PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO – SEXTA REGIÃO
Gabinete da Presidência

ATO TRT-GP Nº 296/2017

Atualiza a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da Sexta Região, instituída pela Resolução Administrativa TRT nº 30/2009.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA SEXTA REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico eficiente e seguro, que favoreça as atividades jurisdicionais e administrativas deste Tribunal,

CONSIDERANDO a constante preocupação deste Regional com a integridade, qualidade, celeridade e credibilidade na prestação de serviços à sociedade,

CONSIDERANDO o dever da Administração de evitar que os serviços jurisdicionais e administrativos sejam prejudicados por ameaças provenientes do uso indevido da tecnologia da informação,

CONSIDERANDO a norma NBR ISO/IEC 27002:2005, a qual estabelece as boas práticas em segurança da informação e recomenda revisões periódicas da política de segurança de tecnologia de informação das instituições,

CONSIDERANDO, ainda, o contido no inciso II do artigo 8º da Resolução Administrativa TRT nº 30/2009,

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação, nos moldes descritos nos anexos a este Ato.

Art. 2º Ficam revogados os Atos TRT-GP nºs 314/2013, 408/2013, 153/2014.

Art. 3º Este Ato entra em vigor na data de sua publicação.

Recife, 17 de outubro de 2017.

IVAN DE SOUZA VALENÇA ALVES
Desembargador Presidente do TRT da Sexta Região

Anexo I - ATO TRT-GP Nº 296/2017

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

REFERÊNCIA NORMATIVA

Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política e Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Resolução nº 90, de 29 de setembro de 2009 do Conselho nacional de Justiça.

Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e suas normas complementares.

Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação / MPOG, de 12 de novembro de 2010.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

CAMPO DE APLICAÇÃO

Esta Política de Segurança da Informação se aplica a todos os usuários no âmbito do Tribunal Regional do Trabalho da 6ª Região.

SUMÁRIO

Anexo I - ATO TRT-GP Nº 296/2017

1 ESCOPO

1.1 Objetivos

Definir a estrutura, os princípios, as diretrizes e as responsabilidades referentes à segurança da informação no âmbito do Tribunal Regional do Trabalho da 6ª Região, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Tribunal.

1.2 Abrangência

Estas diretrizes abrangem todos os ambientes físicos formadores deste Regional e todas as pessoas que tenham acesso às informações e aos recursos de tecnologia da informação do Órgão, inclusive terceirizados, consultores, estagiários e demais colaboradores externos ou eventuais.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Política de Segurança da Informação (PSI) são estabelecidos os seguintes conceitos e definições:

2.1 **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

2.2 **Ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

2.3 **Ativos de informação**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

2.4 **Autenticidade**: asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino;

2.5 **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

2.6 **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

2.7 **Incidente de segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

2.8 **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

2.9 **Gestão da continuidade do negócio**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

2.10 **Gestão de riscos**: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. Geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

2.11 **Recurso de tecnologia da informação**: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação e as instalações físicas que os abrigam;

2.12 **Risco**: algo que pode ocorrer e seus efeitos interferem nos objetivos da organização. O risco é geralmente quantificado como uma média de seus efeitos, por meio da soma do efeito de todas as consequências possíveis ponderada pela probabilidade associada a cada consequência, de forma a obter um "valor esperado";

2.13 **Plano de continuidade do negócio**: conjunto de ações e procedimentos de recuperação a serem seguidos em uma eventual ocorrência de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos;

2.14 **Tratamento de incidentes**: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação prejudicial e também a identificação de tendências;

2.15 **Termo de Ciência**: termo assinado pelo usuário declarando ter ciência da Política de Segurança da Informação, bem como suas normas complementares, comprometendo-se a cumprir as diretrizes traçadas;

2.16 **Termo de Responsabilidade e Sigilo**: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

2.17 **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas; e

2.18 **Usuários**: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados, cedidos e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando os recursos tecnológicos deste Regional.

3 ESTRUTURA NORMATIVA

Os documentos que compõem a estrutura normativa são divididos em três categorias:

3.1 **Política de Segurança da Informação**: constituída do presente documento, define a estrutura, estabelece os princípios e as diretrizes, e define as responsabilidades referentes à segurança da informação;

3.2 **Normas Complementares**: estabelecem obrigações a serem seguidas de acordo com as diretrizes da PSI. A elaboração das normas seguirá as orientações definidas na Norma Complementar nº 01/IN01 do Departamento de Segurança da Informação e

Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR); e

3.3 **Procedimentos**: define as regras operacionais conforme o disposto nas diretrizes, nas normas e na política de segurança, permitindo sua utilização nas atividades do Tribunal.

4 PRINCÍPIOS

As ações relacionadas à segurança da informação são norteadas pelos seguintes princípios (sem prejuízo aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal):

4.1 **Alinhamento estratégico**: a PSI e as normas associadas devem estar alinhadas à missão institucional e seu planejamento estratégico;

4.2 **Conhecimento**: os usuários deverão tomar ciência de todas as normas de segurança da informação permitindo-lhes a execução de suas atribuições sem comprometer a segurança;

4.3 **Continuidade**: as ações de segurança da informação devem ser planejadas; implantadas, verificadas e, se necessário for, reestruturadas em períodos cíclicos e continuados;

4.4 **Privilégio mínimo**: as permissões concedidas a cada identidade devem ser as mínimas necessárias para o exercício do cargo, função ou papel do seu detentor;

4.5 **Proporcionalidade**: o nível, a complexidade e os custos das ações de segurança da informação serão proporcionais ao valor do ativo a proteger e ao seu grau de confidencialidade e de criticidade da informação;

4.6 **Propriedade da informação**: as informações, sistemas e métodos gerados ou criados pelos usuários, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são de propriedade do Tribunal;

4.7 **Responsabilidade**: todos os usuários são responsáveis pelo tratamento da informação e pelo cumprimento das normas de segurança da informação; e

4.8 **Uso exclusivo**: os recursos de tecnologia da informação pertencentes ao Tribunal, disponíveis aos usuários, deverão ser utilizados exclusivamente em atividades relacionadas às suas funções institucionais, visando a garantir a continuidade da prestação jurisdicional deste Tribunal.

5 DIRETRIZES GERAIS

Ficam estabelecidas as seguintes diretrizes gerais que devem subsidiar a elaboração das normas complementares:

5.1 **Tratamento da Informação**:

a) a informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do Tribunal;
b) os ativos de informação do Tribunal deverão ser identificados e classificados em

termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento; e

c) todo ativo de informação deve possuir um responsável explicitamente identificado.

5.2 **Tratamento de Incidentes**: os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, procurando extrair informações que permitam impedir a continuidade da ação prejudicial e também a identificação de tendências.

