TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO
Gabinete da Presidência

RESOLUÇÃO GP N. 134, DE 19 DE DEZEMBRO DE 2019

Institui a Política de Segurança da Informação e Comunicação do Tribunal Regional do Trabalho da 3ª Região (POSIC-TRT3).

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o art. 9º da Resolução n. 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça (CNJ), que incumbiu ao Comitê Gestor de Segurança da Informação de cada órgão elaborar e aplicar política, gestão e processo de segurança da informação, a serem desenvolvidos em todos os níveis da instituição, em harmonia com as diretrizes nacionais preconizadas por aquele Conselho;

CONSIDERANDO a Instrução Normativa n. 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República (GSIPR), que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal (APF), direta e indireta, e dá outras providências;

CONSIDERANDO os controles do Perfil de Governança de TI, editados pelo Tribunal de Contas da União (TCU), a fim de induzir o melhor uso da tecnologia da informação para aprimoramento dos serviços públicos e de ser referência no desenvolvimento digital em benefício da sociedade; e

CONSIDERANDO as Normas Técnicas da Série ABNT NBR ISO/IEC 27000 como referências para a implementação de boas práticas para gestão de segurança da informação e para o **benchmarking** com outros Tribunais,

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução institui a Política de Segurança da Informação e Comunicação do Tribunal Regional do Trabalho da 3ª Região (POSICTRT3).

Art. 2º A POSIC-TRT3 tem por finalidade estabelecer diretrizes e padrões para garantir a disponibilidade, a integridade, a confiabilidade e a autenticidade das informações necessárias ao exercício da prestação jurisdicional.

Parágrafo único. Integrarão a POSIC-TRT3 normas e procedimentos complementares relativos à segurança da informação, editadas pelo Tribunal.

Art. 3º As disposições desta Resolução se aplicam aos usuários de recursos de Tecnologia da Informação e Comunicação (TIC) deste Tribunal.

§ 1º Os contratos e convênios celebrados por este Tribunal, cujo objeto envolva o uso de recursos de TIC, conterão cláusula exigindo a observância da POSIC-TRT3.

§ 2º A POSIC-TRT3 será divulgada no site deste Tribunal na internet.

Seção Única
Das Definições

Art. 4º Para os efeitos desta Resolução, considera-se:

I - confidencialidade: qualidade da informação indisponível a pessoa, sistema, órgão ou entidade não autorizados ou não credenciados;

II - disponibilidade: qualidade da informação acessível e utilizável por indivíduos, equipamentos e sistemas autorizados;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

III - integridade: qualidade da informação não modificada ou destruída por indivíduos, entidades ou processos;

IV - autenticidade: qualidade da informação produzida, expedida, recebida, modificada ou destruída por indivíduo, equipamento ou sistema;

V - recurso de TIC: equipamento, dispositivo ou sistema de informática, infraestrutura para acesso à rede de computadores do Tribunal e internet;

VI - usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados ou cedidos e, quando previamente autorizados, voluntários, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas a serviço da Justiça do Trabalho que utilizem os recursos de TIC do Tribunal; e

VII - informação: dados, processados ou não, utilizáveis para produção e transmissão de conhecimento e peças processuais, contidos em qualquer meio, suporte ou formato.

CAPÍTULO II
DAS DIRETRIZES

Art. 5º O uso adequado dos recursos de TIC visa a garantir a continuidade da prestação jurisdicional deste Tribunal.

Parágrafo único. Os recursos de TIC disponibilizados ao usuário serão utilizados em atividades relacionadas às funções institucionais.

Art. 6º Informações, sistemas e métodos gerados ou criados por usuário no exercício de suas atribuições, ainda que fora das dependências onde esteja lotado e independentemente da forma de apresentação ou armazenamento, pertencem ao Tribunal e serão utilizados exclusivamente para fins relacionados às atividades institucionais.

Art. 7º A classificação das informações quanto ao grau e prazos de sigilo observará o disposto na Resolução GP n. 59, de 13 de outubro de 2016.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

Parágrafo único. As informações serão classificadas de forma que permitam tratamento diferenciado de acordo com seu grau de importância, criticidade, sensibilidade, em conformidade com os requisitos legais.

CAPÍTULO III
DO MONITORAMENTO E DAS AUDITORIAS

Art. 8º A utilização dos recursos de TIC será monitorada exclusivamente para detecção de incompatibilidades entre o uso dos recursos e as normas da POSIC-TRT3, a fim de prevenir e apurar incidentes de segurança da informação.

§ 1º Incidente de segurança da informação é todo evento relacionado à segurança de sistemas de computação ou de redes de computadores, confirmado ou sob suspeita, que:

I - viole os termos da POSIC-TRT3;

II - comprometa normas deste Tribunal ou diretrizes governamentais;

III - esteja em desconformidade com a legislação sobre a matéria;

IV - represente ameaça à disponibilidade de serviços; ou

V - exponha indevidamente informações sob custódia deste Tribunal ou facilite irregularmente o acesso a elas.

§ 2º Os incidentes de segurança da informação serão reportados no Portal da Central de Serviços de TI (Portal CSTI), pelo **link** Atendimento ao Usuário, no endereço eletrônico <https://portal.trt3.jus.br/internet/tec-informacao>.

Art. 9º Auditorias poderão ser realizadas pela SINC e pela DTIC para apurar eventos que possam representar riscos à segurança da informação ou contrariar as boas práticas no uso dos recursos de TIC.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

CAPÍTULO IV
DAS RESPONSABILIDADES

Seção I
Do Comitê Gestor de Segurança da Informação

Art. 10. Compete ao Comitê Gestor de Segurança da Informação (CGSI), assessorado pela Seção de Segurança da Informação e Comunicação (SINC):

I - elaborar e propor normas ou procedimentos internos, relativos à segurança da informação;

II - definir recursos necessários às ações de segurança da informação;

III - estabelecer critérios de classificação de dados e de informações, visando à garantia dos níveis de segurança desejados e normatização de acesso e uso;

IV - realizar ações preventivas e corretivas para tratamento e segurança da informação;

IV - promover cultura de segurança da informação neste Tribunal; e

V - implementar programas contínuos de conscientização e capacitação dos usuários internos.

