



RESOLUÇÃO ADMINISTRATIVA TRT5 Nº 042, DE 28 DE JULHO DE 2014 *

Atualiza a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 5ª Região.

O ÓRGÃO ESPECIAL DO TRIBUNAL REGIONAL DO TRABALHO DA QUINTA REGIÃO, reunido em sua 6ª Sessão Extraordinária, realizada no dia 28 de julho de 2014, no uso de suas atribuições legais e regimentais, tendo como Presidente o Ex.^{mo} Sr. Desembargador **Valtércio de Oliveira**, com a presença do Representante do Ministério Público do Trabalho, Ex.^{mo} Sr. Procurador **Alberto Balazeiro**, e dos Ex.^{mos} Srs. Desembargadores **Paulino Couto, Ana Lúcia Bezerra, Vânia Chaves, Graça Laranjeira, Alcino Felizola, Débora Machado, Marizete Menezes, Edilton Meireles, Léa Nunes, Esequias de Oliveira, Dalila Andrade e Renato Simões**;

CONSIDERANDO as informações constantes da Matéria Administrativa nº 09.54.14.04841-35;

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 necessidade de manter sempre atualizada sua Política de Segurança da Informação;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade,

RESOLVE, por unanimidade:

Art. 1º Atualizar a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 5ª Região – TRT5 definida pela Resolução Administrativa TRT5 023/2011, que passa a vigorar conforme as definições desta Resolução.



Parágrafo único. Todos os atos, normas e procedimentos complementares em vigor e que vierem a ser publicados com aprovação do Comitê de Segurança da Informação tornam-se parte integrante desta Política de Segurança da Informação.

Art. 2º Para os efeitos desta Resolução aplicam-se as seguintes definições:

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

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

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

IV – Segurança da informação: conservação da integridade, confidencialidade e disponibilidade da informação; adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas;

V – Ativo: qualquer coisa que tenha valor para uma organização.

VI – Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

VII – Usuários: todas as pessoas que façam uso dos recursos de tecnologia da informação do TRT5 incluindo 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, operadores do direito, e outras pessoas que recebam permissão de acesso aos recursos tecnológicos do TRT5 em caráter temporário ou permanente;

VIII – Sistema de Gestão de Segurança da Informação (SGSI): a parte do sistema de gestão global de uma organização, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;

IX – Plano de Continuidade do Negócio: conjunto de ações e procedimentos documentados que guiam uma organização para responder, recuperar,



retomar e restaurar a um nível pré-definido de operação após um incidente que causou a interrupção de operação.

Art. 3º As disposições desta Resolução aplicam-se a todos os usuários de recursos de tecnologia da informação do TRT5.

Art. 4º O uso adequado dos recursos de tecnologia da informação visa garantir a continuidade da prestação jurisdicional deste TRT5.

§ 1º Os recursos de tecnologia da informação pertencentes ao TRT5, disponíveis para o usuário, serão utilizados em atividades estritamente relacionadas às suas funções institucionais.

§ 2º A utilização dos recursos de tecnologia da informação será monitorada, sendo seus registros mantidos pela Secretaria de Tecnologia da Informação e Comunicações – SETIC.

Art. 5º As informações geradas no âmbito deste Tribunal são de sua propriedade, independentemente da forma de sua apresentação ou armazenamento, e serão adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades desenvolvidas neste Tribunal.

§ 1º Toda informação gerada no Tribunal deverá ser classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

§ 2º 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. 6º Fica estabelecido o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO DO TRT5 – SGSI5. O SGSI5 é um processo organizacional que integra o sistema de gestão estratégica do Tribunal para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Art. 7º Fica estabelecido o COMITÊ DE SEGURANÇA DA INFORMAÇÃO, composto por pelo menos um representante de cada uma das seguintes áreas: Associação dos Magistrados da Justiça do Trabalho da 5ª Região – AMATRA5; Secretaria-Geral da Presidência; Secretaria da Corregedoria Regional, Diretoria-Geral, Secretaria de Administração, Secretarias de



Coordenação Judiciária de Primeira e Segunda Instância e Secretaria de Tecnologia da Informação e Comunicações – SETIC. O referido Comitê ficará vinculado à Comissão de Informática.