5.3 **Gestão de Risco**:

a) deve ser estabelecido um processo de Gestão de Riscos de Segurança da Informação com vistas a identificar e implementar as medidas de proteção necessárias para tratar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos; e

b) o processo deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação.

5.4 **Gestão de Continuidade**: deve ser estabelecida a Gestão de Continuidade de Negócio no âmbito do Tribunal visando aumentar a capacidade estratégica e tática de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

5.5 **Auditoria e Conformidade**: o cumprimento desta PSI deve ser avaliado, periodicamente, em conformidade com normas complementares, procedimentos e legislação relacionada à segurança da informação, buscando a certificação do atendimento aos requisitos estabelecidos.

5.6 **Controles de Acesso**:

a) devem ser instituídas normas que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, às instalações e aos sistemas de informação; e

b) deve ser conduzida a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.

5.7 **Uso de *e-mail***:

a) o serviço de correio eletrônico constitui recurso disponível na rede de comunicação de dados do Tribunal para aumentar a agilidade, segurança e economia da comunicação oficial e informal; e

b) destina-se o seu uso ao intercâmbio de informações oficiais e informais decorrentes das relações funcionais ou inerentes ao interesse do serviço, facultado o uso de caráter pessoal, somente nos casos de excepcional relevância.

5.8 **Acesso à *Internet***:

a) todos os usuários poderão ter acesso à *Internet*; e

b) para garantir a utilização adequada para fins diretos e complementares às atividades funcionais, poderão ser impostas limitações ao acesso.

6 PENALIDADES

A violação de um ou mais itens da PSI, bem como de suas normas complementares e procedimentos, poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais, assegurada aos envolvidos ampla defesa.

7 COMPETÊNCIAS E RESPONSABILIDADES

É de responsabilidade de todos que têm acesso aos ativos de informação do Tribunal manter níveis de segurança da informação adequados, segundo preceitos desta política. São definidas ainda as seguintes responsabilidades:

7.1 **À Presidência compete**:

a) estabelecer e manter atualizadas as diretrizes relativas à segurança da informação no âmbito deste Tribunal, divulgadas na Política de Segurança da Informação;
b) instituir e determinar a composição do Comitê Gestor de Segurança da Informação (CGSI); e
c) decidir sobre matérias referentes ao descumprimento da Política de Segurança da Informação e/ou normas, encaminhadas pelo Comitê Gestor de Segurança da Informação.

7.2 **Ao Comitê Gestor de Segurança da Informação do Tribunal compete**:

a) elaborar propostas de normas e políticas de uso dos recursos de informação;
b) rever periodicamente a política de segurança e normas a ela relacionadas, sugerindo possíveis alterações;
c) estabelecer diretrizes e definições estratégicas para a elaboração do Plano Diretor de Segurança da Informação;
d) dirimir dúvidas acerca da aplicação das normas de segurança da informação deste Tribunal, submetendo à deliberação da Presidência as situações não contempladas pela política e estrutura normativa vigentes;
e) propor e acompanhar planos de ação para aplicação desta política, assim como campanhas de conscientização dos usuários;
f) receber as comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal, instruindo-as com os elementos necessários à sua análise e apresentando parecer à autoridade competente;
g) solicitar, sempre que necessário, a realização de auditorias à área de segurança da informação, referentes ao uso dos recursos de tecnologia da informação no âmbito do Tribunal;
h) avaliar relatórios e resultados de auditorias apresentados pela área de Segurança da Informação;
i) apresentar à Administração os resultados da Política de Segurança da Informação;
j) estabelecer o Sistema de Gestão da Continuidade do Negócio (SGCN) do Tribunal:
   - elaborar e manter o Programa de Gestão da Continuidade de Negócio;
   - garantir a aderência do escopo do SGCN às diretrizes estratégicas do Tribunal e a requisitos externos, promovendo, quando necessário, as devidas adequações;
   - aprovar as estratégias de continuidade e os planos de continuidade do negócio propostos pela área de Segurança da Informação; e
k) patrocinar ações de comunicação e promoção da cultura de Segurança da Informação no âmbito do Tribunal.

7.3 **À Seção de Gestão da Segurança da Informação compete**:

a) fornecer subsídios para as atividades do CGSI do Tribunal;
b) gerir a Segurança da Informação;
c) elaborar, junto com a Divisão de Infraestrutura de TI o Plano de Continuidade do Negócio em Tecnologia da Informação;
d) promover palestras e treinamentos para conscientização dos usuários e atualização das ações de segurança;
e) realizar análises de riscos relacionados à Segurança da Informação;
f) coordenar ações que se fizerem necessárias na ocorrência de incidentes de segurança da informação;
g) atuar de forma coordenada com outras áreas nos assuntos de segurança da informação;
h) informar ao CGSI do Tribunal:
   - nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de risco; e
   - incidentes de segurança tecnológica.
i) gerir, junto com a Divisão de Infraestrutura de TI o Plano de Continuidade do Negócio em Tecnologia da Informação do Tribunal (PCNTI):
   - realizar Análises de Impacto de acordo com o escopo definido;
   - propor estratégias de continuidade a partir dos resultados fornecidos e pela análise/avaliação de riscos, e submetê-las ao Comitê Gestor de Segurança da Informação para aprovação;
   - elaborar, e manter os planos de continuidade do negócio em Tecnologia da Informação;
   - coordenar a execução dos testes dos planos e de treinamentos dos participantes de atividades relativas à Gestão de Continuidade do Negócio em Tecnologia da Informação;
   - conduzir a revisões e auditorias periódicas no PCNTI.

7.4 **À Assessoria Jurídica compete**:

a) informar ao CGSI sobre alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolva a gestão da segurança da informação;
b) avaliar, sempre que solicitado, as normas, procedimentos e outros documentos relativos à gestão da segurança da informação;
c) assessorar o CGSI nas demais questões legais.

7.5 **À Secretaria de Gestão de Pessoas compete**: obter e manter junto aos registros funcionais dos servidores e magistrados um termo de ciência sobre a PSI e normas associadas e outro de responsabilidade e sigilo.

7.6 **À Escola Judicial compete**: promover ações de capacitação em segurança da informação aos servidores deste Tribunal.

7.7 **À Comunicação Social compete**:

a) assessorar a criação do Plano de Comunicação e Conscientização em Segurança da Informação; e
b) atuar na divulgação e promoção de assuntos relativos à segurança da informação.

7.8 **Ao Superior hierárquico do usuário compete**: divulgar e verificar a observância, no âmbito de sua unidade, da PSI e normas associadas, comunicando ao CGSI eventuais irregularidades.

7.9 **Aos Usuários compete**:

a) atender aos princípios e diretrizes contidos nesta PSI, nas normas e nos procedimentos definidos;
b) proteger os ativos de informação, incluindo informação, evitando perda e modificação de dados propositais ou indevidas; e
c) relatar incidentes de segurança da informação e violação da segurança que houver conhecimento.

