



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO
Secretaria do Tribunal Pleno, Órgão Especial e da Seção Especializada

RESOLUÇÃO ADMINISTRATIVA

85/2018

CERTIFICO e DOU FÉ que, nesta data, sob a presidência da excelentíssima Desembargadora Marlene T. Fuverki Suguimatsu, presentes os excelentíssimos Desembargadores Nair Maria Lunardelli Ramos (Vice-Presidente), Sérgio Murilo Rodrigues Lemos (Corregedor), Rosemarie Diedrichs Pimpão, Arnor Lima Neto, Fátima T. Loro Ledra Machado, Ana Carolina Zaina, Sueli Gil El Rafihi, Célio Horst Waldraff, Marco Antônio Vianna Mansur, Eneida Cornel, Arion Mazurkevic, Benedito Xavier da Silva, Archimedes Castro Campos Junior, Edmilson Antonio de Lima, Neide Alves dos Santos, Ricardo Tadeu Marques da Fonseca, Francisco Roberto Ermel, Paulo Ricardo Pozzolo, Thereza Cristina Gosdal, Cláudia Cristina Pereira, Aramis de Souza Silveira, Adilson Luiz Funez, Sergio Guimarães Sampaio e o excelentíssimo Procurador-Chefe Gláucio Araújo de Oliveira, representante do Ministério Público do Trabalho, **RESOLVEU** em Sessão Plenária o Tribunal Regional do Trabalho da 9ª Região, por unanimidade de votos, **INSTITUIR** a **Política Nº 28/2018**, que trata da Política de Segurança da Informação (PSI) e do Sistema de Gestão de Segurança da Informação (SGSGI) no âmbito do Tribunal Regional do Trabalho da 9ª Região, revogando-se o Ato Presidência 171/2011.

OBS.: Ausentes, justificadamente, os excelentíssimos Desembargadores Rosalie Michaele Bacila Batista, Luiz Eduardo Gunther (em férias), Altino Pedrozo dos Santos (em licença médica), Ubirajara Carlos Mendes (convocado para o TST), Cássio Colombo Filho (afastado da jurisdição), Ney Fernando Olivé Malhadas (em férias) e Eliázer Antonio Medeiros (afastado da jurisdição). Presentes os excelentíssimos juízes Fabrício Nicolau dos Santos Nogueira, Auxiliar da Corregedoria, e Camila Gabriela Greber Caldas, Presidente da AMATRA-PR.

Curitiba, 26 de novembro de 2018.

ANA CRISTINA NAVARRO LINS
Secretária do Tribunal Pleno, Órgão Especial e da Seção Especializada

Disponibilizada no DEJT de 28/11/2018

Publicação: 29/11/2018



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

POLÍTICA nº 28, de DE OUTUBRO DE 2018.

Institui a Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI) no âmbito do Tribunal Regional do Trabalho da 9ª Região.

A DESEMBARGADORA DO TRABALHO, PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO:

- as recomendações contidas no Acórdão nº 1.603/2008 - Plenário do TCU, em especial o item 9.1.3 para que os órgãos integrantes da estrutura do Poder Judiciário Federal orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar o gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

- as diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação estabelecidos na Norma ISO/IEC 27002;

- as diretrizes constantes em 02/IN01/DSIC/GSIPR.

- as diretrizes para elaboração de Política de Segurança da Informação constantes na NC 03/IN01/DSIC/GSIPR.

- o Código de Práticas para a Gestão da Segurança da Informação estabelecido na Norma ISO/IEC 27002:2013;

- as Diretrizes para Classificação, Rotulação e Tratamento da Informação estabelecido na Norma ABNT NBR 16167:2013;



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

III, Seção I;

- os termos da Resolução CNJ nº 211/2015, em especial o art. 9º do Cap.

- os termos da Resolução CNJ nº 215/2015, em especial o art 3º, item "III - utilização de meios de comunicação viabilizados pela tecnologia";

- a reunião Ordinária do Comitê de Segurança da Informação (CSI), ocorrida em 28 de setembro de 2018.

RESOLVE, ad referendum do Tribunal Pleno:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º Instituir a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) e o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI) no âmbito do Tribunal Regional do Trabalho da 9ª Região, política da qual são partes integrantes as seguintes normas e procedimentos complementares, estabelecidos com o objetivo de garantir a segurança das informações:

I - Política de Classificação e Tratamento da Informação;

II - Norma de Identidade Digital e Controle de Acesso;

III - Norma de Utilização de Recursos de Tecnologia da Informação; e

IV - outras normas que venham a ser necessárias.

Parágrafo Único. As normas de segurança da informação propostas pelo Comitê de Segurança da Informação (CSI) e aprovadas pela Presidência do Tribunal ou Secretaria de Tecnologia da Informação tornam-se parte integrante da Política de Segurança da Informação, doravante denominada apenas PSI.

