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos. (item alterado pela Portaria n° 6.493/2019)

6.2.10. 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. (item alterado pela Portaria nº 6.493/2019)

6.2.11. 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. (item incluído pela Portaria nº 6.493/2019)

7. Registros (log) de Eventos

7.1. Serão mantidos, por um período mínimo de três (3) meses, os registros dos acessos dos usuários e dos acessos privilegiados aos recursos tecnológicos disponibilizados pelo TRT4, inclusive para fins de apuração e comprovação de incidentes de segurança. (item alterado pela Portaria nº 1.885/2018)

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 compilado com as alterações promovidas pelas Portarias nº 7.138/2014, 4.145/2016, 7.628/2016, 7.137/2017, 230/2019, 6.493/2019, 4.786/2020 e 299/2022)

1. Objetivo

1.1. Estabelecer diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicações, no âmbito do Tribunal Regional do Trabalho da 4ª Região.

2. Motivações

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

2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo às necessidades do Tribunal.

2.3. Alinhar expectativas no processo de salvaguarda e *restore* dos dados armazenados em backup, visto que tal procedimento é uma das ações do processo de restauração/restabelecimento do ambiente. (item incluído pela Portaria nº 299/2022)

3. Conceitos e definições

3.1. *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*.

3.2. *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).

3.3. *Backup* completo – são copiados todos os arquivos existentes no momento do backup.

3.4. *Backup* em fita - mídia magnética. Pode ser movida para cofre resistente a fogo.

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

3.6. Disco rígido - Dispositivo de armazenamento local de dados utilizados pelos computadores.

3.7. Equipamento servidor - Computador com alta capacidade de armazenamento e processamento, destinado ao provimento de serviços e sistemas de TIC.

3.8. Produto, sistema ou serviço - soluções tecnológicas que demandam a salvaguarda de dados por ele utilizados;

3.9. Responsável pelo produto, sistema ou serviço - magistrado, servidor ou área de negócio que responde e/ou define os requisitos da solução.

3.10. 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. Em outras palavras, RPO (em tradução livre "Objetivo do Ponto de Recuperação", resumidamente engloba o volume de dados perdidos nos casos de tempo de inatividade do serviço. Se a recuperação de um sistema com erro foi feita rapidamente (em minutos), isso não significa que a empresa perderá apenas esses minutos de trabalho, pois os dados recuperados podem ter sido capturados há uma semana, de modo que a perda real de dados nesse caso seria de uma semana.

3.11. RTO (*Recovery-Time Objective*) – tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente. RTO (em tradução livre "Objetivo de Tempo de Recuperação", define o período de tempo desejado necessário para realizar todas as tarefas de recuperação antes que um aplicativo ou serviço possa executar solicitações normalmente novamente. Resumidamente quanto tempo um serviço ou estrutura de TI pode ficar parada aguardando recuperação. Para fins dessa norma, o RTO deve ser considerado apenas para a restauração dos dados. (item alterado pela Portaria nº 299/2022)

3.12. Versão ativa - é a última versão do arquivo no backup.

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

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

3.15. *Virtual Tape Library* (VTL) - tecnologia que emula fitas magnéticas em disco, o que garante gravação e restauração em alta velocidade. No TRT há duas soluções de VTL, em locais físicos distintos, para fins de continuidade e disponibilidade.

4. Referências Normativas

4.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de estão de Segurança da Informação e Comunicações na Administração Pública Federal. (item alterado pela Portaria nº 299/2022)

4.2. 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.

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

5. Procedimentos de *backup* (item alterado pela Portaria nº 4.786/2020)

5.1. O responsável pelo produto, sistema ou serviço deve solicitar formalmente à Coordenadoria de Infraestrutura Tecnológica a inserção de dados ao sistema de backup, previamente à entrada em operação de tais soluções.

5.1.1. Cabe ao responsável pelo produto, sistema ou serviço, definir, com apoio da SETIC, os requisitos para realização do backup, tais como: os dados que

devem estar contemplados no backup, tempo de retenção, RTO, RPO, dentre outros.

5.1.2. Em caso de alteração dos requisitos para realização do backup, o responsável deverá atualizar a Coordenadoria de Infraestrutura Tecnológica das novas demandas, para correta salvaguarda das informações.