Art. 11. O CGSI é composto pelos seguintes membros:

I - Desembargador presidente da Comissão de Informática, que também o presidirá;

II - representante da magistratura de segundo grau da 3ª Região;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

III - representante da magistratura de primeiro grau da 3ª Região;

IV - representante da Presidência;

V - representante da Corregedoria;

VI - representante da Escola Judicial;

VII - Diretor-Geral;

VIII - Diretor Judiciário;

IX - Secretário-Geral da Presidência;

X - Diretor de Administração;

XI - Diretor de Orçamento e Finanças;

XII - Diretor de Gestão de Pessoas;

XIII - Diretor de Tecnologia da Informação e Comunicações;

XIV - Secretário de Comunicação Social;

XV - Secretário de Controle Interno;

XVI - Secretário de Documentação; e

XVII - Chefe da Seção de Segurança da Informação e Comunicação.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

§ 1º Nos afastamentos temporários de seu Presidente, o CGSI será presidido pelo membro a que se refere o inciso II.

§ 2º Os integrantes do CGSI serão nomeados para um mandato de dois anos, coincidente com o mandato dos membros da Administração do Tribunal.

Art. 12. Os membros do CGSI se reunirão, pelo menos, a cada seis meses, e também sempre que forem convocados pelo Presidente do Comitê.

Seção II
Da Seção de Segurança da Informação e Comunicação

Art. 13. Compete à SINC:

I - elaborar minutas de normas de segurança da informação e encaminhá-las ao CGSI para deliberação;

II - gerir políticas, normas e processos vinculados à segurança da informação;

III - prestar assessoramento e apoio técnico especializado ao CGSI, mantendo-o informado a respeito de incidentes de segurança da informação;

IV - realizar monitoramento e auditorias, com emissão de relatórios sobre a adequação ou não do uso dos recursos de TIC à POSIC-TRT3;

V - analisar periodicamente os riscos de segurança da informação;

VI - promover ações de capacitação para conscientização de magistrados e servidores sobre segurança da informação e uso adequado da tecnologia;

VII - atuar de forma coordenada com outras unidades organizacionais em assuntos relacionados à segurança da informação;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

VIII - gerir riscos de segurança da informação;

IX - gerir a continuidade de serviços essenciais de TIC; e

X - gerir incidentes de segurança da informação.

Seção III
Da Responsabilidade dos Usuários

Art. 14. Compete aos gestores assegurar a observância da POSIC-TRT3 em suas unidades, e a todos os usuários, conhecê-la e cumpri-la.

Seção IV
Das Penalidades

Art. 15. O não cumprimento das determinações e diretrizes constantes da POSIC-TRT3 poderá caracterizar infração funcional, passível de apuração em processo administrativo disciplinar ou sindicância, sem prejuízo do reconhecimento das Responsabilidades penal e civil, assegurados aos envolvidos os direitos ao contraditório e à ampla defesa.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 16. Competem à SINC a supervisão e o acompanhamento do cumprimento da POSIC-TRT3.

Parágrafo único. Nos limites das respectivas competências, as unidades organizacionais deste Tribunal adotarão providências para a implementação da POSIC-TRT3.

Art. 17. A POSIC-TRT3 e suas normas e procedimentos complementares serão revistos sempre que necessário.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

Parágrafo único. As minutas de atos normativos resultantes dos trabalhos de revisão mencionados no **caput** serão apreciadas pelo CGSI, após manifestação do Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC).

Art. 18. As normas complementares à POSIC-TRT3 serão editadas sob a forma de Anexos, que integrarão a presente Resolução.

Art. 19. Os casos omissos serão submetidos à deliberação do CGSI.

Art. 20. Revoga-se a Resolução GP n. 7, de 21 de novembro de 2014.

Art. 21. Esta Resolução entra em vigor na data de sua publicação.

MARCUS MOURA FERREIRA
Desembargador Presidente

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

ANEXO I
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 1
EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR)

1. Missão

Coordenar as atividades, o tratamento e a resposta a incidentes em redes computacionais, com o objetivo de assegurar a disponibilidade e a segurança na prestação de serviços do Tribunal.

2. Público-alvo

O público-alvo da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) é formado pelos usuários da rede de computadores e sistemas deste Tribunal.

3. Estrutura

A ETIR compõe-se de servidores da SINC, que podem solicitar apoio multidisciplinar às demais áreas, sempre que houver necessidade, para responder a incidentes de segurança.

4. Atribuições da ETIR

4.1. Opinar sobre assuntos relacionados a tratamento e resposta a incidentes em redes computacionais;

4.2. Propor metodologias e processos específicos para tratamento e resposta a incidentes em redes computacionais, tais como análise, avaliação de riscos e vulnerabilidades;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

4.3. Prover ações de monitoria, auditoria e registro de dados em redes computacionais;

4.4. Participar da elaboração de planos de continuidade;

4.5. Analisar tecnicamente e monitorar incidentes de segurança da informação;

4.6. Realizar testes e verificações em sistemas e serviços de redes computacionais;

4.7. Participar de investigações de incidentes de segurança da informação; e

4.8. Identificar e avaliar os riscos decorrentes da implementação de mudanças no ambiente computacional.

5. Atuação

Serão submetidas à aprovação do CGSI as ações a serem tomadas em face de incidente ou ameaça de segurança que possa afetar a imagem institucional ou a confidencialidade das informações do Tribunal.

ANEXO II
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 2
GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TIC

1. Objetivos

1.1. Estabelecer diretrizes para o processo de Gestão de Continuidade de Serviços de TIC deste Tribunal; e

1.2. Mitigar o risco causado por interrupções dos serviços e sistemas de TIC que suportam as atividades críticas deste Tribunal.

