PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 51/2017

Institui a Central de Monitoramento e Operacionalização da Segurança Institucional do TRT da 7ª Região e dá outras providências.

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

CONSIDERANDO as determinações de adoção de providências para a instalação de Sistema de Segurança Eletrônico, bem como circuito fechado de televisão e monitoramento, contidas na Resolução CNJ nº 104/2010 (art. 1º, inciso II), na Resolução CNJ nº 176/2013 (art. 9º, inciso III) e na Resolução CSJT nº 175/2016 (art. 1º, inciso III);

CONSIDERANDO o conteúdo da Resolução TRT7 nº 313/2010, a qual trata sobre a Política de Segurança Institucional do Tribunal Regional do Trabalho da 7ª Região;

CONSIDERANDO que, em 2014, por ocasião da análise do ambiente interno do TRT7, que precedeu ao Plano Estratégico Institucional 2015-2020, a segurança (ou mais propriamente, a falta dela) foi considerada uma fraqueza do Tribunal;

CONSIDERANDO os projetos contratados para a implantação e a atualização do sistema de CFTV /Alarmes/Controle de Acesso/Detecção de Incêndio do Tribunal Regional do Trabalho da 7ª Região, de que trata o Processo nº 10.176/2012, onde existe a previsão de uma sala de monitoramento para o controle do conjunto;

CONSIDERANDO a recente aquisição feita por este Regional de um Sistema Integrado de Segurança Eletrônica, composto por sistema de videomonitoramento e seus equipamentos, softwares com licença de uso, serviços de instalação, configuração e manutenção corretiva durante o período de garantia, para o Complexo Sede do TRT7, conforme Processo nº 2449/2016,

R E S O L V E:

CAPÍTULO I
DA CENTRAL DE MONITORAMENTO E OPERACIONALIZAÇÃO

Art. 1º Fica instituída a Central de Monitoramento e Operacionalização (CMO), subordinada diretamente à Divisão de Segurança e Transporte (DSET), que tem por finalidade o assessoramento técnico e operacional relativo à segurança institucional dentro das áreas internas e adjacentes do Tribunal Regional do Trabalho da 7ª Região (TRT7), com a utilização de equipamentos de vigilância eletrônica instalados em pontos estratégicos das edificações do TRT7, os quais permitirão o acesso remoto às áreas sensíveis e o reforço das que não se encontram totalmente cobertas pelas atividades exercidas pela DSET.

§ 1º A CMO será diretamente responsável por armazenar, catalogar e controlar imagens captadas pelo Sistema de Segurança Eletrônica(SSE), bem como pelo fornecimento de registros e arquivos de situações e eventos relevantes que visem esclarecer fatos ocorridos no âmbito do TRT7 e suas adjacências e dados analíticos e informações para que a área de inteligência possa identificar e listar pessoas, veículos e outros objetos que devam ser acompanhados ou investigados preliminarmente por equipes da DSET, tendo como finalidade a segurança institucional e dos usuários dos serviços da Justiça do Trabalho.

§ 2º O videomonitoramento será realizado por câmeras de segurança instaladas nas edificações do TRT7 e conectadas a dispositivos digitais de armazenamento de imagens em ambiente próprio da CMO.

§ 3º A CMO realizará o videomonitoramento de todas as unidades do TRT7, devendo propor ações que possibilitem meios para ampliação e instalação de novos equipamentos e tecnologias.

CAPÍTULO II
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º O usuário deve zelar pela informação obtida pelo Sistema de Segurança Eletrônica, que terá acesso no exercício de suas atribuições funcionais, e ser responsável pelo seu correto armazenamento, transmissão, transporte e confidencialidade.

Art. 3º É vedado o acesso, armazenamento, transmissão e transporte de conteúdo considerado incompatível com a moralidade administrativa, com as atividades funcionais ou com a Política de Segurança Institucional.

Art. 4º É vedado promover ações que, intencionalmente, com prometam a segurança do sistema e equipamentos de CFTV da Justiça do Trabalho da 7ª Região e das informações neles disponíveis.

