



PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 256, DE 16 DE DEZEMBRO DE 2024

Institui o Sistema de Segurança Eletrônica (SSE) do Tribunal Regional do Trabalho da 7ª Região (TRT-7) e dá outras providências.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais,

CONSIDERANDO as determinações de que trata o art. 14, inciso III, da Resolução nº 435, de 28 de outubro de 2021, do Conselho Nacional de Justiça (instalação de monitoramento eletrônico das instalações e áreas adjacentes), e o art. 5º, inciso III, da Resolução nº 315, de 26 de novembro de 2021, do Conselho Superior da Justiça do Trabalho (instalação de sistema eletrônico de segurança, bem como circuito fechado de televisão e monitoramento, incluindo as salas de audiência e áreas adjacentes).

CONSIDERANDO a recente contratação de prestação de serviços de video-monitoramento remoto com fornecimento de equipamentos em regime de comodato de Sistema de CFTV e de Alarme Patrimonial 24 horas por dia, 7 dias da semana, ininterruptamente durante a vigência do contrato, para as áreas internas e externas das edificações do Tribunal Regional do Trabalho da 7ª Região, conforme o Processo Administrativo Eletrônico (PROAD) nº 3578/2024,

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Instituir o Sistema de Segurança Eletrônica (SSE) do Tribunal Regional do Trabalho da 7ª Região, sob o gerenciamento de sua área de segurança Institucional.

Parágrafo único. O SSE do TRT-7 poderá ser composto por diferentes tipos de equipamentos que permitam a prevenção, proteção e o combate a situações que possam colocar em risco a integridade de ambientes, bens e pessoas, a exemplo de câmeras de vigilância, alarmes, sensores de movimento, barreiras de perímetro, controles de acesso, detectores de fumaça, calor ou chama, meios de comunicação, entre outros.

CAPÍTULO II

DO SISTEMA DE SEGURANÇA ELETRÔNICA

Art. 2º Consiste no conjunto de dispositivos e tecnologias utilizadas para prevenir, monitorar, detectar e alertar em casos de atividades criminosas ou ameaças externas ou internas, utilizados de acordo com as características e as necessidades de cada ambiente, objetivando proteger pessoas, patrimônio e informações, podendo ser integrados para oferecer uma solução mais robusta e eficaz.

§ 1º Será de responsabilidade da área de segurança institucional o gerenciamento do SSE, por meio da sua Central de Monitoramento e Operacionalização (CMO), localizada no Complexo Sede do Tribunal.

§ 2º O sistema poderá ser composto tanto por soluções pertencentes ao patrimônio do Tribunal como por aquelas contratadas em comodato.

§ 3º Empresas contratadas para serviços continuados de segurança poderão administrar as soluções pertencentes ao Tribunal, sob fiscalização da área técnica responsável, após analisadas as viabilidades que sejam favoráveis neste sentido, caso haja interesse pelo Tribunal.

CAPÍTULO III

DA CENTRAL DE MONITORAMENTO E OPERACIONALIZAÇÃO

Art. 3º A Central de Monitoramento e Operacionalização (CMO) tem por finalidade o assessoramento técnico e operacional relativo ao Sistema de Segurança Eletrônica, prioritariamente, dentro das áreas internas, externas e adjacentes do Complexo Sede do Tribunal Regional do Trabalho da 7ª Região (TRT-7) e, acessoriamente, das áreas internas, externas e adjacentes do Complexo do Fórum Autran Nunes e dos Fóruns sediados na Região Metropolitana de Fortaleza (RMF) e no interior do Estado do Ceará, no que tange às atividades de videomonitoramento, vigília de perímetros e alertas internos, com a utilização de equipamentos de vigilância eletrônica, barreiras físicas e virtuais e de alarme patrimonial instalados em pontos estratégicos das edificações, os quais permitirão o acesso remoto às áreas sensíveis e a identificação de intrusões, bem como o reforço dos ambientes que ainda não se encontram totalmente cobertos pelas atividades presenciais exercidas pela segurança institucional.

§ 1º A Sala de Monitoramento do Fórum Autran Nunes será parte integrante da CMO, como unidade destacada, responsável pela vigilância eletrônica daquele complexo, no acompanhamento de seu cotidiano e no reforço das atividades de segurança institucional.

§ 2º O videomonitoramento será realizado por câmeras de segurança instaladas nas edificações do TRT- 7 e conectadas a dispositivos digitais de armazenamento de imagens em ambiente próprio da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do estado.