8 ATUALIZAÇÃO

Esta Política de Segurança da Informação, bem como o conjunto de Normas Complementares gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

9 VIGÊNCIA

Esta Política de Segurança da Informação entra em vigor a partir da data de sua publicação.

Anexo II - ATO TRT-GP Nº 296/2017

CONTROLE DE ACESSO FÍSICO

1 OBJETIVO

Este documento faz parte dos instrumentos normativos de Segurança da Informação do Tribunal Regional do Trabalho da Sexta Região. Tem por objetivo dispor sobre as regras de segurança que nortearão a definição e a implantação de medidas para o controle de acesso físico às instalações e aos equipamentos de Tecnologia da Informação do Tribunal Regional.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Acesso físico**: permissão de acesso, concedida ao usuário mediante apresentação de uma identidade válida, aos ambientes destinados a dar suporte ou abrigar os equipamentos de armazenamento e de processamento de dados;

2.2 ***Backup*** **(Cópia de segurança das informações)**: é a cópia das informações fundamentais para a continuidade da prestação jurisdicional armazenadas em recursos de tecnologia da informação que permitem a recuperação após um desastre ou falha;

2.3 **Biblioteca de Software Definitiva (BSD):** área lógica ou física nas quais as versões de todos os *softwares* aprovados (cópias-mestre de todos os *softwares* controlados, incluindo mídias dos *softwares* comprados), licenças e documentações são armazenadas de forma segura;

2.4 **Controle de acesso lógico:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso, utilizando para isto barreiras lógicas;

2.5 **Controle de acesso físico:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso, utilizando para isto barreiras físicas;

2.6 **Depósito de *Hardware* Definitivo (DHD):** área destinada ao armazenamento físico dos componentes de *hardware* (equipamentos e peças) sobressalentes;

2.7 **Princípio de privilégio mínimo**: as permissões concedidas a cada identidade devem ser as mínimas necessárias para o exercício do cargo, função ou papel do seu detentor;

2.8 **Proprietário**: no contexto dessa norma, o termo "proprietário" identifica uma pessoa ou área que tenha uma responsabilidade autorizada para controlar o acesso, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo;

2.9 **Recursos de TI**: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação e as instalações físicas que os abrigam; e

2.10 **Sala técnica**: ambiente crítico destinado a abrigar os equipamentos operantes de armazenamento e processamento de dados.

3 CONSIDERAÇÕES INICIAIS

3.1 Os dados corporativos armazenados nas instalações e equipamentos do Regional são os ativos mais valiosos da instituição e, eventualmente, podem tornar-se os maiores alvos de ataques e ameaças.

3.2 A proteção física dos dados tem papel fundamental na continuidade da prestação jurisdicional do Tribunal.

3.3 A dependência da instituição em relação aos recursos de TI exige a prática de controles rígidos sob a exposição dos dados e dos ambientes de processamento e de armazenamento.

3.4 Há a necessidade de adequar a estrutura física aos requisitos de segurança da informação relacionados ao Processo Judicial Eletrônico e à preservação dos dados de natureza administrativa e jurisdicional.

3.5 Convém que a identificação, a autorização e o princípio do privilégio mínimo sejam condicionantes prévias para a concessão de acesso aos ativos e aos serviços de Tecnologia da Informação.

3.6 Convém que a implementação dos controles de acesso lógico e físico sejam obtidos como consequência do nível de riscos apontado pelo gestão de riscos de segurança da informação.

4 PROCEDIMENTOS

Cabe à Secretaria de Tecnologia da Informação definir procedimentos para a gestão do acesso físico às instalações e equipamentos de TI do Regional.

4.1 O Tribunal Regional do Trabalho da Sexta Região, por meio da Secretaria de Tecnologia da Informação, estabelecerá diretrizes de segurança para credenciamento de acesso de usuários aos equipamentos de Tecnologia da Informação em conformidade com a legislação vigente, e em especial quanto ao acesso às áreas e instalações consideradas críticas.

4.2 De acordo com as boas práticas de segurança da informação, é conveniente que todas as instalações e os equipamentos de TI sejam classificados de acordo com os requisitos do negócio, relevância para o Tribunal e para a segurança da informação, e que tenham um proprietário identificado e a ele seja atribuída a responsabilidade pela proteção adequada.

4.3 Deve-se instituir formas de identificação capazes de distinguir servidores de

visitantes e terceirizados. Se for o caso, podem ser criadas categorias específicas de servidores para facilitar a gestão do acesso.

4.4 Convém que sejam utilizados mecanismos de controle de acesso físico em salas e áreas de acesso restrito (fechaduras eletrônicas, biometria, câmeras de vídeo, alarmes, etc).

5 DO CONTROLE DE ACESSO FÍSICO

5.1 O objetivo do controle é proteger as instalações e os equipamentos de Tecnologia da Informação, visando prevenir perda, dano ou comprometimento dos ativos de informação, de modo a reduzir as ameaças à continuidade das atividades do Tribunal.

5.2 A responsabilidade pelo controle de acesso físico às salas técnicas do Regional é da Divisão de Infraestrutura de Tecnologia da Informação, devendo ela definir e executar procedimentos específicos de acordo com as diretrizes de segurança elaboradas pela Seção de Gestão da Segurança da Informação.

5.3 O acesso às salas técnicas é inicialmente restrito aos servidores da Secretaria de Tecnologia da Informação autorizados pelo Chefe da Divisão de Infraestrutura de Tecnologia da Informação:

a) qualquer acesso não previamente autorizado somente será permitido mediante identificação e justificativa do propósito e das atividades que serão realizadas no local;
b) serviços de terceiros deverão ser agendados previamente, com identificação da pessoa que executará o serviço e o detalhamento das atividades a serem realizadas no local; e
c) qualquer acesso realizado conforme previsto nos itens a) e b) será supervisionado por servidor designado pelo Chefe da Divisão de Infraestrutura de Tecnologia da Informação.

5.4 A responsabilidade pelo controle de acesso físico aos Depósitos de Hardware Definitivo (DHD) e às Bibliotecas de Software Definitiva (BSD) do Regional é do Núcleo de Relacionamento da Secretaria de Tecnologia da Informação, devendo ela definir e executar procedimentos específicos de acordo com as diretrizes de segurança elaboradas pela Seção de Gestão da Segurança da Informação.

5.5 O acesso aos DHDs e às BSDs é inicialmente restrito aos servidores da Secretaria de Tecnologia da Informação autorizados pelo Chefe do Núcleo de Relacionamento:

a) qualquer acesso não previamente autorizado somente será permitido mediante identificação e justificativa do propósito e das atividades que serão realizadas no local;
b) serviços de terceiros deverão ser agendados previamente, com identificação da pessoa que executará o serviço e o detalhamento das atividades a serem realizadas no local; e

c) qualquer acesso realizado conforme previsto nos itens a) e b) será supervisionado por servidor designado pelo Chefe do Núcleo de Relacionamento.