CAPÍTULO III
DOS CONCEITOS

Art. 5º Para fins desta Norma de Segurança, considera-se:

I - CFTV: componente do Sistema de Segurança Eletrônica com câmeras especiais, transmitindo imagens de pontos estratégicos para uma central de monitoramento, onde as imagens são acompanhadas, em tempo real, possibilitando ações imediatas caso aconteça alguma anormalidade;

II - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, o cadastramento de código de identificação e definição de perfil de acesso aos recursos do sistema de monitoramento;

III - credenciais de acesso: permissões concedidas por autoridade competente, que habilitam determinada pessoa, sistema ou organização ao acesso à informação ou recurso. A credencial pode ser física, como crachá, cartão, token, selo ou lógica para identificação de usuários;

IV - perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

V - coordenador: Agente de Segurança Judiciária com poderes para realizar modificações nas configurações de programas e dispositivos de um equipamento, sejam estas provisórias ou permanentes, e fiscalizar as atividades desenvolvidas pelo Operador;

VI - operador: Agente de Segurança Judiciária responsável pelo a companhamento diário do Sistema de Segurança Eletrônica;

VII - usuário: pessoa que não compõe as equipes de videomonitoramento e a quem houve a concessão de acesso ao sistema.

CAPÍTULO IV
DAS ATRIBUIÇÕES

Art. 6º Constituem-se atribuições da Central de Monitoramento e Operacionalização:

I - administrar informações geradas pelo sistema de monitoramento, atuando junto à DSET para garantir o cumprimento das normas vigentes relativa s à segurança institucional, gerenciando e fiscalizando as atividades de videomonitoramento realizadas no âmbito do TRT7;

II - gerar e controlar registros de fatos relevantes o corridos nas áreas internas e externas das edificações do TRT7, elaborando e encaminhando relatórios e comunicados internos à DSET;

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

IV – deter o controle exclusivo sobre o armazenamento e 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;

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

VI – acompanhar equipes técnicas designadas pela DSET, durante visitas às edificações do TRT7, visando à correção de falhas de funcionamento nos equipamentos;

VII - processar todas as imagens e informações, cientificando à DSET sobre quaisquer inconformidades, sobretudo no que se referem a eventuais interrupções, totais ou parciais, no funcionamento dos sistemas de monitoramento.

Seção I
DAS EQUIPES DE VIDEOMONITORAMENTO

Art. 7º As Equipes de Videomonitoramento da Central de Monitoramento e Operacionalização (CMO) serão constituídas por Agentes de Segurança Judiciária efetivos, na quantidade mínimo de 01 (um) coordenador e 02 (dois) operadores por equipe, 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 TRT7.

Parágrafo único. Os servidores de que trata o deste artigo serão cientificados formalmente sobre as obrigações que irão assumir no exercício das atividades 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.

Subseção I
DA COORDENAÇÃO DAS EQUIPES

Art. 8º O Coordenador da equipe de operadores será designado dentre os demais membros da área de segurança da DSET, com conhecimentos comprovados sobre o

serviço de segurança eletrônica, o qual deverá prestar assessoramento técnico à DSET nas questões referentes ao Sistema de Segurança Eletrônica das edificações do TRT7, e terá as seguintes atribuições:

I - coordenar os serviços realizados pela Equipe;

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

III - reportar à DSET 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 realizados;

IV - cadastrar os operadores das equipes e manter atualizados esses cadastros;

V - habilitar ou desabilitar códigos de operadores e de administrador de acesso;

VI - garantir o cumprimento dos objetivos relativos a o 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, bem como verificar se a postura dos operadores é compatível com as exigências da função;

VIII - demandar sempre que necessário, junto à DSET, solicitação de 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 novos usuários ou quando for adicionado novas tecnologias;

XI - cumprir, no que couber e quando aplicável, com as demais atribuições do cargo de Agente de Segurança Judiciária.

Subseção II
DOS MEMBROS DAS EQUIPES

Art. 9º Os Agentes de Segurança Judiciárias que integrarão as Equipes de Videomonitoramento, como operadores, 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 sistema de videomonitoramento e suas respectivas instalações, com vista a detectar ou identificar quaisquer irregularidades, efetuando as devidas comunicações para a solução imediata das que forem encontradas;

III - 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 atenção dos Agentes, nos diferentes postos, quando da ocorrência de quaisquer irregularidades, atitudes suspeitas, sinistros, comportamentos inadequados de usuários da Justiça;

IV - 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;

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

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

VII - preencher relatório de ocorrências para os principais eventos, procedimentos realizados, tarefas agendadas, irregularidades identificadas, dentre outras anotações que sejam importantes e mereçam ser de conhecimento da Diretoria imediata ou dos Agentes de Segurança que estiverem operando o sistema de monitoramento;

VIII - acompanhar as visitas técnicas de manutenções, atualizações e aprimoramentos técnicos, devidamente agendadas e identificados funcionalmente os seus responsáveis;

IX - controlar os bens que compõem a carga patrimonial da CMO;

X - realizar solicitações de materiais de consumo e de uso permanente junto à DSET;

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

XII – atualizar diariamente os dados dos relatórios gerados conforme as informações fornecidas pelo sistema;

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

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

XV - não permitir ou colaborar com o acesso à Central e aos sistemas de monitoração por parte de pessoas não autorizadas, sob pena de ser corresponsabilizado pelos eventuais problemas que esses acessos vierem a causar;

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

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

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

XIX - não conectar fisicamente ou remotamente nenhum componente externo, como *modem*, *pendrive*, hd externo e computadores, sem uma autorização formal específica;

XX - respeitar os direitos de propriedade intelectual e imagem, de acordo com a regulamentação pertinente, em particular a lei de direitos autorais;

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

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;

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

XXV - cumprir, no que couber e quando aplicável, com as demais atribuições do cargo de Agente de Segurança Judiciária.