Seção I

Das Atribuições da CMO, da Sala de Monitoramento do Fórum Autran Nunes e das Representações

Art. 4º As atribuições da Central de Monitoramento e Operacionalização, da Sala de Monitoramento do Fórum Autran Nunes e das representações da área de segurança institucional para assuntos sobre segurança eletrônica nos Fóruns da RMF e do interior do estado constituem:

I - realizar o acompanhamento do videomonitoramento das unidades do TRT-7, devendo propor ações que possibilitem meios para atualização, ampliação e instalação de novos equipamentos e de tecnologias;

II - armazenar, catalogar e controlar imagens captadas pelo Sistema de Segurança Eletrônica (SSE);

III - administrar informações geradas pelo sistema de monitoramento, atuando para garantir o cumprimento das normas vigentes relativas à segurança institucional;

IV - gerenciar e fiscalizar as atividades de videomonitoramento realizadas no âmbito do TRT da 7ª Região;

V - gerar e/ou controlar registros de fatos relevantes ocorridos nas áreas internas e externas das edificações do TRT-7;

VI - elaborar e encaminhar relatórios e comunicados internos para conhecimento das chefias imediatas sobre fatos relevantes;

VII - participar ativamente da elaboração de projetos de sistemas de monitoramento, bem como acompanhar sua execução de modo a garantir sua eficiência;

VIII - deter o controle exclusivo sobre o armazenamento e o fornecimento de imagens captadas e gravadas pelos sistemas de monitoramento, de modo a garantir a segurança dos dados, bem como a legalidade de todos os atos necessários à gestão das informações;

IX - cumprir diligências para fins de fiscalização, acompanhamento e confecção de relatórios de todos os serviços realizados no âmbito de sua competência;

X - processar todas as imagens e as informações, cientificando à chefia imediata sobre quaisquer inconformidades, sobretudo no que se referem a eventuais interrupções, totais ou parciais, no funcionamento dos sistemas de monitoramento e no de vigília de perímetro;

XI - fornecer dados analíticos e informações para que a área de inteligência possa identificar e listar pessoas, veículos e outros objetos que devam ser acompanhados;

dos ou investigados preliminarmente por equipes da área de segurança institucional, tendo como finalidade a proteção de magistrados(as), servidores(as), advogados(as), terceirizados(as), estagiários(as), jurisdicionados(as), demais usuários(as) e o patrimônio da Justiça do Trabalho;

XII - fornecer registros e arquivos de situações e eventos relevantes que visem esclarecer fatos ocorridos no âmbito do TRT-7 e suas adjacências, obedecendo às previsões deste ato;

XIII - acompanhar equipes técnicas designadas, durante visitas às edificações do TRT-7, visando à correção de falhas de funcionamento nos equipamentos.

Seção II

Das Equipes de Videomonitoramento

Art. 5º As Equipes de Videomonitoramento da CMO serão constituídas por Agentes da Polícia Judicial, na quantidade de 1 (um) Coordenador e 2 (dois) Operadores por equipe, quando possível, e divididas em turnos de trabalho, respeitadas as jornadas diárias de 7 (sete) horas, as quais exercerão as atividades de operadores do Sistema de Segurança Eletrônica das edificações do TRT-7.

§ 1º Na ausência de efetivo suficiente para a composição das equipes, estas poderão ser complementadas nas atividades de operadores por servidores(as) terceirizados(as) contratados(as) especificamente para atuarem na área de segurança institucional.

§ 2º Os(As) servidores(as) de que trata o caput e o parágrafo § 1º deste artigo serão cientificados(as) formalmente sobre as obrigações que assumirão no exercício das atividades de coordenadores e de operadores do Sistema de Segurança Eletrônica, assinando para tanto termo nesse sentido, no qual constará as responsabilizações administrativas que poderão advir de atitudes adversas às normas previstas neste ato, sem prejuízo das demais de natureza civil e penal cabíveis.

Art. 6º O coordenador da equipe de operadores será designado(a) dentre os demais membros da área de segurança institucional, com conhecimentos comprovados sobre o serviço de segurança eletrônica, o qual deverá prestar assessoramento técnico nas questões referentes ao Sistema de Segurança Eletrônica das edificações do TRT-7, e terá as seguintes atribuições:

- I** - coordenar os serviços realizados pela Equipe;
- II** - cadastrar os(as) operadores(as) das equipes e manter atualizados os cadastros;
- III** - habilitar ou desabilitar códigos de operadores(a) e de administrador(a) de acesso;

IV - zelar pela segurança das imagens e das informações geradas pelo sistema de monitoramento;

V - verificar se a postura dos(as) operadores(as) é compatível com as exigências da função;

VI - garantir o cumprimento dos objetivos relativos ao gerenciamento, controle e fiscalização das atividades de monitoramento realizadas pela CMO;

VII - acompanhar a realização dos serviços executados de modo a garantir a qualidade e a eficiência necessárias ao êxito do monitoramento no âmbito das atividades de segurança eletrônica;

VIII - solicitar, sempre que necessário, providências e/ou recursos necessários ao bom andamento das atividades de monitoramento;

IX - manter-se atualizado sobre as instruções de segurança e zelar pelas suas aplicações;

X - ministrar treinamento para os(as) novos(as) operadores(as) ou quando forem adicionadas novas tecnologias;

XI - realizar, em parceria com a área de inteligência da segurança institucional, avaliação dos(as) servidores(as) terceirizados(as) que terão acesso ao SSE;

XII - reportar à chefia imediata os fatos relevantes envolvendo as atividades realizadas, bem como qualquer situação de irregularidade, encaminhando relatórios estatísticos quanto ao funcionamento dos sistemas e registros de ocorrências;

XIII - cumprir, no que couber e quando aplicável, as demais atribuições do cargo de Agente da Polícia Judicial.