2. Referências normativas

2.1. Norma Complementar n. 06/IN01, de 11 de novembro de 2009, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), que estabelece diretrizes para gestão de continuidade de negócios, nos aspectos relacionados à Segurança da Informação e Comunicação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

2.2. 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;

2.3. 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; e

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

3. Conceitos e definições

3.1. Atividades Críticas: devem ser realizadas de forma que garantam a consecução dos produtos e serviços fundamentais do órgão ou entidade, visando atingir seus objetivos mais importantes e sensíveis ao tempo;

3.2. Gestão de Continuidade: processo de gestão que identifica ameaças potenciais para a organização e seus possíveis impactos nas operações de negócio, visando ao desenvolvimento de resiliência organizacional, capaz de responder e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

salvaguardar os interesses das partes interessadas, a reputação da instituição, a marca da organização e suas atividades de valor agregado;

3.3. Gestão de Continuidade de TIC: processo que visa a mitigar o risco causado por interrupções dos serviços e sistemas de TIC que suportam as atividades essenciais da organização, especialmente no que se refere aos serviços judiciais; e

3.4. Plano de Continuidade de TIC: documento em que são registrados os procedimentos a serem realizados em cenários de falhas nos serviços essenciais de TIC, visando à sua continuidade e ao restabelecimento da normalidade.

4. Diretrizes

4.1. Elaborar estratégias e definir procedimentos para manter os sistemas e serviços críticos de TIC em um nível operacional aceitável durante a ocorrência de um desastre, visando a não se interromper a prestação jurisdicional;

4.2. Identificar dependências e recursos que suportam as atividades jurisdicionais, incluindo fornecedores, terceiros e demais partes interessadas relevantes;

4.3. Observar o resultado das análises de riscos de TIC e da análise de impacto de negócio realizado (negócio realizado ou análise realizada?), visando a nortear as estratégias de continuidade;

4.4. Documentar no Plano de Continuidade de TIC a estratégia e os procedimentos necessários à operação de contingência e as comunicações apropriadas em caso de interrupções dos serviços e sistemas essenciais de TIC; e

4.5. Revisar o Plano de Continuidade de TIC após mudanças na infraestrutura ou em razão do resultado de testes.

5. Responsabilidades

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

5.1. Compete à Secretaria de Infraestrutura Tecnológica (SEIT), com o apoio das Secretarias de Sistemas (SESIS) e de Suporte e Atendimento (SESA), a elaboração e implementação do Plano de Continuidade de Serviços de TIC; e

5.2. Cabe à SINC monitorar e analisar a Gestão de Continuidade de Serviços de TIC, reportar os resultados ao CGSI e propor, quando for o caso, melhorias e correções.

6. Etapas da Gestão de Continuidade

6.1. Planejamento: delimitação do escopo do plano de continuidade, com estipulação dos processos críticos para o negócio, a fim de estabelecer atividades de TIC e ativos de informação essenciais para a prestação jurisdicional, identificar os que devem ser tratados e indicar as estratégias empregadas durante a ocorrência de um incidente;

6.2. Implementação: elaboração ou revisão do Plano de Continuidade de TIC pelas equipes técnicas, com descrição dos cenários de falhas e dos procedimentos técnicos para lidar com os problemas, realização de testes (cumprimento parcial ou integral dos procedimentos) e aprovação, armazenamento e divulgação dos planos;

6.3. Verificação: realização de testes do Plano de Continuidade de TIC desenvolvido e análise dos incidentes críticos ocorridos (desastres); e

6.4. Melhoria: identificação das oportunidades de melhoria e divulgação, a fim de dar início a novo ciclo do processo.

ANEXO III
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 3
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. Objetivos

1.1. Estabelecer diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico deste Tribunal; e

1.2. Assegurar a identificação, o registro e a avaliação em tempo hábil dos incidentes de segurança da informação, com a tomada de medidas de contenção ou a entrega de solução adequada.

2. Referências normativas

2.1. Norma Complementar n. 01/IN01, de 15 de outubro de 2008, do DSIC/GSIPR, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da APF, direta e indireta;

2.2. Norma Complementar n. 05/IN01, de 14 de agosto de 2009, do DSIC/GSIPR, que disciplina a criação de ETIR nos órgãos e entidades da APF;

2.3. Norma Complementar n. 08/IN01, de 14 de agosto de 2010, do DSIC/GSIPR, que disciplina o gerenciamento de incidentes de segurança em redes de computadores realizado pelas ETIRs dos órgãos e entidades da APF;

2.4. 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 do contexto da organização;

2.5. 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; e

2.6. Norma Complementar n. 21/IN01, de 8 de outubro de 2014, do DSIC/GSIPR, que estabelece as diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes computacionais nos órgãos e entidades da APF.

3. Conceitos e definições

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

3.1. Artefato malicioso: 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 ou redes de computadores;

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

3.3. 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 controle, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

3.4. Incidente de segurança da informação: um ou uma série de eventos de segurança da informação, indesejados ou inesperados, que possam prejudicar as operações do negócio e ameaçar a segurança da informação;

3.5. Tratamento de Incidentes de Segurança em Redes Computacionais: consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, visando a extrair informações que impeçam a continuidade da ação maliciosa e também identificar tendências; e

3.6. Vulnerabilidade: fragilidade de um ativo de informação ou de um controle, que possibilite a ocorrência de uma ameaça, como a exploração maliciosa ou o acesso indesejável ou não autorizado a sistemas ou redes de computadores.

4. Escopo

A Gestão de Incidentes de Segurança da Informação tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC, que suportam os principais processos de negócio deste Tribunal.

5. Diretrizes

Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

ambiente tecnológico do Tribunal, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a POSICTRT3, dos quais decorram interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações ou ato definido como crime ou infração administrativa.

6. Processo de Gestão de Incidentes de Segurança da Informação

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

6.1.1. Detecção e registro: compreende a detecção, recebimento, registro e autorizações necessárias para o encaminhamento da investigação;

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

6.1.3. Encerramento: compreende a análise do incidente quando é verificada eventual necessidade de outras ações, providências ou comunicações e, na sequência, o seu encerramento propriamente dito;

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

6.2. Os incidentes, notificados ou detectados, serão registrados, a fim de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7. Responsabilidades

7.1. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, no Portal CSTI, pelo **link** Atendimento ao Usuário, no endereço eletrônico <https://portal.trt3.jus.br/internet/tec-informacao> ou diretamente à SINC, por telefone ou pelo **e-mail** sinc@trt3.jus.br.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

7.2. As equipes DTIC responsáveis pelo monitoramento dos ativos, serviços e sistemas notificarão a ocorrência de incidentes à SINC, para registro e encaminhamento.