5.2. Os procedimentos de *backup* realizados pela SETIC serão executados por soluções automatizadas, seguindo especificações técnicas definidas pela equipe técnica responsável, em conformidade com a presente política, abrangendo os dados armazenados no ambiente tecnológico disponibilizado pelo TRT.

5.3. O *backup* dos dados armazenados nos servidores das unidades do interior do Estado será realizado diariamente, à noite.

5.4. Os dados armazenados no disco rígido de estações de trabalho ou de notebooks não serão objeto de *backup* de dados. Nesse sentido, sua recuperação não é garantida em casos de indisponibilidade causados por erros de hardware no disco rígido, apagamentos acidentais ou intencionais, falhas no sistema operacional, ação de códigos maliciosos, dentre outros.

5.5. Os dados objeto de *backup* tipo "*archive"* 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.

5.6. 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):

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

5.7.A periodicidade, o tempo de retenção, o RPO e o RTO dos *backups* do banco de dados Postgresql relativos ao PJe-JT observarão as seguintes regras:

Tipo de Backup	**BANCO DE DADOS POSTGRESQL**	
***Backup* diário VTL**	**Dias e horários**	Completo, todos os dias.
	Retenção	A versão objeto do *backup* será retida pelo período de quinze (15) dias.
Backup semanal (tipo archive) Tape	**Dia**	Todo final de semana que não coincidir com o backup mensal
	Retenção	15 dias
***Backup* mensal (tipo *archive*) Tape**	**Dia**	Primeiro final de semana de cada mês
	Retenção	A versão objeto do *backup* será retida pelo período de um (1) ano
***Backup* anual (tipo *archive*) Tape**	**Dia**	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.
	Retenção	A versão objeto do *backup* será retida pelo período de cinco (5) anos.
VTL - RPO (tempo máximo de perda dos dados)	4 horas	
VTL - RTO (tempo estimado para a restauração)	20 horas	
RPO (tempo máximo de perda dos dados) Tape	1 semana	
RTO (tempo estimado para a restauração) Tape	20h + procedimentos de inserção das fitas	

5.8. No caso de serviços armazenados em nuvem, a responsabilidade pelo *backup* será da prestadora de serviços, assegurado um prazo de retenção de, no mínimo, 30 dias.

5.9. As mídias de backup, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.

5.9.1. A movimentação de mídias de *backup* deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a data e hora da movimentação.

6. Recuperação de dados

6.1. 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.

7. Testes de recuperação de dados

7.1. Periodicamente serão realizados testes de recuperação de dados.

7.2. 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: (item alterado pela Portaria nº 299/2022).

Grupo de *backup*	**Equipes responsáveis pela recuperação**	**Periodicidade**	**Recuperação**	**Equipe responsável pela validação**	**Validação**
Arquivos armazenados em diretórios de rede na Capital	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.
	SST	Mensal	Utilizando o recurso “Versões Anteriores”, restaurar versão do dia anterior de arquivos das cópias intradiárias	SST	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Arquivos armazenados em diretórios de rede do interior	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.
PJe/Banco de dados	SGDB	Trimestral	Restauração efetuada em um servidor específico para essa funcionalidade, em ambiente VMware.	SGBD	Testar a integridade dos dados e funcionamento da base principal do PJe restaurada.

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

7.4. 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.

8. Atualização da Norma

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de backup, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO 5

NSI005 – Comitê Gestor de Segurança da Informação

(Anexo incluído pela Portaria nº 2.937/2014 e alterado pelas Portarias n° 8.736/2015, 7.628/2016, 7.137/2017, 3.241/2019, 486/2020, 4.786/2020, 882/2021, 2.926/2021 e 299/2022)

1. Integrantes do Comitê (item alterado pela Portaria nº 299/2022)

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

- EDUARDO MUNARI PRETO, Assessor-Jurídico da Presidência do Tribunal;
- JOAO HENRIQUE CARVALHO DE LIMA RIBAS, Diretor da Secretaria de Administração;
- ADOLFO MARQUES PEREIRA, Secretário-Geral Judiciário;
- JEFERSON ANDRADE, Assessor Técnico-Operacional da Corregedoria;
- MARIA AUGUSTA KINNEMANN, Diretora da Secretaria de Gestão de Pessoas;
- ANDRÉ SORAES FARIAS, Diretora da Secretaria de Tecnologia da Informação e Comunicações;
- JOÃO LUIZ PEIXOTO DA SILVA, Coordenador da Coordenadoria de Segurança Institucional;
- LUCAS POZATTI, Assistente-chefe do Escritório de Segurança da Informação, que coordenará o grupo;