Art. 7º Os(As) Agentes da Polícia Judicial e os(as) servidores terceirizados(as) que integrarão as equipes de videomonitoramento, como operadores(as), terão como principais atribuições:

I - operar os equipamentos do sistema de monitoramento com esmero, habilidade e perícia, sendo responsável pelo controle e sigilo de suas senhas;

II - realizar, logo no início do expediente, inspeção de segurança em todo o sistema de videomonitoramento e em suas respectivas instalações, com vista a detectar ou identificar quaisquer irregularidades, efetuando as devidas comunicações para a solução imediata das que forem encontradas;

III - ajustar periodicamente as câmeras, conforme a intensidade de luz de cada ambiente monitorado, a fim de melhorar a qualidade da imagem;

IV - acompanhar o monitoramento, durante o horário de expediente, em sistema de escala, observar os monitores e fiscalizar o sistema de gravação, para alertar e chamar a atenção dos(as) agentes da Polícia Judicial e dos(as) servidores(as) terceirizados(as), nos diferentes postos, quando da ocorrência de quaisquer irregularidades, atitudes suspeitas, sinistros e de comportamentos inadequados detectados dentro das dependências do TRT-7;

V - realizar backup das imagens captadas em local próprio, ao término do expediente diário, efetuando diligências de recuperação e, quando aplicável e expressamente autorizado, fazer gravações de vídeos ou demais arquivos em mídias externas;

VI - preencher relatório de ocorrências para os principais eventos, procedimentos realizados, tarefas agendadas, irregularidades identificadas, dentre outras anotações que sejam importantes e merecem ser de conhecimento da chefia imediata, dos(as) agentes da Polícia Judicial e dos(as) servidores(as) terceirizados(as) que estiverem operando o sistema de monitoramento;

VII - acompanhar as visitas técnicas de manutenções, atualizações e aprimoramentos técnicos, devidamente agendadas e identificados por meio de credenciais da empresa contratada os(as) seus(suas) responsáveis;

VIII - controlar os bens que compõem a carga patrimonial da CMO e da Sala de Monitoramento do Fórum Autran Nunes;

IX - realizar solicitações de materiais de consumo e/ou de uso permanente junto às suas chefias imediatas;

X - digitalizar os comunicados internos, classificá-los e encaminhá-los adequadamente;

XI - atualizar diariamente os dados dos relatórios gerados, conforme as informações fornecidas pelo sistema;

XII - não explorar falhas ou vulnerabilidades porventura existentes nos sistemas;

XIII - manter suas senhas de acesso secretas e não compartilhar com terceiros(as) as suas credenciais de segurança;

XIV - não permitir ou colaborar com o acesso à CMO, à Sala de Monitoramento do Fórum Autran Nunes, aos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do Estado e aos sistemas de monitoração por parte de pessoas não autorizadas, sob pena de ser corresponsabilizado(a) pelos eventuais problemas que esses acessos vierem a causar;

XV - manter descrição quanto a tudo o que foi visto e observado no decorrer da monitoração, vedados quaisquer comentários e especulações ociosas e desnecessárias;

XVI - respeitar os limites de sua autorização de acesso ou conta;

XVII - não interferir ou interromper a operação normal do sistema ou da rede;

XVIII - não burlar a operação normal dos mecanismos de proteção do computador, terminal, rack, dos ativos de rede, etc;

XIX - não conectar fisicamente ou remotamente nenhum componente externo, como modem, pendrive, disco rígido (hard disk – hd) externo e computadores, sem uma autorização formal específica;

XX - não acessar websites proibidos ou que não tenham finalidade com a segurança institucional;

XXI - não utilizar a rede de conexão da área de segurança institucional para fins particulares;

XXII - não manusear líquidos ou alimentos ao utilizar os equipamentos de monitoramento;

XXIII - não utilizar ferramentas ou explorar funcionalidades dos sistemas para fins de obtenção de dados de autenticação de usuários(as);

XXIV - utilizar apenas produtos de software com as licenças de uso válidas;

XXV - cumprir as condições de acesso ao Sistema de Segurança Eletrônica expressas em termo de responsabilidade;

XXVI - respeitar os direitos de propriedade intelectual e imagem e de tratamento de dados pessoais, de acordo com a regulamentação pertinente, em particular a lei de direitos autorais (Lei nº 9.610, de 19 de fevereiro de 1998) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018);

XXVII - cumprir, no que couber e quando aplicável, com as demais atribuições do cargo de Agente da Polícia Judicial ou constantes em contrato.