7.3. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da POSIC-TRT3, será observado o sigilo durante todo o processo (inserir aqui o fundamento legal para a colocação sob sigilo), ficando as evidências, informações e os demais registros restritos aos envolvidos na investigação.

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

ANEXO IV
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 4
GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Estabelecer as diretrizes para o processo de gestão de riscos de segurança da informação.

2. Escopo

2.1. Esta norma tem como escopo ações de segurança da informação direcionadas às medidas de proteção dos ativos de informação, independentemente do meio ou da tecnologia utilizados; e

2.2 O gerenciamento de riscos em projetos e os riscos das contratações de TIC observarão o disposto na metodologia adotada no Tribunal.

3. Referências normativas

3.1. Norma ABNT NBR ISO/IEC 27005:2008 (Tecnologia da Informação Técnicas de segurança Gestão de riscos de segurança da informação);

3.2. Norma Complementar n. 04/IN01 (Revisão 01), de 15 de fevereiro de 2013, do DSIC/GSIPR, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações GRSIC nos órgãos ou entidades da APF, direta e indireta; e

3.3. Resolução GP n. 71, de 17 de março de 2017, que institui a Política de Gestão de Riscos do Tribunal Regional do Trabalho da 3ª Região; e

3.4. Norma ABNT NBR ISO/IEC 31000:2018 (Gestão de riscos Princípios e diretrizes).

4. Conceitos e definições

4.1. Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;

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

4.3. Vulnerabilidade: fragilidade de um ativo de informação ou de um controle, que possibilite a ocorrência de uma ameaça, como a exploração maliciosa ou o acesso indesejável ou não autorizado a sistemas ou redes de computadores; e

4.4. Riscos de Segurança da Informação: probabilidade associada à exploração de uma ou mais vulnerabilidades de um ativo de informação e suas consequências.

5. Diretrizes

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

5.1. A Gestão de Riscos de Segurança da Informação deve estar alinhada à Gestão de Riscos Corporativa, ao Planejamento Estratégico Institucional, ao Planejamento Estratégico de TIC e à POSIC-TRT3;

5.2. Os riscos serão analisados e avaliados em função da relevância para os principais processos de negócio deste Tribunal e tratados de forma que assegurem respostas tempestivas e efetivas;

5.3. 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;

5.4. A SINC encaminhará as principais vulnerabilidades identificadas nos ativos tecnológicos para análise de riscos pelas áreas técnicas responsáveis;

5.5. Os planos de tratamento de riscos de segurança da informação e de vulnerabilidades de TIC serão apresentados ao GCTIC; e

5.6. Os indicadores e resultados do tratamento de riscos serão apreciados pelo CGSI.

6. Processo de Gestão de Riscos e Vulnerabilidades de Segurança da Informação

6.1. O processo de Gestão de Riscos de Segurança da Informação conterá, no mínimo, as seguintes fases:

6.1.1. Contextualização: na qual se define o contexto da análise e a avaliação de riscos a ser realizada, com a identificação de seu escopo, limites e partes interessadas;

6.1.2. Análise e avaliação do risco: na qual se estima o nível do risco, considerando a probabilidade e o impacto, a fim de elaborar o plano de tratamento dos riscos;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

6.1.3. Tratamento do risco: na qual são implementadas ações do plano de tratamento dos riscos;

6.1.4. Monitoramento e revisão: na qual se monitoram a realização dos planos de tratamento dos riscos, os próprios riscos e as atividades de gestão, e são feitos ajustes, se necessários; e

6.1.5. Comunicação e consulta: na qual é estabelecida e mantida a comunicação com partes interessadas, para informá-las ou consultá-las.

6.2. São definidos os seguintes papéis para o processo:

6.2.1. CGSI: aprecia os planos de tratamento de riscos, os indicadores e os relatórios gerenciais;

6.2.2. CGTIC: prioriza, aprova e acompanha a evolução dos planos de tratamento de riscos;

6.2.3. SINC: unidade gestora do processo, que condensa métricas e indicadores, identifica e consolida vulnerabilidades e interage com todos;

6.2.4. Líder de projeto: estabelece o contexto do projeto e monitora a análise e o tratamento dos riscos;

6.2.5. Equipe de avaliação de riscos: identifica os ativos e realiza a avaliação de riscos; e

6.2.6. Responsável pelo ativo: analisa os riscos e implementa ações para o tratamento deles.

ANEXO V

(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

NORMA COMPLEMENTAR N. 5
USO DE RECURSOS DE TIC E CONTROLE DE ACESSO

1. Objetivos

1.1. Estabelecer diretrizes e padrões para a utilização dos recursos de TIC e para o controle de acesso, no Tribunal; e

1.2. Garantir que os acessos aos recursos tecnológicos sejam feitos de forma adequada e controlada, visando à segurança e à continuidade das atividades deste Tribunal.