5.6 Todas as portas externas as salas técnicas, aos DHDs e à BSDs deverão permanecer trancadas, mesmo durante horário de expediente.

6 MONITORAMENTO

6.1 O registro de pessoas não previamente autorizadas deve conter: nome, empresa, data, hora de entrada, hora de saída, nome do servidor que acompanhou a pessoa, motivo, equipamento manipulado pelo prestador de serviços e assinatura da pessoa e do servidor.

6.2 Convém que as salas técnicas, os DHDs e as BSDs tenham pelo menos um mecanismo de identificação que possibilite o registro de entrada e saída:

a) quando mais de uma pessoa entrar ou sair em uma sala técnica, DHD ou DSD, no mesmo intervalo de tempo, é obrigatório que todos utilizem o mecanismo para fins de registro; e
b) para armazenar os registros de entrada e saída e os registros visuais (câmeras) deve-se obedecer a normas específicas sobre backup.

7 INFRAESTRUTURA

7.1 É responsabilidade de todos que tenham acesso às salas técnicas, aos DHDs e às BSDs zelar pelo bom funcionamento dos mecanismos de segurança: portas, fechaduras e chaves, dispositivos biométricos, câmeras, sensores, entre outros.

7.2 Qualquer falha nos mecanismos referenciados no item anterior deve ser imediatamente reportada ao responsável pelo ambiente e, por este, ao responsável pela manutenção dos mecanismos, para que sejam tomadas as devidas providências.

8 DISPOSIÇÕES FINAIS

8.1 O Diretor da Secretaria de Tecnologia da Informação poderá limitar, mediante portaria, o acesso de pessoas estranhas à secretaria aos espaços destinados ao desenvolvimento de sistemas de tecnologia da informação e à manutenção de equipamentos de informática.

8.2 Não será permitido o uso de câmeras fotográficas de qualquer espécie e gravadores de vídeo ou áudio nas salas técnicas, salvo se for autorizado pela Secretaria de Tecnologia da Informação.

8.3 Responde pelo acesso em desacordo com esta Norma Complementar o usuário que o tenha realizado e, solidariamente, o responsável pela unidade organizacional onde ocorrer a infração.

8.4 Os casos omissos e as dúvidas surgidas na aplicação desta norma serão dirimidos

pelo Comitê Gestor de Segurança da Informação.

9 VIGÊNCIA E ATUALIZAÇÃO

A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Anexo III - ATO TRT-GP Nº 296/2017

CONTROLE DE ACESSO LÓGICO

1 OBJETIVO

Este documento dispõe sobre as regras de segurança que nortearão a definição e implantação de medidas para identificação e controle de acesso lógico aos ativos de informação do Tribunal Regional do Trabalho da Sexta Região.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do Regional;

2.2 **Acesso lógico**: permissão de acesso aos ativos de informação concedida ao usuário mediante apresentação de uma identidade válida;

2.3 **Administrador de ativo de informação**: usuário ou grupo de usuários responsável por definir critérios de utilização e autorizar, conceder ou modificar permissões de uso sobre o ativo de informação;

2.4 **Administrador de grupo**: usuário responsável pela criação e manutenção de grupos de usuários;

2.5 **Ativos de informação**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

2.6 **Autenticação**: processo de validação da identidade do usuário, que pode ser feito por diversos meios, tais como: combinação de usuário/senha, reconhecimento biométrico ou utilização de certificado digital;

2.7 **Autorização**: processo de enumerar as permissões que um determinado usuário possui após a verificação de sua identidade;

2.8 **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

2.9 **Conta**: identificação única de usuário, com senha associada, para acesso aos ativos de informação do Regional;

2.10 **Conta de uso coletivo**: conta para acesso aos ativos de informação do Tribunal utilizada por mais de um usuário, com finalidade específica;

2.11 **Controle**: políticas, procedimentos, práticas e estruturas organizacionais criadas para prover uma razoável garantia de que os objetivos do Tribunal serão atingidos e que

eventos indesejáveis serão evitados ou detectados e corrigidos;

2.12 **Identidade**: conjunto de atributos (lógicos e/ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação;

2.13 **Identificação**: processo pelo qual o usuário apresenta uma identidade aos sistemas e serviços de informação;

2.14 **Necessidade de conhecer**: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

2.15 **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

2.16 **Permissões**: conjunto de direitos que um usuário possui para acessar/alterar informações nos sistemas ou serviços de informação;

2.17 **Privilégio**: permissão concedida a usuário e grupos de usuários de um recurso de TI;

2.18 **Princípio de privilégio mínimo**: as permissões concedidas a cada identidade devem ser as mínimas necessárias para o exercício do cargo, função ou papel do seu detentor;

2.19 **Rede de computadores do Tribunal**: conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do Regional ou por ele providos, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;

2.20 **Senha**: conjunto de caracteres, de uso e conhecimento exclusivo do usuário, que permite autenticá-lo e, assim, conceder o acesso aos sistemas ou serviços de informação; e

2.21 **Usuários**: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados, cedidos e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando os recursos tecnológicos deste Regional.

3 CONSIDERAÇÕES INICIAIS

3.1 O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e da comunicação.

3.2 A identificação, a autorização, a autenticação, o interesse do serviço, o princípio do privilégio mínimo e a necessidade de conhecer são condicionantes prévias para concessão de acesso aos ativos de informação no âmbito do Tribunal.

4 TIPOS DE USUÁRIOS

São usuários do Tribunal do Trabalho da Sexta Região:

4.1 **Usuário interno**: autoridade ou servidor ativo do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Regional;

4.2 **Usuário colaborador**: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Regional;

4.3 **Usuário externo**: servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal e que não se enquadre nas definições contidas nos itens 4.1 e 4.2; e

4.4 **Usuário visitante**: pessoa física, que não se enquadre na definição disposta nos itens 4.1, 4.2 e 4.3 desta norma, com acesso temporário, somente à internet, autorizado a partir da rede do Tribunal.

5 DAS CONTAS DE ACESSO

Cada usuário deve possuir uma única conta para acesso aos ativos de informação do Tribunal, exceto nos casos explicitamente definidos e formalmente autorizados pela Secretaria de Tecnologia da Informação.

