



RESOLUÇÃO ADMINISTRATIVA Nº 66/2022

Define a Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região.

PROAD: 4670/2011

INTERESSADO: TRT/24ª Região.

ASSUNTO: Política de Segurança da Informação.

AUTORIDADE REQUERIDA: Egrégio Tribunal Pleno.

O Egrégio Tribunal Regional do Trabalho da 24ª Região, na 5ª Sessão Administrativa Ordinária, realizada em 2 de junho de 2022, sob a Presidência do Desembargador André Luís Moraes de Oliveira, com a participação dos Desembargadores João Marcelo Balsanelli (Vice-Presidente), João de Deus Gomes de Souza, Nicanor de Araújo Lima, Marcio Vasques Thibau de Almeida, Francisco das C. Lima Filho e Tomás Bawden de Castro Silva e da representante do Ministério Público do Trabalho da 24ª Região, Procuradora Cândice Gabriela Arosio,

CONSIDERANDO a observância e adoção das recomendações do framework de governança de TIC COBIT 5.0;

CONSIDERANDO as normas da família ISO 27000, que tratam da definição de requisitos para um sistema de segurança da informação;

CONSIDERANDO o disposto na Resolução CNJ de No 370 de 10 de junho DE 2021, que institui a estratégia nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução Administrativa nº 122/2021 de 09 de setembro de 2021 que instituiu a Política de Governança dos Colegiados Temáticos do Tribunal Regional do Trabalho da 24ª Região,

DECIDIU, por unanimidade, definir a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 24ª Região, nos seguintes termos:

TÍTULO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO

TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

CAPÍTULO I DAS DEFINIÇÕES



Art. 1º Para fins deste ato, considera-se:

I - **Ativos de Tecnologia da Informação e Comunicações (TIC)**: qualquer mecanismo ou dispositivo de software ou hardware que compõe a infraestrutura da rede de dados do TRT24;

II - **Ativos críticos do negócio**: ativos de TIC que suportam a operação dos processos críticos do negócio;

III - **Processos críticos do negócio**: o conjunto de atividades através das quais a instituição produz valor para os seus clientes;

IV - **Infraestrutura básica de segurança**: conjunto de ativos críticos do negócio necessários para suportar os processos críticos do negócio;

V - **Segurança da Informação**: conjunto de medidas que tem como objetivo o estabelecimento dos controles necessários à preservação da confidencialidade, integridade e disponibilidade das informações durante sua criação, uso ou armazenamento, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais;

VI - **Confidencialidade**: garantia de que a informação seja acessível apenas às pessoas autorizadas;

VII - **Integridade**: garantia de exatidão e completeza da informação e dos métodos de armazenamento e/ou processamento;

VIII - **Disponibilidade**: garantia de que as pessoas autorizadas tenham acesso às informações;

IX - **Usuário de TIC**: todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em qualquer unidade organizacional do TRT da 24ª Região.

CAPÍTULO II

PRINCÍPIOS E DIRETRIZES GERAIS

Art. 2º A Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região obedecerá aos seguintes princípios e diretrizes:

I - Priorização de ações que promovam um sistema de segurança da informação eficiente, e que tornem o espaço cibernético mais confiável, resistente e seguro;

II - Contemplar ações destinadas a assegurar o funcionamento dos processos de trabalho institucionais e a continuidade das atividades fim e administrativas do TRT24, que utilizem ativos de TIC;

III - Estabelecer os processos de trabalho de segurança da informação para garantir a confidencialidade, integridade e disponibilidade das informações da instituição armazenados em meio computacional, de modo a mitigar os riscos associados à dependência da organização em relação ao uso massivo da TI;



IV - Definir o escopo mínimo de processos e ativos críticos do negócio, para priorização nas ações e atividades de segurança da informação;

V - Definir os procedimentos básicos a serem adotados para a utilização mais segura dos ativos de TIC do TRT24;

VI - Definir as atribuições e responsabilidades relativas aos processos de trabalho.