Art. 8º Compete ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

I – Elaborar e submeter à Presidência do Tribunal propostas de normas e políticas de uso dos recursos de informação, tais como:

- a) Classificação da Informação;
- b) Gerenciamento de Identidade e controle de acesso lógico;
- c) Controle de acesso físico;
- d) Controle de acesso à Internet;
- e) Utilização do correio eletrônico;
- f) Utilização de equipamentos de tecnologia da informação;
- g) Utilização de programas e aplicativos;
- h) Utilização de armazenamento lógico;
- i) Monitoração e auditoria de recursos tecnológicos;
- j) Contingência e Continuidade do Negócio;

II – Revisar e atualizar periodicamente esta Política de Segurança e normas relacionadas sugerindo possíveis alterações.

III – Dirimir dúvidas e deliberar sobre questões não contempladas nesta política e normas relacionadas.

IV– Propor e acompanhar planos de ação para aplicação desta política, assim como campanhas de conscientização dos usuários.

V – Receber e analisar as comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal, apresentando parecer à autoridade/órgão competente a sua apreciação.

VI – Solicitar, sempre que necessário, a realização de auditorias pelo Escritório de Segurança da Informação relativamente ao uso dos recursos de tecnologia da informação, no âmbito do Tribunal.



VII – Aceitar Riscos de Segurança da Informação e aprovar Plano de Tratamentos de Riscos proposto pelo Escritório de Segurança da Informação.

VIII – Aprovar e assinar a Declaração de Aplicabilidade que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI5.

IX – Realizar análises críticas regulares da eficácia do SGSI5 (incluindo o atendimento da política de segurança da informação e dos objetivos do SGSI5, e a análise crítica dos controles de segurança), levando em consideração o resultado das auditorias de segurança da informação, incidentes de segurança da informação, resultado das medições de eficácia, sugestões e realimentação de todas as partes interessadas.

X – Realizar análises críticas regulares do SGSI5 para assegurar que o escopo continua adequado e que são identificadas melhorias no processo do SGSI5.

XI – Avaliar e aprovar todos os documentos que compõem a documentação do SGSI5 elaborados e apresentados pelo Escritório de Segurança da Informação.

Art. 9º O Comitê de Segurança da Informação é a única instância do Tribunal Regional do Trabalho da 5ª Região competente para realizar aceitação de riscos de segurança da informação e aprovação de planos de tratamento de riscos de segurança da informação.

Parágrafo único. Aceitação de riscos de segurança da informação realizada por outras unidades, não terá qualquer valor no âmbito deste Tribunal e será considerada grave violação desta Política de Segurança da Informação.

Art. 10. O Comitê de Segurança da Informação se reunirá em caráter ordinário trimestralmente para deliberar sobre os encaminhamentos realizados pelo Escritório de Segurança da Informação no período e avaliar a Segurança da Informação do Tribunal.

§ 1º O Comitê de Segurança da Informação poderá ser convocado extraordinariamente sempre que necessário.

§ 2º As reuniões do Comitê de Segurança da Informação serão instaladas com a presença de no mínimo 51% dos seus membros.



§ 3º Todas as reuniões deverão ser registradas em atas que serão lidas, aprovadas e assinadas na reunião subsequente.

§ 4º Sempre que necessário poderão ser convidados a participar das reuniões do Comitê de Segurança da Informação outros colaboradores do Tribunal ou convidados externos sem direito a voto.

§ 5º As decisões do Comitê de Segurança da Informação serão aprovadas por maioria simples dos votos presentes.

Art. 11. Fica estabelecido o Escritório de Segurança da Informação, vinculado à SETIC, cujo objetivo é gerir o SGTI5 agregando valor aos serviços prestados pelo TRT da 5ª Região.