Art. 8º Poderá haver a concessão de acesso ao sistema ao(à) servidor(a) efetivo(a) pertencente aos quadros do TRT-7 que seja lotado na área de segurança institucional, para o acompanhamento específico de imagens de ambientes sensíveis de sua responsabilidade, a exemplo de almoxarifado geral ou da tecnologia da informação, aos quais será dada a denominação de “usuários(as)”.

§ 1º Os acessos de visualização fornecidos aos(às) usuários(as) não terão a permissão de armazenamento de imagens.

§ 2º Aos(às) usuários(as) serão definidas as atribuições semelhantes aos(às) dos(as) operadores, no que couber, respeitadas as suas limitações de acesso e a estrutura e o cotidiano de suas áreas monitoradas.

Art. 9º O(A) coordenador(a), o(a) operador(a) e o(a) usuário(a) devem zelar pela informação obtida por meio do Sistema de Segurança Eletrônica, que terá acesso no exercício de suas atribuições funcionais, e ser responsável pelo seu correto manuseio, armazenamento, transmissão, transporte e confidencialidade, conforme suas atribuições definidas neste ato.

Art. 10. As representações da área de segurança institucional para assuntos sobre segurança eletrônica nos Fóruns da RMF e do interior do Estado possuirão o status de operador(a).

CAPÍTULO IV

DO FORNECIMENTO DE IMAGENS E DE INFORMAÇÕES

Art. 11. A Central de Monitoramento e Operacionalização, a Sala de Monitoramento do Fórum Autran Nunes e as representações da segurança institucional nos fóruns da RMF e do interior do estado fornecerão imagens e informações, conforme procedimentos definidos por este ato, mediante emissão de TERMO DE COMPROMISSO a ser assinado pelo(a) requisitante no ato do recebimento do material contendo as gravações, após análise dos fundamentos de seu requerimento.

Parágrafo único. No Termo de Compromisso referido no caput deste artigo constarão:

- a) descrição sucinta das informações disponibilizadas;
- b) tipo de mídia no qual os dados foram gravados;
- c) destinação – conforme documento de solicitação;
- d) identificação completa do(a) solicitante/recebedor(a) (nome, Registro Geral (RG), Cadastro de Pessoa Física (CPF), contatos e endereço), com a entrega de cópias para compor o processo de fornecimento, ou da pessoa por ele formalmente autorizada para o recebimento, quando aplicável;
- e) outras informações julgadas relevantes em face das peculiaridades do caso concreto.

Art. 12. Apenas servidores(as) do TRT-7 e que estejam enquadrados na Seção II do Capítulo III deste ato têm legitimidade para copiar e processar as imagens armazenadas

e realizar os demais procedimentos técnicos relacionados ao manuseio do material que contém as referidas imagens, devendo todas as ações serem registradas e documentadas

Art. 13. Todos(as) os(as) servidores(as) efetivos(as) e terceirizados(as) envolvidos(as) nas atividades de videomonitoramento deverão prezar pelo sigilo das informações, as quais, por serem de caráter restrito, somente sairão do espaço interno da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do estado:

I - para trâmite interno: mediante expressa autorização da área de segurança institucional e das Diretorias dos Fóruns, devendo haver comunicação à Presidência do Tribunal sobre os fatos relevantes;

II - para trâmite externo: mediante expressa autorização da Presidência do Tribunal, depois de avaliados os fundamentos do requerimento apresentado e a análise técnica da área de segurança institucional, a qual contará com parecer da sua Seção de Inteligência.

Art. 14. O acesso às imagens e informações somente será permitido:

I - para cumprir as atribuições da segurança institucional do Tribunal, principalmente nos fatos que alterem o cotidiano de segurança das unidades ou que envolvam o conhecimento de ações de mera identificação de pessoas ou objetos, sem o registro de imagens, cujas autorizações podem ser concedidas pelas chefias da área de segurança no Complexo Sede e no Complexo do Fórum Autran Nunes ou seus representantes nas unidades da RMF e do interior;

II - para atender, na forma da lei, às necessidades de investigação administrativa ou criminal, cujas autorizações devem ser concedidas pelos(as) magistrados(as) dos fóruns, com a comunicação à Presidência do Tribunal;

III - para atender ao interesse público, principalmente no que concerne aos processos judiciais de responsabilidade da Justiça do Trabalho, cujas autorizações devem ser concedidas pelos(as) magistrados(as) dos fóruns, com a comunicação à Presidência do Tribunal;

IV - Por ordem da Presidência ou da Diretoria-Geral e, para os demais casos, por requisição nos termos dos arts. 11 e 12 deste ato.