2. Competências do Comitê (item alterado pela Portaria nº 2.926/2021)

2.1 Compete ao Comitê Gestor de Segurança da Informação:

I – assessorar a alta administração do órgão do Poder Judiciário em todas as questões relacionadas à segurança da informação;

II - estabelecer diretrizes e definições estratégicas para as ações e projetos relacionados à Segurança da Informação;

III – propor alterações na política de segurança da informação e deliberar sobre assuntos a ela relacionados, incluindo atividades de priorização de ações e gestão de riscos de segurança;

IV – propor normas internas relativas à segurança da informação;

V - 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;

VI – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

VII – consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.

3. Funcionamento do Comitê (item alterado pela Portaria nº 299/2022)

3.1. Nos impedimentos ou afastamentos do assistente-chefe do Escritório de Segurança da Informação, o Comitê Gestor de Segurança da Informação será presidido pelo Diretor da Secretaria de Tecnologia da Informação e Comunicações.

3.2. As deliberações do Comitê Gestor de Segurança da Informação poderão ser realizadas por meio de reunião presencial ou remota, ou por outro meio eletrônico.

3.3. O quórum mínimo para deliberação é de quatro membros.

3.4. Compete ao coordenador do Comitê a convocação para as reuniões.

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

3.4.1.1. Membros não integrantes não terão direito a voto nas deliberações do Comitê Gestor de Segurança da Informação.

3.4.2. A pauta da reunião e os respectivos documentos serão previamente disponibilizados 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 por todos os integrantes do Comitê presentes na reunião, em expediente administrativo eletrônico classificado como sigiloso, quando necessário.

3.5. As deliberações do Comitê Gestor de Segurança da Informação serão 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 e alterado pelas Portarias nº 7.628/2016, 7.137/201, 6.493/2019, 4.786/2020, 2.926/2021 e 299/2022).

1. Objetivos

1.1. 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).

2. Aplicabilidade

2.1. 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.

3. Motivações

3.1. 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.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. Referências normativas

4.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. (item alterado pela Portaria nº 299/2022)

4.2. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. (item alterado pela Portaria nº 299/2022)

4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.4. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos. (item alterado pela Portaria n° 6.493/2019)

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

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

segurança da informação dentro do contexto da organização.

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

4.8. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação. (item incluído pela Portaria nº 4.786/2020)

5. Conceitos e definições

5.1. Ameaça - causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização; (item alterado pela Portaria nº 4.786/2020)

5.2. Análise de riscos - processo para compreender a natureza do risco e determinar o nível de risco; (item alterado pela Portaria nº 4.786/2020)

5.3. Avaliação de riscos - processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis; (item alterado pela Portaria nº 4.786/2020)

5.4. 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;

5.5. Comunicação do risco - conjunto de processos contínuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos; (item alterado pela Portaria nº 4.786/2020)

5.6. Estimativa de riscos - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

5.7. 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;

5.8. 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;

5.9. 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.

5.10. 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.

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

5.12. 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;

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

5.14. 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;

5.15. 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;

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

5.17. Vulnerabilidade - fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças. (item alterado pela Portaria nº 4.786/2020)

6. Escopo

6.1 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.

7. Diretrizes

7.1. 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.

7.2. 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.

7.3. 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.

8. Gestão de riscos em projetos de TIC

8.1. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada pela Secretaria de Tecnologia da Informação de Comunicações. (item alterado pela Portaria n° 6.493/2019)

9. Gestão de riscos em processos de TIC

9.1. 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. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo. (item alterado pela Portaria n° 7.137/2017 e pela Portaria nº 6.493/2019)

9.2. A gestão de riscos em processos de TIC é monitorada pelo Seção de Conformidade e Processos de Tecnologia da Informação e Comunicações. (item alterado pela Portaria n° 2.926/2021)

10. Gestão de riscos em Segurança da Informação e Comunicações (GRSIC-TRT4) (item alterado pela Portaria n° 4.786/2020)

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

10.2. O processo de GRSIC-TRT4 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011 e ABNT NBR ISO/IEC 31000:2018 e na Instrução Normativa GSI/PR nº 3. (item alterado pela Portaria nº 299/2022)

10.3. Os critérios para avaliação do risco levam em consideração o "PSR": a) **Probabilidade**, que é a possibilidade de uma vulnerabilidade ser explorada por uma ou mais ameaça(s), 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. 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

10.4. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

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

10.5.1. Contextualização - compreende a definição e aprovação do contexto da análise e avaliação de riscos a ser realizada, com a identificação de seu propósito, escopo, limites e partes interessadas.