5.1 Tecnologia da Informação

A criação e a atualização de conta de usuário interno para acesso aos ativos de informação do Tribunal devem ser realizadas pela Secretaria de Tecnologia da Informação com base nos registros contidos no sistema informatizado de gestão de pessoas:

a) a Secretaria de Tecnologia da Informação deve definir e divulgar os procedimentos a serem executados com vistas à criação e à desativação de contas de usuários externos, colaboradores e visitantes; e
b) a utilização de conta de uso coletivo é permitida para usuário em treinamento e nos casos em que não seja possível trabalhar com conta de usuário individual.

5.2 Da identificação

5.2.1 A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

5.2.2 A alteração da identificação do usuário para acesso aos ativos de informação do Regional, quando não disponível nos próprios sistemas, deverá ser feita de forma presencial pelo usuário, com a apresentação de documento oficial com foto deste ou memorando da autoridade competente, junto ao setor responsável da Secretaria de Informática.

5.3 Da Senha

5.3.1 Composição da senha:

a) as senhas devem ser criadas em conformidade com os procedimentos e regulamentos vigentes quanto à qualidade e período de validade; e
b) é proibida a utilização de senhas sem nenhum processo criptográfico aplicado, excetuando-se os casos em que não houver alternativa.

5.3.2 Senha de uso coletivo

A senha associada à conta de uso coletivo só deve ser divulgada para as pessoas que efetivamente utilizam a conta para o treinamento ou para a finalidade para a qual foi criada.

5.3.3 Alteração da senha:

a) a alteração da senha associada à conta de usuário para acesso aos ativos de informação do Tribunal pode ser solicitada ou efetuada pelo próprio usuário ou, mediante seu pedido, pela chefia imediata; e
b) a alteração de senha associada à conta de uso coletivo deve ser solicitada por quem demandou a criação ou pelo responsável pelo treinamento a ser ministrado.

5.4 Prazo de Validade das Contas de Acesso

As contas para acesso aos ativos de informação do Tribunal têm os seguintes prazos de validade:

a) contas de magistrados e de servidores ativos e inativos: enquanto durar o vínculo com o Tribunal;
b) contas de usuários colaboradores: durante o exercício de suas atividades para o Tribunal;
c) contas de usuários externos, à exceção daquelas relativas a servidores inativos: sem prazo de validade previamente fixado, ressalvados os casos em que norma específica defina os prazos pertinentes; e
d) contas de usuários visitantes e contas de uso coletivo: pelo período necessário para a execução das atividades que motivaram a criação.

6 DA AUTENTICAÇÃO

6.1 Os ativos de informação do Tribunal somente serão acessíveis aos usuários que apresentem uma identidade válida e que possuam as permissões necessárias.

6.2 O processo de autenticação deve ser realizado de forma segura, visando evitar que informações sobre a identidade sejam acessíveis por outras pessoas.

6.3 Sempre que possível, o controle de acesso aos ativos de informação do Tribunal deverá possuir, pelo menos, dois fatores de autenticação.

7 DAS PERMISSÕES DE ACESSO AOS ATIVOS DE INFORMAÇÃO

As permissões de acesso aos sistemas e serviços de informação do Tribunal somente serão concedidas ou revogadas com base em atos de autoridade ou órgão competente.

7.1 Do usuário interno

Disponibilizar ao usuário interno que não exerce funções de administração de ativo de informação do Tribunal somente uma única conta institucional de acesso à rede local e ao correio eletrônico institucional, pessoal e intransferível.

7.1.1 Das permissões de acesso para exercício da função

As permissões de acesso aos ativos de informação do Tribunal, diferentes da rede local e do correio eletrônico institucional, são concedidas a grupos de usuários pelo respectivo administrador do ativo de informação:

a) os grupos de usuários relativos a unidades de lotação são criados e atualizados pela Secretaria de Informática, com base nas informações lançadas no sistema informatizado de gestão de pessoas; e
b) para os grupos de usuários com atualização manual, cabe ao administrador do grupo a verificação periódica de seus componentes e a inclusão ou retirada tempestiva de membros.

7.1.2 Do privilégio de administrador

a) os usuários da Secretaria de Informática deverão possuir privilégio de administrador de ativos de informação apenas se necessário para o cumprimento de suas atividades, obedecido ao princípio de privilégio mínimo; e
b) nenhum usuário que não pertença ao corpo técnico da Secretaria de Informática deverá possuir privilégio de administrador de ativos de informação. As exceções ocorrerão apenas caso a Secretaria de Informática não consiga alternativas que permitam o desenvolvimento das atividades do usuário.

7.1.3 Das mudanças nas atribuições e/ou lotação

Sempre que houver mudança nas atribuições e/ou lotação de determinado usuário, os seus privilégios de acesso aos ativos de informação do Regional devem ser adequados imediatamente por procedimentos automáticos, ou tempestivamente no caso manual, devendo ser cancelados em caso de desligamento do Regional ou bloqueados em caso de afastamento.

7.1.4 **Das alterações a pedido do superior hierárquico:**

a) as permissões de acesso dos usuários aos ativos de informação do Tribunal poderão ser concedidas ou modificadas a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Informática; e
b) as identidades e permissões de acesso poderão ser restringidas ou suspensas para determinados usuários, a pedido de superior hierárquico., mediante solicitação formal justificada à Secretaria de Informática

7.2 **Dos usuários colaboradores**

Poderão ser concedidas aos usuários colaboradores identidades e permissões de acesso aos ativos de informação do Tribunal durante o período de prestação dos serviços, observando as normas aqui enumeradas, mediante solicitação formal justificada do dirigente da unidade, onde será prestado o serviço colaborativo, à Secretaria de Informática.

8 AUDITORIA

8.1 Os acessos aos sistemas e serviços de informação do Tribunal, bem como as operações realizadas, sempre que possível devem ser registrados, permitindo auditoria.

8.2 As informações das identidades e os registros de acessos devem ser protegidos contra alterações e acessos indevidos.

9 COMPETÊNCIAS E RESPONSABILIDADES

9.1. Da Secretaria de Informática

9.1.1 Propor regulamentação sobre os tipos de identidades homologadas para acesso aos ativos de informação deste Tribunal, bem como os seus requisitos mínimos;

9.1.2 Implantar políticas para criação, renovação, bloqueio, suspensão e expiração de senhas, com o intuito de aumentar o nível de segurança aos ativos de informação do Tribunal;

9.1.3 Propor regulamentação de procedimentos formais referentes à concessão e revogação de identidade de acesso aos ativos de informação deste Tribunal;

9.1.4 Definir e documentar os procedimentos operacionais relacionados a esta norma;

9.1.5 Divulgar amplamente esta política, procedimentos e regulamentos afins junto aos usuários dos ativos de informação deste Tribunal;

9.1.6 Manter a base de identidades e permissões de acesso aos ativos de informação deste Tribunal;

9.1.7 Emitir, suspender e modificar identidades e permissões de acesso aos ativos de informação deste Tribunal;

9.1.8 Implantar controles visando garantir a criação de senhas em conformidade com os procedimentos e regulamentos vigentes quanto à qualidade e período de validade;

9.1.9 Implantar demais controles necessários para o cumprimento desta políticaorma, deixando os sistemas e serviços de informação deste Tribunal em conformidade com a mesma; e,

9.1.10 Comunicar qualquer irregularidade ao Comitê Gestor de Segurança da Informação, a fim de que sejam tomadas as providências cabíveis.