CAPÍTULO V

DOS NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 15. A classificação da informação gerada pelo sistema de videomonitoramento será estipulada pelo seu(sua) operador(a), que são divididas em:

I - nível de alto risco: são informações estratégicas, confidenciais e de sigilo

absoluto, as quais são protegidas do acesso externo;

II - nível de uso restrito: são informações para áreas ou grupo de pessoas com nível confidencial de menor risco, as quais são protegidas do acesso externo, excetuando os casos de investigação policial;

III - nível de uso interno: são informações voltadas para os(as) dirigentes e os(as) servidores(as). Deve ser evitado o acesso externo a essas informações, mas se por acaso essas informações vazarem para o público externo, as consequências não serão críticas;

IV - nível de uso público: são informações direcionadas especificamente para outros órgãos públicos, fornecedores(as) e para terceiros(as), são informações que não precisam de nenhum sigilo, podendo ser de livre acesso para todos(as), não necessitando de nenhum investimento de recursos para sua proteção.

CAPÍTULO VI DO CICLO DE VIDA DA INFORMAÇÃO

Art. 16. O ciclo de vida é identificado e composto pelos momentos em que a informação é colocada em risco, a saber:

I - manuseio da informação: é o momento em que ela é criada ou manipulada, seja na hora em que se utiliza uma senha de acesso para deferimento ou autenticação ou digitar qualquer informação gerada recentemente;

II - armazenamento da informação: é o momento em que ela é guardada ou armazenada em mídia portátil, a exemplo de pendrive, HD externo, banco de dados compartilhado, entre outros;

III - transporte da informação: é o momento em que ela é distribuída (enviada ou transportada), seja falar ao rádio ou por telefone da instituição sobre uma informação confidencial, postar um documento ou encaminhar por correio eletrônico (*e-mail*);

IV - descarte da informação: é o momento em que ela é expurgada, deletada ou descartada pela perda de sua utilidade, seja deletando um arquivo de seu computador, colocando na lixeira de sua mesa um documento impresso ou expurgando uma mídia usada que teve falha na leitura.

CAPÍTULO VII DA CÓPIA DE SEGURANÇA E DA RESTAURAÇÃO

Art. 17. As cópias de segurança devem ser armazenadas em ambiente seguro e distinto daquele onde se encontram as informações originais, em locais ou dispositivos que minimizem a exposição e o manuseio das mídias.

§ 1º Devem ser mantidas cópias de todos os dados necessários a manutenção, em local alternativo, para garantir sua continuidade em casos de contingência.

§ 2º Os servidores e as mídias contendo cópia de segurança de arquivos devem ser mantidos em ambientes distintos e de acesso restrito. Sempre que o valor da informação o exigir, deve ser efetuada cópia de segurança adicional, que também deverá ser armazenada em local distinto.

Art. 18. Os dados/arquivos digitais de cunho institucional e de interesse do TRT-7 deverão ser armazenados dentro de ambiente seguro da área de segurança institucional e das diretorias dos fóruns da RMF e do interior do estado ou de outro local determinado pela administração superior, com o devido registro de recebimento pelo(a) seu(sua) responsável designado(a).

§ 1º Nas hipóteses em que for necessário o armazenamento dos dados de cunho institucional nas estações de trabalho dos(as) operadores(as) do sistema, a sua guarda ficará sob a responsabilidade dos referidos operadores(as).

§ 2º Em razão do volume, o armazenamento de dados de multimídia, por meio da infraestrutura da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do estado, que não forem relacionados à atividade fim do Tribunal, estará sujeito à análise prévia e autorização pela área de segurança institucional e pela diretorias dos fóruns e a devida anuência da Presidência do Tribunal.

§ 3º É vedado o armazenamento de dados pessoais na infraestrutura da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos fóruns da RMF e do interior do estado.

Art. 19. A equipe responsável pelo serviço deve:

I - definir e disponibilizar a estrutura necessária à execução dos serviços de acordo com o volume de dados, a necessidade de armazenamento e a tempestividade de disponibilização das informações;

II - certificar-se da compatibilidade entre as versões e os tipos de softwares utilizados na geração e restauração das cópias de segurança.

CAPÍTULO VIII DO CONTROLE DE ACESSO

Art. 20. O acesso ao sistema e aos equipamentos da segurança eletrônica do TRT-7 dar-se-á por meio do cabeamento próprio estruturado, interno das edificações, e por *link* de comunicação (*internet*) de uso exclusivo da área de segurança institucional

ou administrado pela área de tecnologia da informação do Tribunal, com a utilização de procedimentos e mecanismos definidos por suas áreas técnicas.

Art. 21. A criação de credenciais de magistrados(as), servidores(as) e de estagiários(as) para acesso aos ativos do Sistema de Segurança Eletrônica (SSE), requer procedimentos prévios de registro e identificação perante à área de segurança institucional.

Art. 22. A criação de contas para acesso aos ativos do SSE:

I - para profissionais terceirizados(as) requer autorização do(a) gestor(a) do contrato e deverá seguir os procedimentos definidos neste ato;

II - para representantes de outros órgãos públicos requer autorização da Presidência do TRT-7 e deverá seguir os procedimentos definidos neste ato.