Seção II
DO FORNECIMENTO DE IMAGENS E DE INFORMAÇÕES

Art. 10. A Central de Monitoramento e Operacionalização fornecerá imagens e informações, conforme procedimento autorizado pela DSET, mediante emissão de TERMO DE COMPROMISSO a ser assinado pelo requisitante no ato do recebimento do material contendo as gravações.

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 do solicitante e/ou pessoa por ele formalmente autorizada;

e) outras informações julgadas relevantes em face das peculiaridades do caso concreto;

f) nome completo do solicitante e, quando aplicável, da pessoa por ele autorizada;

g) número de documento individual do solicitante e, quando aplicável, da pessoa por ele autorizada.

Art. 11. Apenas Agentes devidamente autorizados pela DSET 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 todo o serviço ser registrado e documentado.

Parágrafo único. Todos os servidores envolvidos nas atividades de videomonitoramento deverão prezar pelo sigilo das informações, as quais, por serem de caráter restrito, somente sairão do espaço interno da CMO mediante expressa autorização da DSET e anuência da Diretoria-Geral (DG).

Art. 12. O acesso às imagens e informações somente será permitido:

I - para cumprir as atribuições da DSET;

II - para atender, na forma da lei, as necessidades de investigação administrativa ou criminal;

III - para atender ao interesse público;

IV - por ordem da Presidência ou da Diretoria-Geral e, para os demais casos, por requisição, nos termos dos artigos 10 e 11 deste Ato.

CAPÍTULO V
DOS NÍVEIS DE CLASIFICAÇÃO DA INFORMAÇÃO

Art. 13. A classificação da informação gerada pelo sistema de videomonitoramento será estipulada pelo seu operador, que são subdivididas em:

I - nível de alto risco: são informações estratégicas, confidenciais e de sigilo absoluto. Elas são protegidas do acesso externo;

II - nível de uso restrito: são informações para áreas ou grupo de pessoas com um confidencial de menor risco;

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

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

CAPÍTULO VI
DO CICLO DE VIDA DA INFORMAÇÃO

Art. 14. O ciclo de vida é identificado e composto pelos momentos em que a informação é colocada em risco. Esses momentos são:

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, seja numa mídia de CD-ROM, pen drive ou em um banco de dados compartilhado.;

III - transporte da informação: É o momento em que ela é distribuída (enviada ou transportada), seja falar ao rádio ou 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 (CD-ROM) usada que teve falha na leitura.

CAPÍTULO VII
DA CÓPIA DE SEGURANÇA E DA RESTAURAÇÃO

Art. 15. 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.

Parágrafo único. Devem ser mantidas cópias de todos os dados necessários a manutenção, em local alternativo, para garantir sua continuidade em casos de contingência. Os servidores e respectivas mídias contendo cópia 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. 16. Os dados/arquivos digitais de cunho institucional e de interesse do TRT7 deverão ser armazenados dentro de ambiente seguro da DSET ou de outro local determinado pela Administração Superior, com o devido registro de recebimento pelo seu responsável designado.

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

§ 2º Em razão do volume, o armazenamento de dados de multimídia, por meio da infraestrutura da CMO, que não forem relacionados à atividade fim do Tribunal, estará sujeito à análise prévia e autorização pela DSET e devida anuência da Diretoria-Geral.

§ 3º É vedado o armazenamento de dados pessoais na infraestrutura da CMO.

Art. 17. A equipe responsável pelo serviço deve:

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

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

CAPÍTULO VIII
DO GESTOR DO SISTEMA DE SEGURANÇA ELETRÔNICA

Art. 18. O Gestor do Sistema de Segurança Eletrônica será a Diretoria da Divisão de Segurança e Transporte, 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 as suas ações para cada unidade organizacional;

III - definir, após análise do Comitê e da Comissão 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 IX
DO CONTROLE DE ACESSO

Art. 19. O acesso ao sistema e equipamentos da segurança eletrônica do Tribunal Regional do Trabalho da 7ª Região (TRT7) se dará somente por meio do cabeamento próprio estruturado, interno das edificações, com a utilização de procedimentos e mecanismos definidos pela Divisão de Segurança e Transporte.