9.2 Dos Usuários

9.2.1 Os atos decorrentes pela utilização dos sistemas de informática, através de conta de acesso com identificação e autenticação, são de responsabilidade do usuário para o qual a conta está formalmente vinculada; e

9.2.2 A senha associada à conta (identificação) de usuário para acesso à rede do Tribunal é pessoal, intransferível e o devido sigilo é de responsabilidade exclusiva do titular da conta.

9.3 Do Administrador do Ativo

É responsabilidade do administrador do ativo de informação verificar e adequar periodicamente as permissões de acesso.

9.4 Da Chefia Imediata

Compete à chefia imediata do usuário verificar a observância das disposições desta norma no âmbito de sua unidade, comunicando à Secretaria de Informática as irregularidades detectadas.

9.5 Da Secretaria de Gestão de Pessoas

A Secretaria de Gestão de Pessoas será responsável pelo envio imediato à Secretaria de Informática da informação de desligamento, aposentadoria ou movimentação de desembargadores, servidores, estagiários e aprendizes integrantes do Regional, para os devidos ajustes das credenciais de acesso.

Anexo IV - ATO TRT-GP Nº 296/2017

USO DE SENHAS, ESTAÇÕES DE TRABALHO, *SOFTWARES* E REDE

1 OBJETIVO

Esta norma tem por objetivo dispor sobre as responsabilidades dos usuários quanto ao uso seguro de senhas, estações de trabalho, *softwares* e rede local.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Estação de Trabalho**: qualquer computador registrado como patrimônio do Tribunal, incluindo estações de trabalho móvel, utilizado pelos usuários no desempenho de suas atividades;

2.2 ***Hardware***: qualquer componente, acessório ou dispositivo eletro-eletrônico que seja parte de um computador;

2.3 **Incidentes de Segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

2.4 **Programa**: consiste de *softwares* adquiridos pelo Tribunal ou que podem ser baixados pela Internet;

2.5 **Recurso de Tecnologia da Informação (TI)**: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação e as instalações físicas que os abrigam;

2.6 **Rede local**: conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do Tribunal ou por ele providos, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;

2.7 **Senha**: conjunto de caracteres, de uso e conhecimento exclusivo do usuário, que permite autenticá-lo e, assim, conceder o acesso aos sistemas ou serviços de informação;

2.8 **Sistema**: *softwares* desenvolvidos pelo Tribunal para auxiliar as realizações de suas atividades jurisdicionais e administrativas; e

2.9 ***Software***: parte lógica, ou seja, instruções e dados processado pelos circuitos eletrônicos do *hardware* para executar um conjunto de ações previamente definidas. Consiste de programas e sistemas.

3 CONSIDERAÇÕES INICIAIS

3.1 Os recursos de TI devem ser utilizados somente em atividades estritamente relacionadas às funções institucionais.

3.2 Os parâmetros de configuração das estações de trabalho serão definidos pela Secretaria de Tecnologia da Informação, que levará em conta os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do Tribunal.

3.3 A concessão de acesso aos recursos de TI deve obedecer ao princípio do privilégio mínimo, isto é, será concedido acesso ao usuário unicamente àqueles recursos de TI que forem indispensáveis à realização de suas atividades.

3.4 Os usuários são responsáveis pelos recursos de TI por eles utilizados, devendo contribuir para seu funcionamento e segurança.

3.5 É vedada a utilização dos recursos de TI disponíveis com o objetivo de praticar ações maliciosas contra outros recursos da rede de computadores do Tribunal ou redes externas.

4 REGRAS E RESPONSABILIDADES

4.1 Das Senhas

4.1.1 As senhas são de uso pessoal e intransferível, não sendo permitida a utilização de senha de outras pessoas ou fornecimento de senha pessoal a terceiros.

4.1.2 É vedada a utilização de quaisquer programas ou dispositivos para interceptar ou decodificar senhas ou similares.

4.1.3 O usuário deve notificar imediatamente à Secretaria de Tecnologia da Informação sobre qualquer uso não autorizado de sua conta ou qualquer quebra de segurança de seu conhecimento.

4.2 Das Estações de Trabalho

4.2.1 As estações de trabalho devem ser utilizadas apenas por usuários com identificação de acesso à rede do Tribunal e que não tenham infringido as disposições contidas nesta norma.

4.2.2 Prestadores de serviços terceirizados, consultores e estagiários poderão utilizar estações de trabalho durante o período de prestação dos serviços, desde que considerem as regras e responsabilidades dispostas nesta norma, e que haja solicitação formal justificada do dirigente da unidade onde será prestado o serviço

terceirizado ou estágio à Secretaria de Tecnologia da Informação.

4.2.3 A guarda da estação de trabalho móvel é de inteira responsabilidade do magistrado ou servidor, devidamente registrada pela Seção de Gestão de Ativos de TI.

4.2.4 O usuário deve bloquear a estação de trabalho que lhe foi confiado sempre que dela se ausentar.

4.2.5 A homologação de *softwares*, componentes de *hardwares* e equipamentos passíveis de serem instalados e utilizados no ambiente do Tribunal é procedimento de competência da Secretaria de Tecnologia da Informação, sendo vedada a instalação dos que não tenham sido homologados, salvo em razão de testes, se feita pela própria Secretaria.

4.2.6 As estações de trabalho serão instaladas e configuradas pela Secretaria de Tecnologia da Informação.

4.2.7 Não compete à Secretaria de Tecnologia da Informação instalar e configurar equipamentos que não estejam registrados como patrimônio do Tribunal.

4.3 **Dos *Softwares***

4.3.1 Os *softwares* utilizados pelo Tribunal somente podem ser instalados nas estações de trabalho por pessoas autorizadas pela Secretaria de Tecnologia da Informação, podendo ser feita por meio de programas de gerenciamento remoto.

4.3.2 É vedada a cópia de programas, licenças dos programas e sistemas implantados nas estações de trabalho, quer seja para uso externo, quer seja para uso em outra estação de trabalho do Tribunal.

4.4 **Da Rede Local e Armazenamento Lógico**

4.4.1 É vedada a utilização de dispositivos particulares, portáteis ou não, na rede local do Tribunal, exceto em casos de comprovada necessidade, e mediante anuência da Secretaria de Tecnologia da Informação, que velará para que sejam, obrigatoriamente, adotados os padrões de segurança estabelecidos pelo Tribunal.