CAPÍTULO III

DA GOVERNANÇA

Art. 3º A governança e gestão desta política, será realizada pelo Comitê de Segurança da Informação e Proteção de Dados (CSEGINF).

Parágrafo único. A composição e as atribuições do CSEGINF serão definidas por normativo específico, em observância a Política de Governança dos Colegiados Temáticos.

CAPÍTULO IV

DOS PROCESSOS DE TRABALHO

Art. 4º As atividades executadas no âmbito da Política de Segurança da Informação deverão observar os procedimentos descritos no processo de trabalho "**Gerenciar Segurança da Informação**", disponível no site do Portal de Governança de TIC do TRT24, item "Processos de Trabalho".

CAPÍTULO V

DOS INSTRUMENTOS NORMATIVOS COMPLEMENTARES

Art. 5º São complementares à segurança da informação os seguintes normativos:

I - Política de Gestão de Riscos;

II - Política de Controle de Acessos;

III - Política de Gestão de Incidentes de Segurança;

IV - Política de Gestão de Ativos de TIC para a Continuidade de Negócios;

V - Política de Privacidade e Proteção de Dados Pessoais.

§ 1º As ações e atividades desenvolvidas no âmbito da Política de Segurança da Informação deverão seguir os normativos complementares.

§ 2º Os normativos dos incisos I, II, III e IV, serão instituídos por Ato da Presidência do Tribunal, após aprovação do CSEGINF.

CAPÍTULO VI

DOS RESPONSÁVEIS E DAS RESPONSABILIDADES



Art. 6º A responsabilidade sobre a execução das atividades previstas no processo de trabalho Gerenciar Segurança da Informação observará o seguinte:

I - Ao Diretor(a) da Secretaria de Tecnologia da Informação e Comunicações (SETIC) caberá a responsabilidade pelas atividades atribuídas ao papel de "Dono do Processo";

II - Ao Coordenador do CSEGINF caberá a responsabilidade pelas atividades atribuídas ao papel de "Comitê de Segurança da Informação";

III - Ao Chefe da Seção de Proteção de Dados e Segurança da Informação caberá a responsabilidade pelas atividades atribuídas aos papéis de "Gerente do Processo" e de "Seção de Proteção de Dados e Segurança da Informação";

IV - Aos chefes das unidades responsáveis pelos ativos críticos caberá a responsabilidade pelas atividades atribuídas ao papel "Proprietário do Ativo".

CAPÍTULO VII DO ÂMBITO E DA APLICAÇÃO

Art. 7º A Política de Segurança da Informação aplica-se a todos aqueles autorizados a fazer uso dos ativos de TIC administrados pela SETIC, bem como, no que couber, ao relacionamento do TRT da 24ª Região com outros órgãos públicos ou entidades públicas ou privadas.

CAPÍTULO VIII DOS PROCEDIMENTOS BÁSICOS PARA A MELHOR UTILIZAÇÃO DOS ATIVOS DE TIC

Art. 8º O uso dos ativos de TIC obedecerá às seguintes diretrizes gerais:

I. O uso dos ativos de TIC estará sujeito a monitoramento, com intuito de detectar, prevenir e tratar eventuais incidentes de segurança;

II. Os incidentes de segurança serão reportados ao CSEGINF;

III. A utilização dos recursos de TIC destina-se a auxiliar os usuários de TIC do TRT da 24ª Região, em efetivo exercício, na realização de atividades relacionadas estritamente ao serviço;

IV. É vedado o uso dos ativos de TIC deste Órgão para acesso, veiculação ou armazenamento voluntário de matérias:

- a. Pornográficas;
- b. Político-partidárias ou sindicais;
- c. Ofensivas ao princípio da urbanidade;
- d. Ofensivas ao decoro pessoal;
- e. Que contenham manifestações ofensivas à honra e à dignidade de pessoas, instituições e autoridades;



f. Que apresentem linguagem incompatível com o decoro da classe;

g. Que versem assuntos de natureza comercial;

h. Que provoquem sobrecarga no sistema.