10.5.2. Análise e Avaliação dos Riscos - compreende o mapeamento dos ativos, identificação, análise e avaliação dos riscos, bem como a elaboração e aprovação do Plano de Tratamento dos Riscos.

10.5.3. Tratamento dos Riscos - compreende a implementação das ações do Plano de Tratamento de Riscos, seu monitoramento e apresentação dos resultados.

10.5.4. Melhoria contínua - compreende a realização da análise crítica pela Administração, com avaliação dos resultados e das propostas de melhoria apresentadas.

10.6. O desenho do processo de Gestão de Riscos de Segurança da Informação, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como demais documentos relacionados, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

10.7. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior.

11. Atualização da Norma

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

ANEXO 7

NSI007 – Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETRI

(Anexo incluído pela Portaria nº 6.137/2014 e alterado pelas Portarias nºs 7.137/2017, 1.885/2018, 6.493/2019, 4.786/2020, 2.926/2021 e 299/2022)

1. Objetivos

1.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRI) do Tribunal Regional do Trabalho da 4ª Região.

2. Motivações

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

2.2. Necessidade de formalização da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRI) e seu funcionamento.

2.3. Proteção do ambiente tecnológico do Tribunal.

3. Referências Normativas

3.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. (item alterado pela Portaria nº 299/2022)

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 ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação. (item incluído pela Portaria nº 4.786/2020)

4. Conceitos e definições (item alterado pela Portaria nº 4.786/2020)

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. Comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;

4.3. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETRI: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.

4.4. Incidente de segurança da informação: Um único ou uma série de eventos indesejados ou inesperados de segurança da informação que têm uma probabilidade significativa de colocar em perigo as operações da instituição e ameaçar a segurança da informação.

4.5. Tratamento de Incidentes de Segurança da Informação: conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação.

4.6. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

5. Missão da ETRI

5.1. Prover capacidade adequada para resposta e tratamento de incidentes de segurança da informação em ambiente tecnológico. (item alterado pela Portaria nº 4.786/2020)

6. Público-alvo

6.1. O público-alvo da ETRI é formado por todos os usuários do ambiente tecnológico deste Tribunal. (item alterado pela Portaria nº 4.786/2020)

6.2. A ETRI relaciona-se, internamente, com as diversas unidades da Secretaria de Tecnologia da Informação e Comunicações e com o Comitê Gestor de Segurança da Informação. (item alterado pela Portaria nº 299/2022)

6.3. 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.

7. Modelo de Implementação

7.1. 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 de segurança da informação.

8. Estrutura Organizacional e Composição

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

8.2. A ETRI é composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, sendo: (item alterado pelas Portarias nºs 2.926/2021 e 988/2022)

- assistente-chefe do Escritório de Segurança da Informação;

- coordenador(a) da Coordenadoria de Desenvolvimento de Sistemas;

- assistente-chefe da Seção de Portais Corporativos;

- coordenador(a) da Coordenadoria de Atendimento a Usuários;

- coordenador(a) da Coordenadoria de Infraestrutura Tecnológica;

- os(as) assistentes-chefes da Coordenadoria de Infraestrutura Tecnológica;

- coordenador(a) da Coordenadoria de Implantação de Sistemas.

8.3. Para cada uma das posições o substituto formalmente designado será o suplente; (item alterado pela Portaria nº 4.786/2020)

8.4. Caso necessário, deverão ser convocados outros servidores da Secretaria de Tecnologia da Informação e Comunicações e/ou servidores de outras áreas do Tribunal (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades. (item alterado pela Portaria nº 4.786/2020)

9. Autonomia (item alterado pela Portaria nº 4.786/2020)

9.1. A autonomia da ETRI é compartilhada. A equipe recomendará, no mínimo, aos Coordenadores das áreas técnicas envolvidas e à Diretoria da Secretaria de Tecnologia da Informação e Comunicações, 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 ao Comitê de Segurança da Informação e/ou à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

10. Atribuições (item alterado pela Portaria nº 4.786/2020)

10.1. Investigar e propor ações de contenção para os incidentes de segurança da informação relacionados aos ativos de tecnologia de informação;

10.2. Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção;

10.3. Fornecer informações, aos envolvidos, sobre a ocorrência e, ao público interno, orientações de prevenção de incidentes de segurança da informação.