2. Referências normativas

2.1. 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;

2.2. Norma Complementar n. 07/IN01, Revisão 01, de 15 de julho de 2014, do DSIC/GSIPR, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da APF; e

2.3. Norma Complementar n. 14/IN01, Revisão 01, de 13 de março de 2018, do DSIC/GSIPR, que estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3. Conceitos e definições

3.1. Rede cabeada: acesso aos recursos tecnológicos e à transmissão de dados pela utilização de meios físicos (ativos de distribuição de dados, cabos e pontos de rede); e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

3.2. Rede lógica: 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 a essa rede.

4. Uso de recursos de TIC

4.1. Diretrizes gerais

4.1.1. O uso adequado dos recursos de TIC visa a garantir a continuidade das atividades desenvolvidas neste Tribunal;

4.1.2. Os recursos de TIC disponibilizados pelo Tribunal aos usuários serão utilizados em atividades relacionadas às funções institucionais;

4.1.3. Os procedimentos de instalação, configuração e manutenção de equipamentos e **softwares** serão realizados pela DTIC 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;

4.1.4. Não será fornecido suporte a equipamentos particulares (computadores, **notebooks**, **smartphones** e **tablets**), seja quanto à instalação e configuração de sistemas ou aplicativos, seja quanto à conexão à rede sem fio; e

4.1.5. Os equipamentos de TIC em período de garantia somente podem ser abertos pelo fornecedor contratado pelo Tribunal.

4.2. Responsabilidades do usuário

4.2.1. Zelar pela integridade e conservação dos recursos de TIC disponibilizados para o exercício de suas atribuições;

4.2.2. Preservar o sigilo de sua senha ou outro mecanismo de autenticação utilizado para acesso aos recursos tecnológicos disponibilizados; e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

4.2.3. Preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados.

4.3. Da Rede Lógica

4.3.1. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do Tribunal serão monitorados, por questões de segurança e para fins de auditoria;

4.3.2. A cada ponto de acesso à rede de dados do Tribunal poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da DTIC;

4.3.3. É vedado aos usuários conectar dispositivos não institucionais na rede cabeada do Tribunal, salvo quando autorizados pela DTIC, após homologação da SESA;

4.3.4. O acesso à rede sem fio, quando disponível para usuários internos e externos, será realizado mediante cadastramento prévio em sistema específico disponível no portal do Tribunal;

4.3.4.1. Por questões de segurança tecnológica, filtros e regras poderão ser implementados no acesso à internet via rede sem fio; e

4.3.4.2. Serão bloqueados, temporariamente ou por prazo indeterminado, os acessos à rede sem fio de dispositivo móvel identificado, durante o monitoramento, como fonte de ação maliciosa intencional ou não, ou no qual tenha sido detectada vulnerabilidade ou problema de segurança tecnológica; e

4.3.5. Cada unidade do Tribunal 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;

4.3.5.1. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas no item 4.3.5, cabendo aos

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

usuários providenciar cópia de segurança e eliminação periódica dos arquivos armazenados nos discos rígidos locais;

4.3.5.2. É proibido o armazenamento, em qualquer diretório na rede do Tribunal ou nas soluções baseadas em nuvem corporativa, de arquivos não relacionados ao trabalho; e

4.3.5.3. O usuário deve evitar a manutenção de mais de uma cópia por arquivo e, periodicamente, eliminar os desnecessários.

4.4. Das competências da DTIC e secretarias subordinadas

4.4.1. Conectar recursos de TIC à rede do Tribunal;

4.4.2. Avaliar a compatibilidade de novas soluções que envolvam TIC com a infraestrutura existente e calcular as implicações quanto à segurança da informação; e

4.4.3. Verificar a justificação técnica para a contratação de recursos de TIC.

4.5. Equipamentos fornecidos pelo Tribunal

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

4.5.2. Os problemas de **software** serão solucionados por reinstalação padrão desenvolvida pelo Tribunal;

4.5.3. O Tribunal não se responsabiliza por reinstalar e configurar programas instalados pelo usuário sem autorização, nem pela perda de dados nessa hipótese; e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

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

4.6. Licenças de software

4.6.1. As licenças de **softwares**, contratadas ou adquiridas, são de uso privativo deste Tribunal;

4.6.2. O Tribunal utilizará em suas atividades, preferencialmente, **software** livre ou de código aberto;

4.6.3. Fica definida como padrão a suíte de escritório **LibreOffice**, salvo comprovada necessidade de uso de solução diversa;

4.6.4. O padrão de **softwares** utilizáveis pelo Tribunal será indicado no Catálogo de Serviços de TIC, disponível no Portal CSTI, na aba Sistemas, na intranet; e

4.6.5. É proibida a instalação de **softwares** não licenciados ou não homologados pela DTIC nos equipamentos conectados à rede do Tribunal;

4.6.5.1. A instalação de **softwares** não homologados poderá ser autorizada excepcionalmente pelo CGSI, desde que demonstrada a necessidade de utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança e proteção estabelecidas, bem como compatibilidade e adequação aos recursos computacionais disponibilizados pelo Tribunal;

4.6.5.2. As unidades organizacionais do Tribunal poderão encaminhar à DTIC pedido de homologação de **softwares**, para uso em suas atividades;

4.6.5.3. Homologado o uso, o **software** passará a integrar o Catálogo de Serviços de TIC; e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

4.6.5.4. A inobservância do item 4.6.5 poderá ensejar a desinstalação compulsória da solução de TIC não homologada ou não licenciada, mediante comunicação prévia.

5. Do controle e gerenciamento de acesso

5.1. O acesso à rede, aos serviços e aos sistemas computacionais disponibilizados pelo Tribunal será solicitado no Portal CSTI, pelo **link** Atendimento ao Usuário, no endereço eletrônico <https://portal.trt3.jus.br/internet/tec-informacao>;

5.2. Incumbe à chefia imediata solicitar no Portal CSTI, pelo **link** descrito no item 5.1:

5.2.1. Acessos necessários ao desenvolvimento das atividades dos usuários vinculados à sua unidade;

5.2.2. Alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a usuários lotados em sua unidade, sempre que necessária adequação às atividades desenvolvidas; e

5.2.3. Remoção dos acessos concedidos ao usuário, imediatamente após o seu afastamento ou desligamento da unidade;

5.3. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido a informações da unidade;

5.4. A Secretaria-Geral da Presidência (SEGP) e a Diretoria de Gestão de Pessoas (DGP), no âmbito de suas competências, comunicarão à SESA os casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção e cessão a outro órgão, retorno à origem ou término do estágio de estudantes, para remoção dos acessos concedidos aos usuários;

5.5. Os usuários aposentados, cedidos ou removidos terão acesso aos serviços administrativos via extranet;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

5.6. O privilégio de administrador na estação de trabalho é restrito aos membros de equipe técnica de TI que necessitem desse nível de acesso para o desempenho de suas atividades funcionais; e