V. Também é vedado:

a. Participar de ações ilegais ou que de alguma forma caracterizem descumprimento dos deveres para com a Administração;

b. Participar de qualquer ação que comprometa a segurança da rede de computadores do TRT24;

c. A utilização de senha alheia;

d. Revelar ou compartilhar senhas com outros usuários;

e. A disponibilização a pessoas, Órgãos ou entidades externas de mensagens que possam vir a comprometer a boa imagem da instituição;

Art. 9º O uso da rede sem fio (wireless) obedecerá às seguintes diretrizes:

I - A rede wireless dará acesso à internet, sendo vedada a comunicação direta com a rede interna do TRT24;

II - Os usuários internos do TRT24, incluindo estagiários e terceirizados, terão acesso à rede wireless mediante identificação de nome de usuário e senha da rede de computadores, condicionado a disponibilidade da infraestrutura técnica nas dependências dos prédios da Justiça do Trabalho do MS;

III - Os usuários serão unicamente identificados, e a comprovação de utilização do usuário de forma compartilhada ensejará o bloqueio da senha após detectados mais de 5 dispositivos conectados no mesmo instante, e a reincidência será notificada ao CSEGINF para as providências administrativas;

IV - Os advogados terão acesso à rede wireless através de conexão à rede pública (sem senha) disponibilizada pela SETIC, com restrições de navegação a sites governamentais e aplicativos de mensagens;

V - Os usuários externos colaboradores temporários terão acesso à rede wireless através de conexão à rede pública disponibilizada pela SETIC mediante solicitação de concessão de acesso temporário, feita pelo responsável da unidade de atuação do colaborador através do sistema SIATE;

VI - O acesso temporário será concedido através de identificador para uso em um único dispositivo e por um prazo acordado em pedido formalizado, com a utilização justificada em formulário assinado por magistrado ou servidor do quadro, não podendo ser superior a 6 (seis) meses e com revogação automática;



VII - Não será permitida renovação do acesso temporário, devendo ser feito novo pedido;

VIII - Em caso de detecção de uso indevido o acesso será revogado imediatamente.

Art. 10. O uso de computadores, notebooks e dispositivos móveis obedecerá às seguintes diretrizes:

I - É expressamente proibido instalar, configurar ou conectar à rede qualquer tipo de equipamento não pertencente ao TRT24 (tais como tablets, notebooks, computadores pessoais, switches, hubs, modems/roteadores wireless, access points, smartphones, etc.) que possam comprometer a segurança da informação, salvo com autorização formal do Comitê de Segurança da Informação e Proteção de Dados (CSEGINF);

II - Os computadores (estações de trabalho) e notebooks fornecidos pelo TRT24 serão protegidos por software antivírus e regras de segurança definidas pelo CSEGINF;

III - A responsabilidade sobre a inobservância do inciso I deste artigo recai sobre o usuário que a praticar.

Art. 11. O envio e recebimento de mensagens por correio eletrônico obedecerá às seguintes diretrizes:

I - Para comunicação deverá ser priorizada a utilização do correio eletrônico, evitando-se, tanto quanto possível, a impressão do conteúdo das mensagens;

II - O acesso aos e-mails será realizado através da interface de webmail homologada pela SETIC e do protocolo IMAP, não sendo de responsabilidade da SETIC a recuperação de mensagens armazenadas em pastas locais ou baixadas do servidor através do protocolo POP;

III - Cabe a quaisquer dos receptores das mensagens, imagens ou notas indevidas comunicarem o fato à SETIC para as providências cabíveis;

IV - O uso do correio eletrônico será considerado atividade inadequada e passível de apuração por sindicância se não estiver relacionado à matéria de interesse do Tribunal ou às atribuições do cargo do usuário;

V - Mesmo se relacionados a matérias de interesse do Tribunal ou às atribuições do cargo do usuário, são consideradas atividades inadequadas o acesso, a gravação ou a impressão de textos ou gráficos que excedam o limite dos padrões aceitáveis de ética, bom senso e razoabilidade;