4.4.2 É vedado adicionar sem autorização à rede do Tribunal quaisquer recursos que possam interferir de alguma forma no desempenho ou na segurança da rede, como pontos de acesso *wireless*, acesso móvel e impressoras de rede.

4.4.3 É vedado o uso de ferramentas de *hardware* e *software* para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados, exceto quando autorizado pela Secretaria de Tecnologia da

Informação.

4.4.4 A Secretaria de Tecnologia da Informação poderá restringir o espaço disponível para o usuário nas unidades de armazenamento de rede, considerando as limitações dos recursos de tecnologia da informação e as atividades desenvolvidas pelo usuário.

4.4.5 O usuário deve manter, sempre que possível, a cópia dos arquivos de trabalho nas unidades lógicas de armazenamentos de rede disponibilizadas pela Secretaria de Tecnologia da Informação.

4.4.6 É vedado o armazenamento de arquivos não relacionados com as atividades institucionais nas unidades de rede, tais como: músicas, vídeos e fotos.

4.4.7 A Secretaria de Tecnologia da Informação executará cópias de segurança dos arquivos de trabalho armazenados nas unidades de armazenamento de rede.

5 MONITORAMENTO

Compete à Secretaria de Tecnologia da Informação realizar o monitoramento da utilização dos recursos de tecnologia da informação, com a finalidade de detectar não conformidades com as regras e responsabilidades definidas nesta norma. Os registros de eventos monitorados poderão constar, inclusive, como evidências nos casos de incidentes de segurança.

6 DISPOSIÇÃO FINAL

Avaliado o risco, a Secretaria de Tecnologia da Informação poderá proceder à desinstalação sumária dos *softwares* que não se enquadrarem nos critérios estabelecidos nesta norma.

Anexo V - ATO TRT-GP Nº 296/2017

USO DO SERVIÇO DE ACESSO À INTERNET

1 OBJETIVO

Esta norma tem por objetivo dispor sobre as regras relativas ao uso seguro do serviço de acesso à internet.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Acesso à Internet**: ato de acessar qualquer recurso disponível na Internet, como sites, salas de bate-papo, fóruns de discussão, entre outros;

2.2 **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

2.3 ***Download***: (significa descarregar ou baixar, em português) é a transferência de dados hospedados remotamente para um computador ou dispositivo de armazenamento local;

2.4 **Exclusão de acesso**: processo que tem por finalidade suspender definitivamente o acesso;

2.5 **Identificação de acesso à rede**: conjunto de atributos (lógicos e/ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso à rede de computadores do Tribunal;

2.6 **Internet**: consiste na rede mundial de computadores interconectados. É utilizada como uma grande plataforma para a provisão de inúmeros serviços;

2.7 ***Proxy***: computador ou sistema que serve de intermediário entre um navegador da *Web* e a Internet; e

2.8 ***Site* ou sítio**: conjunto de páginas web, disponibilizadas na Internet.

3 CONSIDERAÇÕES INICIAIS

3.1 O acesso à Internet através da rede corporativa do Regional dar-se-á, exclusivamente, por intermédio dos meios autorizados pela Secretaria de Tecnologia da Informação.

3.2 Excetuando-se os casos previstos nesta norma, o acesso à internet provido pela rede do Tribunal deve restringir-se às páginas com conteúdo estritamente relacionado às atividades desempenhadas pelo Órgão.

3.3 A conexão de acesso à Internet deve passar por equipamentos de segurança garantindo o controle de acesso e a aplicação dos demais mecanismos de segurança e, em caso contrário, o equipamento deve estar isolado da rede da entidade institucional.

3.4 Para garantir a utilização adequada para fins diretos e complementares às atividades funcionais, a Secretaria de Tecnologia da Informação poderá impor limitações ao acesso através de ferramentas automáticas.

4 PERMISSÃO DE ACESSO

4.1 Possuem acesso à Internet, os magistrados e servidores em exercício, com identificação de acesso à rede do Tribunal.

4.2 Prestadores de serviços terceirizados e estagiários poderão ter acesso à Internet durante o período de prestação dos serviços desde que seja formalmente solicitado e justificado pelo responsável da unidade onde está sendo prestado o serviço terceirizado ou estágio.

5 RESTRIÇÃO DE ACESSO

O acesso à Internet poderá ser bloqueado ou excluído para determinados usuários, por uso indevido do serviço ou a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Tecnologia da Informação.

6 USO DO SERVIÇO

6.1 Constituem uso indevido do serviço de acesso à Internet:

a) acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: pornografia, pedofilia, racismo, apologia ao crime, calúnia, difamação, injúria, comunidades de relacionamento pessoal, jogos, fóruns não-profissionais, dentre outros;
b) utilizar programas de troca de mensagens em tempo real (bate-papo), exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Tecnologia da Informação;
c) acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto nos casos de comprovada necessidade, através de solicitação à Secretaria de Tecnologia da Informação;
d) obter na Internet arquivos (*download*) que não estejam relacionados com suas atividades funcionais, a saber: imagens, áudio, vídeo, jogos e programas de qualquer tipo;
e) acessar sítios que apresentem vulnerabilidade de segurança ou possam comprometer de alguma forma a segurança e integridade da rede de

computadores do TRT;

f) utilizar sítios, serviços Internet ou *softwares* para acesso anônimo, como *proxies* externos e similares; e

g) utilizar sítios, serviços Internet ou *softwares* para controle remoto de equipamentos, exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Tecnologia da Informação.

6.2 Não constitui utilização indevida o acesso a sítios bancários, sítios de notícias e de pesquisa e busca.

6.3 O acesso aos sítios e serviços que estejam enquadrados como uso indevido, mas que sejam necessários ao desempenho das atribuições funcionais do usuário, será liberado mediante solicitação do dirigente da unidade à Secretaria de Tecnologia da Informação.

6.4 É vedado aos usuários utilizar mecanismos com o objetivo de descaracterizar o uso indevido do serviço.

7 MONITORAMENTO

7.1 Compete à Secretaria de Tecnologia da Informação realizar o monitoramento e o controle do serviço de acesso à Internet do Tribunal, a fim de garantir o cumprimento desta norma.

7.2 A Secretaria de Tecnologia da Informação, sempre que possível, deverá registrar os endereços das páginas acessadas pelos usuários. Comprovada a utilização indevida, o acesso à internet do usuário poderá ser bloqueado e sua chefia imediata comunicada para as providências cabíveis.