Art. 23. O acesso às contas de coordenadores(as), operadores(as) e de usuários(as) aos ativos e às instalações físicas da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do estado, deverá ser revogado ou suspenso quando não mais necessário.

Art. 24. As credenciais de acesso às contas individuais do SSE são únicas, pessoais e intransferíveis.

Art. 25. Caberá à área de segurança institucional:

I - manter cadastro atualizado com dados dos(as) servidores(as) que exerçam funções de administração do Sistema de Segurança Eletrônica;

II - estabelecer procedimentos auditáveis para credenciamento, bloqueio e exclusão de contas de acesso dos(as) usuários(as) aos equipamentos do SSE que possuem esta possibilidade;

III - registrar os acessos aos equipamentos do SSE de forma a permitir a rastreabilidade e a identificação dos(as) administradores(as) e dos(as) usuários(as) por período mínimo de 2 (dois) anos.

Art. 26. As senhas de acesso aos ativos de informação do Sistema de Segurança Eletrônica que forem cadastradas pelos(as) administradores(as) e pelos(as) usuários(as) deverão conter 8 (oito) caracteres, pelo menos, sendo obrigatório combinações de letras, números e caracteres especiais.

Parágrafo único. A senha deverá ser trocada a um período não inferior a 180 (cento e oitenta dias, época em que será notificada a sua expiração pelo sistema.

CAPÍTULO IX

DA MANUTENÇÃO E DO SUPORTE TÉCNICO

Art. 27. As empresas contratadas para este fim farão suporte e manutenção somente nos equipamentos pertencentes ao patrimônio do Tribunal, enquanto que os constantes em contrato de locação ficarão sob a responsabilidade das empresas contratadas.

Art. 28. Não é permitida a manutenção em equipamentos que não façam parte do cadastro de material permanente do TRT-7; entretanto, poderá haver previsão no contrato de locação da possibilidade de realização de manutenções corretivas em equipamentos pertencentes ao Tribunal, caso a contratada possua conhecimentos técnicos comprovados.

Art. 29. A manutenção dos dispositivos pessoais de armazenamento de dados externos e dos dados neles armazenados, cujo uso esteja devidamente autorizado dentro das dependências da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos fóruns da RMF e do interior do estado, é de responsabilidade de seus(suas) proprietários(as), não cabendo à área de segurança institucional prestar suporte e recuperação de dados para esses tipos de mídias.

Art. 30. As solicitações de suporte e manutenção em equipamentos e sistemas pertencentes ao Tribunal deverão ser direcionadas pela coordenação das equipes de videomonitoramento e diretores de secretaria à área de segurança institucional.

Parágrafo único. As solicitações de suporte e manutenção para os locados deverão ser enviadas à(s) contratada(s) pelos canais disponibilizados para esta finalidade.

Art. 31. É vedada a intervenção, manuseio ou abertura de qualquer equipamento do Sistema de Segurança Eletrônica que não seja do conhecimento e autorizado pela área de segurança institucional ou pela empresa contratada.

Art. 32. É vedada a instalação e uso nos equipamentos da CMO, da Sala de Monitoramento do Fórum Autran Nunes e dos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do estado de qualquer aplicativo ou sistema operacional que não sejam aqueles definidos ou autorizados pela área de segurança institucional ou pela empresa contratada.

Art. 33. Os serviços de expansão, atualização, substituição ou de manutenção dos equipamentos do Sistema de Segurança Eletrônica somente serão realizados por empresa devidamente contratada para esse fim.

CAPÍTULO X

DO USO DA REDE DO SISTEMA DE SEGURANÇA ELETRÔNICA

Art. 34. O uso da rede disponibilizada para manuseio do Sistema de Segurança Eletrônica deverá seguir fielmente todas as obrigações constantes deste ato, bem como

as diretrizes constantes da Política de Privacidade e Proteção de Dados Pessoais do Tribunal Regional do Trabalho da 7ª Região (Resolução Normativa TRT7 Nº 1/2021), da Política de Segurança da Informação e Comunicações (POSIC) do Tribunal Regional do Trabalho da 7ª Região (Resolução Normativa TRT7 Nº 5/2023) e Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação (Ato TRT7 Nº 340/2023).

CAPÍTULO XI

DA UTILIZAÇÃO DO *LINK* DE COMUNICAÇÃO (*INTERNET*)

Art. 35. A utilização do *link* de comunicação, disponibilizado por empresa contratada (*Internet*) ou pela SETIC, para o exercício das atividades do Sistema de Segurança Eletrônica do Tribunal Regional do Trabalho da 7ª Região (SSE/TRT7), será realizada observando-se as regras estabelecidas neste ato.