5.7. Os acessos concedidos serão revisados pelo menos uma vez por ano pelos gestores.

6. Da conta de rede e respectiva senha para utilização

6.1. Para obter acesso aos recursos de TI disponibilizados pelo Tribunal, é necessário que o usuário possua credencial de acesso à rede;

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

6.3. 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, para impedir o uso não autorizado dos recursos de TI por meio de sua conta de acesso:

6.3.1. Não compartilhar a senha com outras pessoas;

6.3.2. Não armazenar senhas em local acessível por terceiros;

6.3.3. Não utilizar senhas de fácil dedução, como as que contenham nomes próprios e de familiares, datas festivas e sequências numéricas; e

6.3.4. Ao ausentar-se de sua estação de trabalho, o usuário deverá bloquear ou encerrar a sessão;

6.4. Recomenda-se que a senha de identificação seja alterada a cada 180 dias e satisfaça os seguintes requisitos de segurança:

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

6.4.1. Não conter a sequência dos caracteres de identificação da conta do usuário (**login**);

6.4.2. Não ser mera reprodução da última senha utilizada pelo usuário;

6.4.3. Ter pelo menos oito caracteres; e

6.4.4. Ser composta por letras maiúsculas e minúsculas e por números; e

6.5. Em caso de suspeita de violação da senha ou de outro recurso de autenticação, o usuário deverá acessar imediatamente o Portal CSTI, pelo **link** descrito no item 5.1, para comunicar o incidente à CSTI, que adotará os procedimentos cabíveis.

7. Registros (log) de Eventos

7.1. Serão mantidos, por um período mínimo de seis meses, os registros dos acessos dos usuários e dos acessos privilegiados aos recursos tecnológicos disponibilizados pelo Tribunal, inclusive para fins de apuração e comprovação de incidentes de segurança; e

7.2. Serão registrados, no mínimo, os seguintes dados:

7.2.1. Identificação de usuário que efetuou o acesso;

7.2.2. Data e hora de entrada e saída do sistema;

7.2.3. Origem do acesso;

7.2.4. Erros ou falhas de conexão e acesso; e

7.2.5. Troca de senhas de serviços de infraestrutura de TI.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

ANEXO VI
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 6
GESTÃO DE ATIVOS DA INFORMAÇÃO

1. Objetivo

Disciplinar o processo de gestão de ativos de informação e a definição de responsabilidades apropriadas para proteção desses ativos, quanto à segurança da informação.

2. Referências normativas

2.1. Norma Complementar n. 10/IN01, de 30 de janeiro de 2012, do DSIC/GSIPR, que estabelece diretrizes para o processo de inventário e mapeamento de ativos de informação nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta APF; e

2.2. 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. Conceitos e definições

Ativos de informação: sistemas de informação, meios de armazenamento, transmissão e processamento, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. Precisa repetir o que já está conceituado mais acima?

4. Diretrizes

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

4.1. O processo de gestão de ativos de informação visa à proteção dos ativos críticos do Tribunal e serve de subsídio para a Gestão de Riscos e de continuidade de serviços essenciais de TIC;

4.2. Os ativos de informação devem ser identificados para implementação de controles de segurança adequados e compatíveis com o nível de criticidade e relevância; e

4.3. Na identificação dos ativos tecnológicos, constará, no mínimo, descrição, configurações de **hardware**, versões de **software**, localização, relevância, considerando os serviços e sistemas que eles suportam, responsáveis, proprietários e custodiantes.

5. Processo de gestão de ativos

5.1. Identificação e classificação de ativos de informação quanto à relevância para o Tribunal;

5.2. Identificação de ameaças e vulnerabilidades; e

5.3. Avaliação de riscos.

6. Responsabilidades

6.1. O CGSI definirá o escopo de execução do processo de gestão de ativos de informação;

6.2. A SINC será a guardiã do processo de gestão de ativos;

6.3. O responsável pelo ativo de informação indicará seu valor para o negócio do Tribunal, considerando os processos da cadeia de valor e critérios definidos pelo CGSI; e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

6.4. Os ativos de TIC serão inventariados no processo de gerenciamento e configuração de ativos pelas unidades custodiantes abaixo identificadas:

6.4.1. SEIT: responsável pelo controle de equipamentos e soluções de infraestrutura, bem como pelos **softwares** necessários ao desenvolvimento de suas atividades;

6.4.2. SESA: responsável pelo controle de equipamentos de microinformática, de **softwares** destinados aos usuários em geral, bem como de **softwares** necessários ao desenvolvimento de suas atividades; e

6.4.3. SESIS: responsável pelo controle de **softwares** e sistemas desenvolvidos pelo Tribunal ou cedidos por outros órgãos públicos, bem como pelo controle de **softwares** necessários ao desenvolvimento de suas atividades.

ANEXO VII
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 7
DO SERVIÇO DE CORREIO ELETRÔNICO INSTITUCIONAL

1. Objetivo

Estabelecer diretrizes para a utilização do serviço de correio eletrônico institucional.

2. Conceitos e definições

2.1. Correio eletrônico institucional: serviço corporativo de envio e recebimento de mensagens eletrônicas (**e-mails**), oferecido pelo Tribunal, cujo domínio é trt3.jus.br;

2.2. Caixa postal institucional pessoal: conta de correio eletrônico de um único usuário (magistrado ou servidor);

2.3. Caixa postal institucional da unidade: conta de correio eletrônico de unidade administrativa ou judiciária constante da estrutura organizacional do Tribunal;

2.4. Caixa postal institucional de serviço: conta de correio eletrônico temporária concedida a comissões, grupos de trabalho e programas formalmente constituídos, ainda que não constantes na estrutura organizacional do Tribunal;

2.5. Lista de distribuição: agrupamento de diversos endereços eletrônicos, que permite a distribuição conjunta de mensagem eletrônica a todos os seus integrantes, sem caixa postal específica;

2.6. **Spam**: mensagem de publicidade enviada em massa, sem consentimento prévio do destinatário;

2.7. **Phishing**: mensagem fraudulenta, com o objetivo de subtrair informações de seu destinatário; e

2.8. **Hoax**: mensagens dramáticas ou alarmantes com propagação de boatos ou informações distorcidas.