10.4. Manter os registros dos incidentes de segurança da informação relacionados aos ativos de tecnologia da informação;

10.5. Divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários. (item alterado pela Portaria nº 299/2022)

10.6. Interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, participação em fóruns e redes nacionais e internacionais.

11. Atualização da Norma

11.1. 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 8

NSI008 – Gestão de Incidentes de Segurança da Informação

(Anexo incluído pela Portaria nº 7.791/2015 e alterado pelas Portarias nº 7.628/2016, 7.137/2017, 6.493/2019, 4.786/2020 e 299/2022)

1. Objetivos

1.1. 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. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal; (item alterado pela Portaria nº 299/2022)

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.

3.6. Norma Complementar nº 21/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. (item incluído pela Portaria nº 7.137/2017)

3.7. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação. (item incluído pela Portaria nº 4.786/2020)

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 restabelecimento do sistema/serviço afetado, mesmo eu não seja em sua capacidade total. (item alterado pela Portaria nº 6.493/2019)

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: fragilidade de um ativo ou controle que pode ser explorado por uma ameaça. (item alterado pela Portaria nº 4.786/2020)

4.11. CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI; (item incluído pela Portaria nº 7.137/2017)

5. Escopo

5.1. 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. (item alterado pela Portaria nº 4.786/2020)

6. Diretrizes

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de 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, parcial ou total, 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. (item alterado pela Portaria nº 6.493/2019)

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.

7.4. 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 a reportará Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação. (item alterado pela Portaria nº 4.786/2020)

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

7.6. 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.

7.7. 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 de Segurança da Informação, para o devido registro e encaminhamento. (item alterado pela Portaria nº 7.137/2017)

7.8. 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.

7.9. 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.

7.10. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação deve conduzir, apoiada pelas outras áreas da SETIC, investigação do incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários. (item alterado pela Portaria nº 4.786/2020)

7.11. A coleta de evidência dos incidentes de segurança da Informação deve ser realizada pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação ou por pessoal competente e por ela autorizado. (item alterado pela Portaria nº 7.137/2017)

7.12. 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.

7.13. 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.

7.14. O encerramento do incidente de segurança da informação será realizado pelo Escritório de Segurança da Informação, com comunicação a todas as áreas interessadas e 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. (item alterado pela Portaria nº 4.786/2020)

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

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

7.17. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior. (item alterado pela Portaria nº 7.137/2017)

8. Atualização da norma

8.1. 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.

ANEXO 10

NSI010 – Gestão de Continuidade de TIC

(Anexo incluído pela Portaria n° 2.050/2016 e alterado pelas Portarias nº 7.137/2017, 230/2019, 4.786/2020 e 299/2022)

1. Objetivos

1.1. 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. Manutenção de um nível aceitável de resiliência dos serviços e sistemas de TIC frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria da prestação jurisdicional. (item alterado pela Portaria nº 230/2019)

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

3. Referências normativas

3.1. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal; (item alterado pela Portaria nº 299/2022)

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 22301:2020, 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. (item alterado pela Portaria nº 299/2022)

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 de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável, previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas. (item alterado pela Portaria nº 4.786/2020)

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: conjunto de procedimento documentados que orientam a organização, após a interrupção, em como responder, recuperar, retomar e restaurar para um nível predefinido de operação, composto por Plano de Continuidade Operacional e Plano de Recuperação de Desastres. (item alterado pela Portaria nº 4.786/2020)

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*): ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

(item alterado pela Portaria nº 4.786/2020)

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 aprovação dos planos, seu armazenamento e divulgação. (item alterado pela Portaria nº 230/2019)

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.

6.3. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior. (item alterado pela Portaria nº 7.137/2017)

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.

7.5. 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.

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

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

7.8. 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

8.1. 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.