Art. 36. O *link* de comunicação fornecido por empresa contratada será gerenciado exclusivamente pela área de segurança institucional e não terá integração com o da rede do Tribunal, excetuando casos específicos determinados pela Presidência.

Art. 37. A comunicação entre a rede do Tribunal e o *link* de comunicação do SSE, quando ocorrer, deverá ser mantida de forma a promover, unicamente, a prestação dos serviços definidos para o referido sistema.

Art. 38. A utilização do *link* de comunicação por meio da rede do Tribunal deverá ser controlada por sessão de acesso, com autenticação individual do equipamento e do(a) usuário(a) e por meio de mecanismos e procedimentos definidos pela SETIC e autorizados pela Administração do TRT-7.

Art. 39. Os relatórios individualizados de utilização do *link* de comunicação serão registrados em sistema próprio e ficarão disponíveis para monitoramento.

Art. 40. É permitida a utilização do *link* de comunicação para acesso de informações e de serviços de caráter funcional, voltadas às atividades do SSE/TRT7, desde que a frequência do uso e a quantidade de dados transmitidos não prejudiquem o desempenho e a segurança do sistema e a sua produtividade.

Art. 41. Observadas as normas de utilização do *link* de comunicação para o Sistema de Segurança Eletrônica, os(as) servidores(as) terceirizados(as) poderão ter acesso durante o período de prestação dos serviços, mediante solicitação justificada à área de segurança institucional.

Art. 42. No intuito de preservar a confidencialidade, a integridade e a disponibilidade dos canais de acesso ao *link* de comunicação do SSE/TRT7, fica vedado o acesso aos seguintes sites ou serviços:

I - serviços de compartilhamento de arquivos como Infnit, WeTransfer, Itnsfr, Sendspace, DropSend, WikiSend, Medifire, BearShare, Emule, IMesh, Kazaa, LimeWire, Morpheus, entre outros;

II - serviços de mensagens instantâneas não institucionais, como Instant Messenger, ICQ, MSN Messenger, Skype, Yahoo Messenger, Facebook Messenger, Whatsapp, entre outros;

III - sites de comunidades sociais não institucionais, como Facebook, LinkedIn, Twitter, Instagram, Snapchat, Myspace, entre outros;

IV - serviços de mascaramento proxies e tunelamento http não autorizados pelo Tribunal;

V - sites de compra e venda de ações (Home-Broker) de bancos e corretoras de valores.

§ 1º O disposto nos incisos de I a V deste artigo não se aplica a conteúdos disponíveis em páginas de instituições identificadas pelas terminações “.jus.br”, “.gov.br” e “.edu.br”.

§ 2º O acesso aos conteúdos relacionados neste artigo será bloqueado, tanto quanto possível, não isentando, porém, o(a) usuário(a) da responsabilidade em acessá-los quando não houver bloqueio previsto ou praticável.

Art. 43. Pedidos de acesso a sites e serviços vedados, em situações urgentes e com acesso temporário para atendimento de demanda específica, deverão ser precedidos de solicitação justificada, encaminhada à área de segurança institucional e que submeterá ao Comitê de Segurança Institucional, com a necessidade de ratificação futura pela Presidência do Tribunal.

Art. 44. Ao(À) usuário(a) que descumprir as normas aqui estabelecidas, poderá ser imposto o bloqueio de acesso, sem prejuízo das demais penalidades legais cabíveis.

CAPÍTULO XII

DO ACESSO REMOTO PARA SUPORTE TÉCNICO

Art. 45. O acesso remoto aos equipamentos do Sistema de Segurança Eletrônica do TRT-7, tem por finalidade diminuir a necessidade do deslocamento do(a) operador(a) e da equipe de manutenção preventiva e corretiva de sua localidade até onde estejam instalados os equipamentos do Sistema de Segurança Eletrônica do TRT-7.

§ 1º O acesso remoto somente será efetuado a partir de equipamentos de propriedade ou de uso do TRT-7 e de empresa contratada, com o intuito de prestar suporte e promover a solução de problemas registrados formalmente por usuário(a).

§ 2º A liberação de acesso remoto dar-se-á mediante equipamentos autorizados pelas áreas de segurança institucional e de tecnologia da informação, no caso de uso de rede do tribunal, e com o conhecimento prévio do(a) usuário(a) para acompanhamento.

§ 3º À pessoa que realizar o acesso remoto é vedado:

I - acesso sem finalidade específica de prestar suporte, na forma regulamentada por este ato ou em norma da SETIC;

II - visualizar conteúdo lógico contido no equipamento por curiosidade ou por má-fé;

III - alterar ou adulterar conteúdo lógico de equipamento do Tribunal sem autorização;

IV - obter cópia de conteúdos protegidos ou não, sem autorização;

V - fazer cópias sem autorização;

VI - sabotar ou interromper intencionalmente o funcionamento de Sistema de Segurança Eletrônica;

VII - qualquer ação que comprometa a segurança do SSE do TRT-7, do equipamento acessado e das informações nele disponíveis.