3. Diretrizes

3.1. Todo magistrado e servidor terá uma caixa postal institucional pessoal para recebimento e envio de comunicações institucionais, sendo obrigatória a utilização no exercício da função;

3.2. A caixa postal institucional pessoal de magistrados ou servidores removidos, cedidos, redistribuídos, retornados à origem, exonerados, aposentados ou falecidos será excluída, definitivamente, em 30 dias, a contar da comunicação da SEGP ou da DGP à CSTI, nos termos do item 4.2;

3.3. Na hipótese do item 3.2, o aposentado ou o seu representante informará conta de **e-mail** pessoal para recebimento de informações funcionais;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

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

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

3.5.1. Informação privilegiada, confidencial ou de propriedade do Tribunal, para destinatário não autorizado;

3.5.2. Material obsceno, ilegal ou antiético;

3.5.3. Material preconceituoso ou discriminatório;

3.5.4. Material calunioso ou difamatório;

3.5.5. Propaganda com objetivo comercial;

3.5.6. Listagem com endereços eletrônicos institucionais, para destinatário não autorizado;

3.5.7. Material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;

3.5.8. Material protegido por lei de propriedade intelectual;

3.5.9. Material de entretenimento e correntes;

3.5.10. Assunto ofensivo;

3.5.11. Música, vídeo ou animação não relacionada ao trabalho; e

3.5.12. **Spam**, **phishing** e **hoax**;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

3.6. O recebimento de mensagem que contrarie o item 3.5 será informado à SINC, por meio da abertura de chamado no Portal CSTI, pelo **link** Atendimento ao Usuário, no endereço eletrônico <https://portal.trt3.jus.br/internet/tec-informacao>;

3.7. Somente serão criadas as seguintes caixas postais de correio eletrônico:

3.7.1. Caixa postal institucional pessoal;

3.7.2. Caixa postal institucional da unidade;

3.7.3. Caixa postal institucional de serviço; e

3.7.4. Listas de distribuição;

3.8. O identificador do endereço de correio eletrônico poderá, em caso de duplicidade, ser formado por um dos nomes do usuário seguido por um dos sobrenomes, separados pelo sinal de ponto; e

3.9. As unidades administrativas e judiciárias presentes na estrutura organizacional do Tribunal poderão ter caixa postal institucional da unidade (item 2.3), cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.

4. Responsabilidades

4.1. É de responsabilidade do usuário:

4.1.1. Utilizar o correio eletrônico institucional de acordo com os preceitos desta Resolução;

4.1.2. Gerenciar o armazenamento de mensagens da caixa postal; e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

4.1.3. Acessar a conta institucional pessoal de correio eletrônico periodicamente, no mínimo uma vez por semana, para fins do disposto no item 3.1, salvo em caso de afastamento (férias, licença médica, entre outros);

4.2. As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas através do Portal CSTI, pelo **link** descrito no item 3.6;

4.3. A solicitação de caixa postal institucional pessoal para magistrado incumbe à SEGP e, para servidor, à DGP;

4.4. Cabe ao gestor de unidade administrativa ou judiciária:

4.4.1. Solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade;

4.4.2. Autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como providenciar a exclusão desse acesso; e

4.4.3. Solicitar a criação de listas de **e-mail** com a devida justificativa e tempo de utilização (provisória ou permanente);

4.5. A DTIC armazenará os arquivos de registro de mensagens eletrônicas (**logs**) pelo período mínimo de seis meses; e

4.6. Os casos omissos serão submetidos ao CGSI.

ANEXO VIII
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 8
CONTROLE DE ACESSO À INTERNET

1. Objetivo

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

Estabelecer diretrizes para a utilização do serviço de internet no Tribunal.

2. Conceitos e definições

2.1. Credencial: identificação do usuário (**login**); e

2.2. **Proxy**: sistema que viabiliza a navegação na internet.

3. Diretrizes

3.1. O acesso à internet ocorrerá, exclusivamente, pelos meios autorizados, configurados pela DTIC;

3.2. É proibido o uso de **proxies** externos ou similares;

3.3. A credencial para acesso à rede do Tribunal é a mesma do acesso à internet;

3.4. Constituem uso indevido do serviço de acesso à internet as seguintes ações:

3.4.1. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a POSIC-TRT3; ou

3.4.2. Vazar informações;

3.5. Por motivos de segurança, será monitorado todo acesso à internet, cujos registros serão mantidos pelo período mínimo de seis meses;

3.6. Comprovada utilização irregular da internet, o usuário terá o acesso bloqueado, e o fato será comunicado à chefia imediata e, conforme a gravidade, também à Administração do Tribunal, para que sejam tomadas as providências cabíveis; e

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

3.7. No caso de prática da ação mencionada no item 3.4.2, o usuário ficará sujeito à responsabilização pelos danos de qualquer natureza provocados.

4. Responsabilidades

4.1. Compete ao gestor da unidade:

4.1.1. Solicitar à CSTI, por meio de seu Portal, a liberação de acesso a **sites** e a serviços não autorizados, mas necessários ao desempenho das atribuições funcionais do usuário; e

4.1.2. Solicitar a realização de auditoria quando constatados indícios de incidentes de segurança; e

4.2. Os casos omissos serão submetidos ao CGSI.

ANEXO IX
(art. 18 da Resolução GP n. 134, 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 9
PROCEDIMENTOS DE BACKUP E RECUPERAÇÃO DE DADOS

1. Objetivo

Estabelecer diretrizes para a manutenção e restauração de cópias de segurança de dados e assegurar a continuidade das atividades deste Tribunal, mesmo se perda, falha ou desastre incidirem sobre os dados informatizados.