Art. 12. Compete ao Escritório de Segurança da Informação:

I – Elaborar um Plano Diretor de Segurança da Informação, a partir das definições estratégicas estabelecidas pelo Comitê de Segurança da Informação e alinhá-lo com os Planejamentos Estratégicos do Tribunal e da área de Tecnologia da Informação;

II – A gestão da Política de Segurança da Informação e do SGTI5;

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

IV – Coordenar as ações do Plano Diretor de Segurança da Informação e dos projetos nele relacionados;

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

VI – Coordenar as ações necessárias na ocorrência de incidentes de segurança da informação;

VII – Participar do planejamento de projetos que envolvam mudanças na infraestrutura no tocante à segurança da informação;

VIII – Emitir relatórios sobre o uso dos recursos de tecnologia, apontando irregularidades e não conformidades na utilização;

IX – Atuar de forma coordenada com outras áreas nos assuntos de Segurança da Informação prestando-lhes assessoria e consultoria;



X – Informar diretamente ao Comitê de Segurança da Informação:

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

b) Incidentes e eventos de segurança da informação.

XI – Levar a conhecimento do Comitê de Segurança, os casos que não foram previstos na Política de Segurança e nos atos normativos;

XII – Realizar Análises de Risco periódicas com o escopo definido pelo SGSI5;

XIII – Coordenar a execução dos planos de tratamento de riscos aprovados pelo Comitê de Segurança da Informação;

XIV – Realizar auditorias internas de segurança da informação de forma regular;

XV – Coordenar a implementação das ações corretivas e de melhoria resultantes da análise crítica do SGSI5 realizada pelo Comitê de Segurança da Informação;

XVI – Gerir a infraestrutura necessária para prover com segurança os serviços disponíveis nas redes internas, assim como o acesso às redes externas, desenvolvendo ações necessárias para o cumprimento desta Resolução.

Art. 13. Compete à chefia imediata e superior do usuário verificar a observância das disposições desta Resolução no âmbito de sua unidade, comunicando ao Comitê de Segurança da Informação as irregularidades.

Parágrafo único. As ações e projetos derivados dos planos de tratamento de riscos gerados pelo SGSI5 devem ser tratados como de prioridade máxima por todas as chefias de unidades administrativas do Tribunal.

Art. 14. Compete à Secretaria de Assessoramento Jurídico do TRT5:

I – informar ao Comitê de Segurança da Informação alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolvam a gestão da segurança da informação;

II – avaliar, sempre que solicitado, as normas, procedimentos e outros documentos referentes à gestão da segurança da informação;



III – assessorar e prestar consultoria ao Comitê de Segurança da Informação e ao Escritório de Segurança da Informação nas questões legais.

Art. 15. 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, assegurada aos envolvidos ampla defesa.

Art. 16. A Presidência do TRT5 deverá prover o Escritório de Segurança da Informação com recursos humanos necessários e suficientes – em quantidade e nível de capacitação – para a implantação e operação do SGI5.

Art. 17. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação.

Art. 18. Esta Resolução entra em vigor a partir da data de sua publicação, ficando revogadas todas as disposições em contrário.

Publique-se. Registre-se. Cumpra-se.

Sala de Sessões Juiz Nylson Sepúlveda, 28 de julho de 2014.

VALTÉRCIO RONALDO DE OLIVEIRA
Desembargador Presidente

Disponibilizada no DJe TRT da 5ª Região em 30.07.2014, páginas 3-4, com publicação prevista para o 1º dia útil subsequente, nos termos da Lei 11.419/2006 e RA TRT5 33/2007.

*** A RA nº 0025/2020, disponibilizada no DJe TRT5 em 19.08.2020, páginas 1-3, atualizou a Política de Segurança da Informação no âmbito do TRT da 5ª Região.*

Silene Caldas, Chefe do Núcleo de Divulgação - TRT5