VI - O uso inadequado do correio eletrônico compreende a troca de mensagens contendo:

a. Material pornográfico, racista, ofensivo, ilegal, preconceituoso ou discriminatório;

b. Material calunioso ou difamatório;



- c. Propagandas comerciais;
 - d. Listas de endereços dos usuários do correio eletrônico do TRT24;
 - e. Entretenimento ou correntes;
 - f. Músicas e filmes de qualquer formato;
 - g. SPAM;
 - h. Aplicativos;
- VII - Qualquer mensagem endereçada ao grupo de email "TODOS" deverá ser submetida previamente à apreciação da Diretoria-Geral de Coordenação Administrativa;
- VIII - A SETIC definirá os limites de armazenamento e tamanho de mensagens para a utilização das contas de email pessoal e de unidades;
- IX - As unidades judiciais e administrativas que compõem o TRT24 terão contas de correio eletrônico sob responsabilidade dos responsáveis pelas unidades;
- X - Os titulares de conta de e-mail de usuário ou de unidade deverão sempre observar os padrões de envio e recebimento de mensagens estabelecidos pela SETIC;
- XI - A leitura das mensagens recebidas deverá ser realizada diariamente, devendo o titular da conta providenciar, se for o caso, a resposta e o respectivo arquivamento, cuidando, em qualquer hipótese, de manter limpa a caixa postal;
- XII - Nos afastamentos ou impedimentos do titular de conta de unidade, deverá ser designado um responsável pelo acompanhamento das mensagens;
- XIII - As caixas postais das contas de correio eletrônico sem acesso ou movimentação por um período de 120 (cento e vinte) dias serão bloqueadas automaticamente;
- XIV - As caixas postais que não estiverem sendo acessadas há mais de 3 meses e estiverem lotadas bloqueando novos recebimentos, sem contato com a devida justificativa para o aumento de conta, terão 50% de seus e-mails mais antigos excluídos;
- XV - Aposentados inativos, sem vínculo ativo com o TRT24, terão suas contas desativadas e excluídas após 3 meses, prazo para que cópia dos dados de interesse pessoal;
- XVI - As caixas postais das contas de correio eletrônico serão limitadas ao tamanho de 2 GB (dois gigabytes);

Art. 12. O uso da Internet e Intranet obedecerá às seguintes diretrizes:

- I - Por ocasião do acesso a *sites* e páginas da *internet* o usuário deverá:
 - a. Utilizar os navegadores (*browser*) homologados pela SETIC;
 - b. Manter conduta compatível com a moralidade administrativa, inclusive quando da utilização de serviços de computadores remotos e na transferência de arquivos;
 - c. Observar os procedimentos ordinários de segurança indicados pela SETIC, principalmente antivírus,



ficando diretamente responsável pelas consequências decorrentes de práticas contrárias ao recomendado e que danifiquem ou coloquem em risco os sistemas de computadores e os arquivos de dados do Tribunal.

II - O acesso à *internet* será considerado atividade inadequada e passível de apuração por sindicância se não estiver relacionado a matérias de interesse do Tribunal ou às atribuições do cargo do usuário;

III - Mesmo se relacionados a matérias de interesse do Tribunal ou às atribuições do cargo do usuário, são consideradas atividades inadequadas o acesso a gravação ou a impressão de textos ou gráficos que excedam o limite dos padrões aceitáveis de ética, bom senso e razoabilidade;

IV - O uso inadequado do acesso à *internet* compreende:

a. O acesso a *websites* de conteúdo racista, ofensivo, ilegal ou impróprio;

b. O acesso a serviços do tipo chat, bate-papo e troca de mensagens em tempo real que não tenham sido formalmente autorizados e que apresentem vulnerabilidades ou possam comprometer a integridade da rede de computadores do TRT24;

c. O acesso a serviços de downloads de músicas e filmes de qualquer formato, fotos e material pornográfico, programas não homologados ou licenciados;

d. O acesso a serviços de transmissão de programação de TVs ou rádio AM/FM.