2. Conceitos e definições

2.1. Cópia de segurança de dados ou **backup**: cópia dos dados de um dispositivo de armazenamento para outro, para que possam ser restaurados os originais, em caso de evento repentino e não planejado que coloque em risco, danifique ativo de informação deste Tribunal ou suspenda atividade ou serviço essencial;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

2.2. Mídia: meio físico, magnético ou óptico, em que se armazenam dados ou **backup** de dados;

2.3. Retenção: prazo pelo qual o conteúdo da mídia de **backup** deve ser preservado, a fim de que possam ser recuperados os dados nela contidos;

2.4. Recuperação de cópia de segurança: ato de recuperar dados previamente armazenados em mídia de **backup**;

2.5. Servidor de **backup**: equipamento servidor que executa o **software** de gerenciamento de **backups**;

2.6. Versão de arquivos: cópia gerada pelo servidor de **backup** no instante em que é constatada criação, alteração ou deleção de dado de arquivo;

2.7. **Recovery Point Objective** (RPO): tempo que um dado permanece desprotegido desde a última cópia de segurança, ou seja, período máximo aceitável de exposição dos dados a perda definitiva;

2.8. **Recovery Time Objective** (RTO): tempo estimado para recuperar os dados ou tornar os respectivos sistemas disponíveis; e

2.9. **Log** ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional.

3. Diretrizes

3.1. Serão efetuadas, periodicamente, de forma automatizada, cópias de segurança das informações corporativas mantidas nos servidores, sistemas e banco de dados geridos pela DTIC;

3.2. A cópia de segurança será executada, preferencialmente, em horário diverso do de funcionamento do Tribunal;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

3.3. Quando ocorrer falha, o processo de cópia de segurança será reiniciado para salvaguardar a política de retenção, sempre que possível;

3.4. As mídias de armazenamento de cópia de segurança serão copiadas e mantidas em centro de processamento de dados em Belo Horizonte (Capital), onde poderão ser acessadas por pessoas autorizadas;

3.5. As mídias de armazenamento de cópia de segurança serão identificadas por etiqueta, inventariadas e testadas periodicamente quanto à usabilidade;

3.6. A cópia de segurança que deixar de ser útil terá os dados e identificação apagados, inutilizado o meio de armazenamento, e será descartada;

3.7. A periodicidade de execução da cópia de segurança, o tempo de sua retenção, o RPO e o RTO variam de acordo com o tipo de dado armazenado no servidor, conforme definido nos Quadros I e II deste Anexo;

3.8. A equipe responsável pelo gerenciamento de **backup** fará testes de recuperação, observados os critérios mínimos indicados no Quadro III deste Anexo; e

3.9. Os incidentes contrários a disposições desta Norma Complementar serão registrados na Central de Serviços da DTIC, que os encaminhará à SINC, para que sejam tomadas as providências cabíveis.

4. Responsabilidades

4.1. Compete ao usuário:

4.1.1. A guarda e a conservação de informações armazenadas em estações de trabalho ou **notebooks**; e

4.1.2. Solicitar a recuperação de cópia de segurança no Portal CSTI, pelo **link** Atendimento ao Usuário, no endereço eletrônico <https://portal.trt3.jus.br/internet/tec-informacao>;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

4.2. Na solicitação, o requerente informará o nome da pasta ou arquivo, o último local de armazenamento e a data da deleção ou alteração;

4.3. Compete ao Administrador do **backup** acompanhar diariamente os registros de sucesso ou de falha no processo de cópia de segurança de dados e armazenar os **logs** por, no mínimo, 180 dias, para fins de auditoria; e

4.4. Os casos omissos serão submetidos ao CGSI.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

Quadro I
Política de backup geral

Servidores de Arquivos (**Linux** e **Windows**)
Capital
Interior
Backup Diário
Retenção
90 dias
90 dias

Dias e horários
De segunda a sexta-feira
Alguns servidores também no domingo
Início: às 19 horas
De segunda a sexta-feira e domingo
Início: às 23 horas
RPO (tempo máximo de perda dos dados)
24 horas
24 horas
RTO (tempo estimado para restauração)
360 GB/h de dados
360 GB/h de dados

Banco de dados **Oracle**
Produção
Homologação
Desenvolvimento
Backup Completo Semanal
Periodicidade e horário de execução
Sábado / A partir das 2 horas

Backup incremental diário
Retenção
28 dias
14 dias
14 dias

Periodicidade e horário de execução
Diária / Às 2 horas
Diária / Às 20 horas

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

Diária / Às 20 horas
RPO (tempo máximo de perda dos dados)
Do ponto de vista do **backup**: 1 hora
Do ponto de vista da réplica: 0
24 horas
24 horas
RTO (tempo estimado para restauração)

360 GB/h de dados
360 GB/h de dados
360 GB/h de dados

Quadro II
Política de backup do Pje

PJe Servidores Jboss e **WEB**
Capital e Interior
Backup diário
Retenção
180 dias para arquivos de **log** de todos os servidores
90 dias para o **filesystem** de alguns servidores

Dias e horários
De segunda-feira a domingo
Início: às 23 horas
RPO (tempo máximo de perda dos dados)
24 horas
RTO (tempo estimado para restauração)

360 GB/h de dados

PJe Servidores Banco de Dados
Capital e Interior
Backup diário
Retenção
Produção: 28 dias
Homologação: 7 dias

Dias e horários
De segunda a sexta-feira

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.

Produção Início: às 18 horas
Homologação Início: às 22 horas
RPO (tempo máximo de perda dos dados)
Do ponto de vista do **backup**: 1 hora
Do ponto de vista da réplica: 0
RTO (tempo estimado para restauração)

360 GB/h de dados

Quadro III
Periodicidade de testes de recuperação de backup

Grupo de **Backup**
Equipe de Recuperação
Periodicidade
Recuperação
Equipe de Validação
Validação
Banco de dados **Postgres** PJe
Equipe de **backup** / DBA
Teste Bimestral
Recupera-se a última versão
Equipe de **backup** / DBA
Inicializa-se o banco de dados
Banco de dados **Oracle**
Equipe de **backup** / DBA
Teste Bimestral
Recupera-se a última versão
Equipe de **backup** / DBA
Inicializa-se o banco de dados

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 134, de 19 de dezembro de 2019. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2877, 20 dez. 2019. Caderno Administrativo, p. 3-23.