Art. 2º Para os efeitos da PSI ficam estabelecidas as seguintes **conceituações:**

I - ADMINISTRADOR DOS SISTEMAS COMPUTACIONAIS: quaisquer pessoas do quadro funcional ou não, lotadas nas Unidades de Tecnologia da Informação e Comunicação, que tenham sido autorizadas a conhecer o código de acesso e senha de administração de recurso de Tecnologia da Informação e Comunicação (TIC), seja ele de uso geral, de uso restrito a uma unidade ou grupo de pessoas, ou de uso individual;

II - AUTENTICIDADE: propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

III - CICLO DE VIDA DA INFORMAÇÃO: ciclo que compreende etapas e eventos de produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação;

IV - CONFIDENCIALIDADE: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

V - DISPONIBILIDADE: garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário;

VI - GESTOR DE SEGURANÇA DA INFORMAÇÃO: pessoa responsável pela coordenação das atividades relacionadas à segurança da informação em âmbito local, buscando assegurar a integridade, confidencialidade e disponibilidade dos dados corporativos;

VII - INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação;

VIII - INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

IX - INTEGRIDADE: garantia da não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital;

X - RECURSOS DE TIC: equipamentos relacionados à TIC, tais como microcomputadores e dispositivos de armazenamento de dados, softwares, serviços de rede e comunicação de dados, suprimentos e bens de consumo também relacionados à TIC, e dados armazenados em qualquer equipamento;

XI - SEGURANÇA DA INFORMAÇÃO: preservação da autenticidade, confidencialidade, integridade e disponibilidade da informação;

XII - SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI): modelo de gestão, composto por um conjunto de políticas ou normas, que visa estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;

XIII - USUÁRIOS: magistrados, servidores ocupantes de cargo efetivo ou em comissão, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários, advogados, jurisdicionado em geral e outras pessoas que se encontrem a serviço da Justiça do Trabalho, ainda que em caráter temporário.

Parágrafo único. Para os efeitos desta Política, outras definições e conceitos específicos encontram-se definidos no GLOSSÁRIO, disponível em sítio na Intranet ou Internet mantidos por este Tribunal.



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

CAPÍTULO II
DAS DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Art. 3º A Segurança da Informação no Tribunal alinha-se às estratégias organizacionais e visa a assegurar a preservação da Autenticidade, Confidencialidade, Integridade e Disponibilidade da Informação no âmbito deste Tribunal, com o objetivo de:

- I - Garantir a continuidade e eficiência da prestação jurisdicional;
- II - Salvar as informações institucionais;
- III - Resguardar a imagem e objetivos institucionais.

Art. 4º São **princípios** da Segurança da Informação no Tribunal:

I - O MENOR PRIVILÉGIO: que exige que sejam concedidos aos usuários somente os privilégios necessários ao exercício de suas funções institucionais;

II - O CONTROLE DA RESPONSABILIDADE: que estabelece que as pessoas que estejam em posições de maior responsabilidade e risco devam ser submetidas a controles mais rígidos de segurança da informação;

III - A PROPRIEDADE DA ORGANIZAÇÃO: que garante que informações, sistemas, processos, procedimentos ou métodos específicos criados pelos usuários, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são de propriedade deste Tribunal e deverão ser adequadamente protegidos e utilizados exclusivamente para fins relacionados às atividades institucionais;

IV - A IDENTIFICAÇÃO DIGITAL: que preconiza que a identificação de qualquer usuário deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas por meio dessa identidade;

V - A TRANSPARÊNCIA: que determina que as informações de interesse público devem permanecer públicas e disponíveis;

VI - A UNIVERSALIDADE: que estabelece que os controles de segurança da informação devam ser aplicados a todos os meios e etapas do ciclo de vida da informação;

VII - O MONITORAMENTO CONTÍNUO: que estabelece que os meios nos quais trafegam as informações devem ser constantemente monitorados e controlados, com o intuito de evitar ameaças à informação;

VIII - O REPOSITÓRIO ADEQUADO: que estabelece que as informações devem ser armazenadas em repositórios ou locais compatíveis com suas características e requisitos de segurança;

IX - A NÃO EXCLUSIVIDADE: que estabelece que não é permitido que apenas um usuário ou administrador de sistemas computacionais do Tribunal possua



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

controle ou acesso exclusivo de um processo de negócio ou recurso imprescindível para a continuidade do negócio.

Art. 5º As diretrizes, normas e procedimentos de segurança da informação de que trata esta política aplicam-se a todos os usuários de informações e de recursos de tecnologia da informação do Tribunal.