Art. 13. A troca de documentos utilizando a rede de computadores do TRT24 obedecerá às seguintes diretrizes:

I. Para a troca de documentos, oficiais e de mero expediente, deverá ser priorizada a utilização do sistema de Malote Digital;

II. Os documentos oficiais e de mero expediente encaminhados através do sistema de Malote Digital deverão ser assinados digitalmente;

III. As peças processuais encaminhadas através do sistema de Malote Digital ou de outro qualquer deverão ser preferencialmente assinadas digitalmente, cabendo a seu proprietário a guarda do arquivo eletrônico para fins de eventual comprovação de autenticidade;

IV. Documentos eletrônicos assinados digitalmente serão considerados originais e a impressão dos mesmos será considerada cópia;

V. A materialização e juntada de cópias de qualquer tipo de documento eletrônico assinado digitalmente deverá ser acompanhada de certidão, cabendo ao certificador a guarda do arquivo eletrônico para fins de eventual comprovação de autenticidade;

VI. Documentos com assinatura eletrônica recebidos por e-mail que forem juntados ao Sistema de Processo



Administrativo Eletrônico - PROAD, também deverão ser guardados pelo receptor para fins de eventual comprovação de autenticidade.

Art. 14. O uso de certificação digital obedecerá às seguintes diretrizes:

I - A utilização de certificados digitais tipo A3 (smartcard ou token) para assinatura digital de documentos observará os seguintes critérios:

a. O certificado de assinatura digital e o hardware portátil (smart card ou token) serão fornecidos pelo TRT da 24ª Região ao magistrado ou servidor de acordo com a conveniência e necessidade para as atividades exercidas;

b. O uso de certificados de assinatura digital não fornecidos pelo TRT da 24ª Região fica restrito a certificados digitais emitidos por autoridades certificadoras da cadeia AC-JUS e/ou ICP-Brasil;

c. A criação ou renovação das senhas PIN, PUK ou quaisquer outras é de inteira responsabilidade do proprietário do certificado;

d. A renovação da validade do certificado é de inteira responsabilidade do proprietário;

e. O TRT da 24ª Região não fornecerá certificados ou hardwares portáteis para reposição em caso de perda, dano ou esquecimento das senhas PIN e PUK.

II - As aplicações desenvolvidas pela SETIC fornecerão mecanismo de assinatura digital através de certificado tipo A1 (usuário e senha), sendo a renovação da validade do certificado de inteira responsabilidade do proprietário.

Art. 15. A instalação e a utilização de programas de computador no TRT24 estão sujeitas as seguintes diretrizes:

I - Existência de licenças de uso em quantidade suficiente, sendo expressamente vedada a instalação de programa ou aplicativo de terceiros, sem licença de uso regularmente contratada;

II - Conformidade com a atividade da instituição e com a área de atuação das unidades administrativas;

III - Compatibilidade e adequação com os demais programas utilizados e recursos computacionais disponíveis;

IV - Obediência a planejamentos, cronogramas e prioridades existentes;

V - Deverá ser realizada exclusivamente pelos técnicos da SETIC;

VI - A cópia de programa ou aplicativo de computador adquirido/contratado pelo TRT24, para uso particular, somente pode ser cedida com a autorização expressa do CSEGINF, nos termos da licença de uso;

VII - É vedada a utilização de programas ou aplicativo de computador que descaracterizem os propósitos da



instituição ou comprometam, de alguma forma, o ambiente instalado;

VIII - A listagem com os softwares homologados para a utilização no TRT24 será publicada pela SETIC através do Catálogo de Serviços de TIC;

IX - Os softwares provenientes de instalações irregulares poderão removidos sem prévio aviso ao usuário.

CAPÍTULO IX DA INFRAESTRUTURA BÁSICA

Art. 16. A infraestrutura básica de segurança e seus níveis de tolerância e priorização de retorno após incidentes de segurança serão definidos no âmbito da Política de Gestão de Ativos de TIC para a Continuidade de Negócios.