Art. 20. A criação de credenciais de magistrados, servidores e estagiários para acesso aos ativos do Circuito Fechado de TV - CFTV, requer procedimentos prévios de registro e identificação junto à DSET.

Art. 21. A criação de contas para acesso aos ativos do CFTV:

I - para profissionais terceirizados requer autorização do gestor do contrato e deverá seguir os procedimentos definidos pela DSET;

II - para representantes de outros órgãos públicos requer autorização da Presidência e deverá seguir os procedimentos definidos pela DSET.

Art. 22. O acesso às contas de coordenadores, operadores e usuários, aos ativos e às instalações físicas da CMO, deverá ser revogado ou suspenso quando não mais necessário.

Art. 23. As credenciais de acesso às contas individuais do CFTV serão únicas, pessoais e intransferíveis.

Art. 24. Caberá à Divisão de Segurança e Transporte (DSET):

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

II - estabelecer procedimentos auditáveis para credenciamento, bloqueio e exclusão de contas de acesso dos usuários do CFTV;

III - registrar os acessos à rede do CFTV de forma a permitir a rastreabilidade e a identificação dos acessos dos administradores e usuários, por período mínimo de 2 (dois) anos.

Art. 25. As senhas de acesso aos ativos de informação do CFTV que forem cadastradas pelos administradores e usuários deverão conter pelo menos 08 (oito) caracteres, sendo obrigatório combinações de letras, números e caracteres especiais. A senha deverá ser trocada a um período não inferior a 180 (cento e oitenta) dias, período no qual será notificada a sua expiração pelo sistema.

CAPÍTULO X
DA MANUTENÇÃO E DO SUPORTE TÉCNICO

Art. 26. As empresas contratadas para este fim farão suporte e manutenção somente nos equipamentos pertencentes ao patrimônio do Tribunal.

Art. 27. Não é permitida a manutenção em equipamentos que não fazem parte do cadastro de material permanente.

Art. 28. A manutenção dos dispositivos pessoais de armazenamento de dados externos, cujo uso esteja devidamente autorizado dentro das dependências da CMO, e dos dados neles armazenados é de responsabilidade dos coordenadores e operadores proprietários, não cabendo a DSET prestar suporte e recuperação de dados para estes tipos de mídias.

Art. 29. As solicitações de suporte e manutenção em equipamentos e sistemas deverão ser direcionadas pela Coordenação das Equipes à DSET.

Art. 30. É vedada a intervenção, manuseio ou abertura de qualquer equipamento do Sistema de Segurança Eletrônica que não seja do conhecimento e autorizado pela DSET.

Art. 31. É vedada a instalação e uso nos equipamentos da CMO de qualquer aplicativo ou sistema operacional que não sejam àqueles definidos ou autorizados pela DSET.

Art. 32. Os serviços de expansão e atualização, substituição ou manutenção dos equipamentos do Sistema de Segurança Eletrônica somente serão realizado por empresa devidamente contratada para este fim.

CAPÍTULO XI
DAS PRESCRIÇÕES FINAIS

Art. 33. O acesso e a permanência na sala da CMO é permitido, exclusivamente, aos servidores que exercem atividades junto ao Sistema de Segurança Eletrônica, aos profissionais da sua área de manutenção preventiva e corretiva e às pessoas devidamente autorizadas pela Diretoria da DSET.

Parágrafo único. Excetuam-se os casos determinados pela Presidência ou pela Diretoria-Geral.

Art. 34. Devido às questões de afastamento obrigatório por parte dos membros das Equipes de Videomonitoramento, a DSET deverá constituir cadastro de reserva de pessoal habilitado a substituir e operar o Sistema de Segurança Eletrônica.

Art. 35. Os servidores terceirizados contratados para a realização de vigilância armada podem operar equipamentos disponibilizados pelo TRT7 para promover a segurança institucional, conforme previsão em cláusula contratual, cujo treinamento para uso será ministrado pelos membros da CMO.

Art. 36. O ramal telefônico disponibilizado para a CMO deve rá 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 da Central.

Art. 37. Serão afixados avisos em locais de fácil visualização, informando sobre o monitoramento através de Sistema de Segurança Eletrônica.

Art. 38. As imagens e 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 quando se tratar de imagens;

II - 6 (seis) meses quando se tratar de informações.

Art. 39. Este Ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza,04 de abril de 2017.
MARIA JOSÉ GIRÃO
Presidente do Tribunal