§1º Todos os usuários, no âmbito de suas atribuições e competências, são corresponsáveis pela segurança da informação e devem, para tanto, zelar pelo correto conhecimento, entendimento e cumprimento das diretrizes, normas, procedimentos e instruções integrantes desta PSI, devendo comunicar a seu superior ou à direção competente qualquer indício de falha, incidente ou irregularidade de que tiver conhecimento.

§2º As informações geradas no âmbito deste Tribunal devem ser classificadas em termos de seu valor, requisitos legais, sensibilidade, criticidade, nível de proteção e necessidade de compartilhamento, em conformidade com a política de classificação da informação e normas próprias, considerando-se os princípios do **Art. 4º**.

CAPÍTULO III
DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 6º Esta política é parte integrante do Sistema de Gestão de Segurança da Informação (SGSI), composto pelos seguintes processos:

- I - gestão de riscos de segurança da informação;
- II - gestão de incidentes em segurança da informação;
- III - gestão de continuidade de serviços essenciais de TIC;
- IV - gestão de acessos e de uso de recursos de TIC;
- V - gestão e controle de ativos de informação;
- VI - classificação e tratamento da informação.

§ 1º Os processos do SGSI são interdependentes e devem ser estruturados e monitorados de forma a permitir sua melhoria contínua.

§ 2º A gestão de segurança da informação é um processo cíclico, de melhoria contínua, e deve ser realizada por meio das etapas de planejamento, execução, monitoramento e melhoria, seguindo as melhores práticas de Gestão de Segurança da Informação vigentes.

§ 3º Os ciclos de gestão de segurança da informação devem ter duração máxima de 2 (dois) anos.



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

Art. 7º O Sistema de Gestão de Segurança da Informação será coordenado pelo Comitê de Segurança da Informação (CSI), com o apoio da Secretaria de Tecnologia da Informação (STI) e do Gestor de Segurança da Informação.

Art. 8º O CSI é responsável pela proposição e acompanhamento da gestão de segurança da informação no âmbito do Tribunal, e tem por finalidade:

I - elaborar, institucionalizar e manter o Sistema de Gestão de Segurança da Informação (SGSI);

II - revisar esta política e formular normas e diretrizes para o SGSI, bem como analisar periodicamente sua efetividade;

III - promover a cultura de segurança da informação no Tribunal e implementar programas contínuos destinados à conscientização e capacitação dos usuários internos;

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

V - estabelecer critérios de classificação dos dados e dos repositórios, com vistas à garantia dos níveis de segurança desejados e à normatização do acesso e uso das informações;

VI - cumprir outras obrigações relativas ao tema de segurança da informação definidas em outros normativos.

Art. 9º Cabe à STI:

I - executar os processos elencados no **Art. 6º**, I a VI.

II - gerir a infraestrutura de hardware e software necessária à prestação dos serviços corporativos, estabelecendo os procedimentos de segurança adequados;

III - registrar ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI;

IV - executar ações preventivas e corretivas que impactem positivamente na gestão de segurança da informação;

V - monitorar a utilização dos recursos de tecnologia da informação, com o intuito de detectar infrações a normas, procedimentos e diretrizes que integram a PSI, fornecendo evidências no caso de incidentes de segurança.

Art. 10. Cabe ao Gestor de Segurança da Informação, em conjunto com a área de Tecnologia da Informação:

I - monitorar a execução dos processos e das ações de segurança da informação;



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

II - medir os indicadores e os controles de segurança da informação, previstos no PLSI;

III - propor ajustes nos procedimentos de segurança da informação;

IV - acompanhar as eventuais alterações nas leis, resoluções e nos normativos de outras esferas que afetem a segurança da informação, propondo possíveis modificações nesta política, nas normas e nos processos;

V - comunicar as ações de segurança a todas as partes interessadas;

VI - coordenar as atividades da equipe de tratamento de incidentes de incidentes computacionais.

Parágrafo único. O gestor de segurança da informação será o chefe da Divisão de Segurança da Informação e Redes, ou unidade administrativa equivalente.

Art. 11. Fica instituída a **Equipe de Tratamento e Resposta a Incidentes de Segurança Computacionais do TRT9** (CSIRT-TRT9), composta por servidores indicados pela Secretaria de Tecnologia da Informação, responsável pela triagem, coleta de evidências, análise, registro e resposta a incidentes computacionais que envolvam a segurança das informações.

Parágrafo único. O funcionamento da CSIRT-TRT9 será regulado por documento formal de constituição, publicado pela Secretaria de Tecnologia da Informação.

Art. 12. A CSIRT-TRT9 tem autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão caso as recomendações não forem seguidas.