CAPÍTULO X DOS ATIVOS CRÍTICOS DO NEGÓCIO

Art. 17. Os ativos críticos de negócio serão propostos pela Seção de Proteção de Dados e Segurança da Informação e aprovados pelo Comitê de Segurança da Informação e Proteção de Dados observados, no mínimo, os seguintes tipos:

I - Microcomputadores utilizados pelos usuários de TIC;

II - Pessoas;

III - Sistemas e aplicações;

IV - Processos de trabalho;

V - Equipamentos e Softwares de rede e infraestrutura;

VI - Gerenciadores de banco de dados PostgreSQL, ORACLE e Mysql;

VII - Servidores de rede do interior;

VIII - Servidores de virtualização.

CAPÍTULO XI DA COMUNICAÇÃO

Art. 18. A comunicação a respeito da Política de Segurança da Informação será direcionada aos usuários de TIC do Tribunal Regional do Trabalho da 24ª Região, de acordo com a conveniência da instituição, através dos seguintes meios:

I - A comunicação entre os envolvidos nos processos de trabalho deverá utilizar o processo administrativo correspondente ao Processo Gerenciar Segurança da Informação;

II - A comunicação ao público interno deverá utilizar meios eletrônicos de envio, tais como e-mail e malote digital.

CAPÍTULO XII



DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 19. A Política de Segurança da Informação se aplica a todos os integrantes do TRT24: magistrados, servidores (sejam do quadro permanente ou não), estagiários, e eventuais agentes externos, prestadores de serviços, contratados ou regidos por instrumento equivalente, que participem em qualquer nível na utilização de serviços de tecnologia da informação.

Art. 20. Os usuários de TIC deverão tomar ciência e manifestar sua concordância com os termos da presente norma através da Declaração de Ciência da Política de Segurança da Informação do anexo, assinada preferencialmente no recadastramento anual de magistrados e servidores.

Parágrafo único. Para usuários que não participam do recadastramento, como estagiários, terceirizados, e outros colaboradores, deverá ser providenciada a assinatura da declaração de ciência, sob pena de cancelamento dos acessos aos serviços de tecnologia da informação do TRT24.

Art. 21. A inobservância da presente Política de Segurança da Informação acarretará a apuração da responsabilidade penal, civil e administrativa, previstas nas normas internas do TRT24 e na legislação em vigor, de acordo com o fato denunciado perante o Comitê de Segurança da Informação e Proteção de Dados.

Art. 22. Os casos omissos relacionados aos temas de Proteção de Dados e Segurança da Informação serão tratados pelo Comitê de Segurança da Informação e Proteção de Dados, que os encaminhará caso necessário para deliberação da Presidência.

Art. 23. Revogam-se a Resolução Administrativa nº 53/2018, a Portaria TRT/GP/DG nº61/2020 e a Portaria GP nº 26/2021.

Art. 24. Esta Resolução Administrativa entra em vigor na data de sua publicação.

ANDRÉ LUÍS MORAES DE OLIVEIRA
Desembargador Presidente



ANEXO

TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Declaro que li e estou ciente da Política de Segurança da Informação do TRT24 regulamentada RESOLUÇÃO ADMINISTRATIVA N° ____.

E assumo:

I) Tratar os ativos de informação como patrimônio do TRT da 24ª Região;

II) Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do TRT da 24ª Região;

III) Utilizar as contas de acesso e os ativos de TIC em conformidade com a legislação vigente e normas específicas do TRT da 24ª Região;

IV) Estar ciente de que as senhas de acesso são pessoais e intransferíveis, cabendo ao detentor a responsabilidade pelo seu uso indevido;

V) Responder perante o TRT da 24ª Região pelo uso indevido da minha conta de acesso e dos ativos de informação sob minha responsabilidade.

Declaro, por fim, estar ciente de que uma violação desta Política poderá resultar em medidas legais e administrativas, assim como obrigações civis e criminais.

Campo Grande, MS, ____ de ____ de ____.

Assinatura

Nome do usuário