§ 4º O acesso remoto em equipamentos da empresa contratada, sem autorização expressa do(a) usuário(a), será realizada somente em regime de exceção, mediante autorização da área de segurança institucional, por meio do(a) seu(sua) gestor(a).

CAPÍTULO XIII

DO GESTOR DO SISTEMA DE SEGURANÇA ELETRÔNICA

Art. 46. O(A) gestor(a) do Sistema de Segurança Eletrônica será servidor(a) da área de segurança institucional designado(a) pela Presidência do Tribunal, a quem caberá:

I - definir formalmente os perfis de acesso às suas instalações, equipamentos, ações e material desenvolvido pelo sistema;

II - definir e atribuir as restrições de acesso às suas ações para cada unidade organizacional;

III - definir, após análise do Comitê de Segurança Institucional, quais gabinetes, diretorias e/ou setores devem utilizar as operações dos seus aplicativos e disponibilizá-las;

IV - manter atualizada a relação de liberações de uso e auditar as utilizações;

V - definir quais de suas operações devem ser executadas com o uso de senhas e qual nível operacional deve ser vinculada às equipes de videomonitoramento;

VI - definir o nível de classificação das operações dos seus aplicativos, segundo as normas de classificação da informação;

VII - definir e determinar a implementação de registros de auditoria das operações dos seus aplicativos e o prazo de retenção desses registros;

VIII - monitorar o uso dos seus aplicativos;

IX - autorizar o fornecimento de informações sobre os registros de auditoria das suas operações.

CAPÍTULO XIV

DISPOSIÇÕES FINAIS

Art. 47. O acesso e a permanência na sala da CMO, na Sala de Monitoramento do Fórum Autran Nunes e nos ambientes destinados para esta natureza nos Fóruns da RMF e do interior do estado serão permitidos, exclusivamente, aos(às) servidores(as) que exercem atividades no Sistema de Segurança Eletrônica, aos(às) profissionais da sua área de manutenção preventiva e corretiva e às pessoas devidamente autorizadas pela área e segurança institucional, exceto os casos determinados pela Presidência do Tribunal .

Art. 48. Devido às questões de afastamento obrigatório por parte dos membros das equipes de videomonitoramento, deverá ser constituído cadastro de reserva de pessoal habilitado a substituir e a operar o Sistema de Segurança Eletrônica.

Art. 49. Os(Os) servidores(as) terceirizados(as) contratados(as) para a realização de vigilância armada podem operar equipamentos disponibilizados pelo TRT-7 para promover a segurança institucional, conforme previsão em cláusula contratual, cujo treinamento para uso será ministrado pelos membros da CMO, da Sala de Monitoramento do Fórum Autran Nunes e das representações da segurança institucional nos Fóruns da RMF e do interior do estado, bem como por profissionais designados(as) pelas empresas contratadas para prestação de serviços em comodato.

Art. 50. O ramal telefônico disponibilizado para a CMO e para a Sala de Monitoramento do Fórum Autran Nunes deverá ser utilizado, única e exclusivamente, para as atividades profissionais, ficando terminantemente proibido o uso para assuntos que não sejam do interesse institucional e que possam trazer prejuízo ao atendimento das obrigações das unidades mencionadas.

Art. 51. Avisos serão afixados em locais de fácil visualização, informando sobre o monitoramento através de Sistema de Segurança Eletrônica.

Art. 52. As imagens e as informações gravadas pelo Sistema de Segurança Eletrônica são de caráter reservado e deverão ser armazenados com segurança e mantidos à disposição por período mínimo de:

I - 30 (trinta) dias em equipamentos de armazenamento instalados em unidades do Tribunal, quando se tratar de imagens;

II - 6 (seis) meses em equipamentos de armazenamento instalados em unidades do Tribunal, quando se tratar de informações;

III - 15 (quinze) dias, no mínimo, em equipamentos de armazenamento pertencentes à empresa contratada para prestação do serviço em comodato, quando se tratar de imagens.

Art. 53. É vedado o acesso, armazenamento, transmissão e transporte de conteúdo considerado incompatível com a moralidade administrativa, com as atividades funcionais ou com o Plano de Segurança Institucional, instituído pela Resolução Normativa TRT7 nº 20, de 10 de dezembro de 2023.

Art. 54. É vedado promover ações que, intencionalmente, comprometam os dispositivos e as tecnologias do Sistema de Segurança Eletrônica do TRT-7 e das informações neles disponíveis, cuja infração a esta regra poderá gerar responsabilizações administrativas, sem prejuízo das demais penalidades legais cabíveis.

Art. 55. Fica revogado o Ato TRT7 nº 51, de 4 de abril de 2017.

Art. 56. Este Ato entra em vigor na data de sua publicação.

Fortaleza, 16 de dezembro de 2024.

DURVAL CÉSAR DE VASCONCELOS MAIA

Presidente do Tribunal