Parágrafo único. A Presidência do Tribunal Regional do Trabalho da 9ª Região será a responsável pela avaliação e aprovação de ações decorrentes em resposta a um incidente ou ameaça de segurança que afetem a imagem institucional ou a confidencialidade das informações do Regional.

CAPÍTULO IV
DO PLANEJAMENTO DA SEGURANÇA DA INFORMAÇÃO

Art. 13. O CSI deverá, no início de cada ciclo de gestão, apresentar à Presidência, para sua aprovação, o PLSI, referente ao novo ciclo da gestão.

Parágrafo único. O PLSI deve considerar os conceitos e objetivos dos planos estratégicos institucionais e estabelecer para o próximo ciclo:

I - o escopo da gestão de segurança da informação no âmbito do Tribunal;

II - os objetivos de controle de segurança da informação desejados;



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

III - os critérios de análise e avaliação de riscos que devem ser seguidos;

IV - as ações de segurança que devem ser priorizadas;

V - os mecanismos e indicadores com os quais o CSI deve controlar o processo de gestão da segurança da informação;

VI - sugestões de alteração desta política, bem como de outras normas e processos de segurança da informação.

CAPÍTULO V
DA EXECUÇÃO DO PLANO DE SEGURANÇA DA INFORMAÇÃO

Art. 14. O PLSI deverá servir de base para todas as ações da gestão de segurança da informação.

§ 1º A STI deverá, com base no PLSI, coordenar a revisão de processos e procedimentos.

§ 2º O gestor de segurança da informação deve coordenar as atividades de identificação e análise dos riscos de segurança da informação.

§ 3º O resultado da análise de risco deve ser pré-avaliado pelo Comitê Gestor de TIC, com base nos critérios de avaliação de risco definidos no PLSI.

§ 4º Os riscos residuais que não possam ser avaliados segundo os critérios pré-definidos, devem ser submetidos à avaliação do CSI, que proporá o **Plano de Tratamento de Riscos** (PTR) à Presidência.

§ 5º Cabe à Presidência do Tribunal referendar o PTR e priorizar ações e recursos para a sua execução.

CAPÍTULO VI
DO MONITORAMENTO E MELHORIA

Art. 15. Cabe ao Presidente do CSI convocar reuniões de acompanhamento do SGSI, tomando ciência dos indicadores e eventos relevantes de segurança da informação, com o intuito de:

I - acompanhar a execução dos processos de segurança da informação;

II - desembaraçar a execução de atividades e ações que visem à segurança da informação;

III - identificar não-conformidades e possíveis ações de melhoria do SGSI;



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

IV - executar a análise crítica e propor ajustes ao SGSI, a esta política, a normas e processos, com base nas lições aprendidas e na experiência de outros órgãos e organizações;

V - conduzir à implementação as melhorias identificadas aplicáveis no SGSI, assegurando que atinjam os objetivos pretendidos;

VI - garantir a retroalimentação de todo o processo, com novos dados e estatísticas originadas de análise crítica do processo.

CAPÍTULO VII
DO PROCESSO DE ELABORAÇÃO, ACOMPANHAMENTO E REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 16. A STI deve modelar processo de elaboração, acompanhamento e revisão da PSI, o qual deverá ser revisado anualmente e aperfeiçoado quando necessário.

Parágrafo único. A elaboração, acompanhamento e revisão da Política de Segurança da informação devem ocorrer por meio do CSI.

CAPÍTULO VIII
DA PRESTAÇÃO DE CONTAS

Art. 17. O CSI apresentará à Presidência, via Comitê de Governança de TIC (CGTIC), com antecedência mínima de 15 (quinze) dias às Reuniões deste Comitê, rol das políticas ou normas de segurança da informação vigentes, em elaboração, modificadas ou extintas desde a última prestação de contas a respeito do mesmo tema.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 18. O descumprimento desta política, bem como das diretrizes, normas e procedimentos de segurança da informação estabelecidos, poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais, assegurada aos envolvidos ampla defesa.

Art. 19. Deve a STI modelar o processo de elaboração, acompanhamento e revisão da Política de Segurança da informação, em até 90 (noventa) dias da publicação desta Política, submetendo-o à aprovação do CSI, com a respectiva instituição formal do processo como norma de cumprimento obrigatório.

Art. 20. Os casos omissos e as dúvidas surgidas na aplicação desta política serão dirimidos pela Presidência do Tribunal, com apoio do CSI.



PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

Art. 21. Esta Política entra em vigor na data de sua publicação, revogando-se o Ato nº 171, de 18 de agosto de 2011.

A handwritten signature in black ink, appearing to read 'Marlene T. Fuverki Sugumatsu'.

MARLENE T. FUVERKI SUGUMATSU
Desembargadora Presidente