8 DISPOSIÇÕES FINAIS

8.1 As permissões de acesso dos usuários em afastamento definitivo da organização devem ser excluídas.

8.2 As permissões de acesso dos usuários em afastamento temporário devem ser bloqueadas no período da ausência.

Anexo VI - ATO TRT-GP Nº 296/2017

CORREIO ELETRÔNICO

1 OBJETIVO

Esta norma tem por objetivo dispor sobre as regras relativas ao uso seguro do serviço de correio eletrônico.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

2.2 **Boato**: mensagem que possui conteúdo alarmante ou falso, como correntes ou pirâmides, com o objetivo de aplicar golpes;

2.3 **Caixa postal**: conta de correio eletrônico onde são armazenadas as mensagens recebidas pelo usuário;

2.4 **Certificado Digital**: credencial emitida por autoridade certificadora, que no país é a ICP-Brasil, responsável pela emissão de certificados digitais com validade legal;

2.5 **Código malicioso**: termo genérico que se refere a todos os tipos de *software* que executam ações danosas e atividades maliciosas em um computador, a exemplo, os vírus e os "cavalos de tróia";

2.6 **Exclusão de acesso**: processo que tem por finalidade suspender definitivamente o acesso;

2.7 ***Phishing***: mensagem enviada com o objetivo de obter informações sensíveis, tais como senhas e números de cartão de crédito, para utilização em fraudes;

2.8 **Serviço de correio eletrônico institucional**: serviço de envio e recebimento de mensagens eletrônicas (*e-mails)* do Tribunal gerenciado pela Secretaria de Tecnologia da Informação;

2.9 **Serviço externo de correio eletrônico**: qualquer serviço de correio eletrônico disponibilizado por terceiros;

2.10 ***Spam***: mensagem não solicitada enviada para vários destinatários; e

2.11 ***Webmail***: serviço de correio eletrônico disponível através de um *site*.

Anexo VI - ATO TRT-GP Nº 296/2017

3 CONSIDERAÇÕES INICIAIS

3.1 O usuário deverá utilizar o correio eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais.

3.2 A Secretaria de Tecnologia da Informação poderá estabelecer limites de utilização do correio eletrônico que se façam necessários para o bom funcionamento do serviço, aí incluídos os de quantidade de destinatários, o tamanho máximo da caixa postal e das mensagens enviadas ou recebidas, dos tipos permitidos de arquivos anexados às mensagens.

3.3 A denominação do endereço de correio eletrônico do usuário será composta valendo-se preferencialmente de um nome e um sobrenome, separados por um sinal de ponto e acrescidos do sufixo "@trt6.jus.br".

3.4 É de responsabilidade do usuário efetuar periodicamente a manutenção de sua caixa postal.

3.5 O acesso a serviços de correio eletrônico externos somente poderá ser feito via Webmail, podendo este ser bloqueado a qualquer momento se confirmado uso não apropriado.

4 PERMISSÃO DE ACESSO

4.1 Possuem acesso ao correio eletrônico institucional os usuários com identificação de acesso para utilização do serviço.

4.2 Prestadores de serviços terceirizados, consultores e estagiários poderão ter acesso ao correio eletrônico institucional durante o período de prestação dos serviços, mediante solicitação formal justificada, do dirigente da unidade onde será prestado o serviço terceirizado ou estágio, à Secretaria de Tecnologia da Informação.

4.3 As unidades administrativas poderão ter listas de correio eletrônico observada no endereço a denominação usualmente utilizada no Tribunal.

4.4 Sistemas ou aplicativos que necessitem enviar *e-mails* poderão ser configurados para ter acesso a uma caixa postal.

4.5 Solicitações para criação ou exclusão de caixas postais deverão ser encaminhadas formalmente à Secretaria de Tecnologia da Informação.

5 RESTRIÇÃO DE ACESSO

O acesso ao serviço de correio eletrônico institucional poderá ser bloqueado ou excluído

para determinados usuários, por uso indevido do serviço ou a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Tecnologia da Informação.

6 USO DO SERVIÇO

6.1 Caracteriza-se por uso recomendável do serviço de correio eletrônico:

a) eliminar, periodicamente, as mensagens desnecessárias da caixa postal pessoal institucional de forma a não exceder o limite de tamanho definido;
b) evitar clicar em *links* de acesso a páginas de *Internet* existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem tratar-se de golpes que objetivam o roubo de informações pessoais;
c) evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência;
d) fazer o uso, preferencialmente, do campo de cópia oculta (BCC/CCO) do cliente de correio eletrônico sempre que enviar uma mensagem para mais de um destinatário; e
e) evitar o envio de documentos anexos, como boletins, periódicos, memorandos e ofícios, substituindo o anexo por uma referência (*link*) ao documento no corpo da mensagem.

6.2 Caracteriza-se por uso não apropriado do serviço de correio eletrônico enviar mensagens contendo:

a) material obsceno, ilegal ou antiético;
b) material preconceituoso ou discriminatório;
c) material calunioso ou difamatório;
d) material considerado apologia ao crime, racismo ou pedofilia;
e) listas de endereços eletrônicos dos usuários do correio eletrônico do TRT6;
f) códigos maliciosos ou qualquer programa que execute ações danosas ou atividades maliciosas;
g) material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;
h) material protegido por leis de propriedade intelectual;
i) boatos, *spam* e *phishing*;
j) assuntos ofensivos;
k) imagens, áudio ou vídeo que não estejam relacionados ao desempenho das atividades funcionais;
l) arquivos executáveis de qualquer tipo;
m) mensagens comerciais não solicitadas, também conhecidas como *spam*;
n) mensagens que representem riscos de segurança ou que afetem o desempenho dos recursos de tecnologia do Tribunal, ou ainda que possam comprometer, de alguma forma, a integridade, a confidencialidade ou a disponibilidade das

informações institucionais; e

o) outros conteúdos notadamente desnecessários para o desempenho das atribuições funcionais.

6.3 Caracteriza-se por uso vedado do serviço de correio eletrônico:

a) utilizar clientes de correio eletrônico que não sejam homologados pela Secretaria de Tecnologia da Informação;
b) utilizar mecanismos com o objetivo de descaracterizar o uso indevido do serviço;
c) acessar a caixa postal de outro usuário, salvo mediante prévia autorização;
d) configurar o redirecionamento automático de mensagens para serviços externos de correio eletrônico;
e) o envio de mensagens destinadas a todos os usuários, cujo conteúdo esteja relacionado somente a determinado grupo de magistrados e servidores.

7 MONITORAMENTO

7.1 Compete à Secretaria de Tecnologia da Informação realizar o monitoramento e o controle do serviço de correio eletrônico, a fim de garantir o cumprimento desta norma.

7.2 A Secretaria de Tecnologia da Informação poderá rastrear ou varrer o conteúdo das mensagens, de forma automática, por *softwares* especiais, a fim de verificar a adequação de seu conteúdo às disposições estabelecidas.

7.3 Os anexos das mensagens de correio eletrônico poderão ser bloqueados quando oferecerem riscos à segurança da informação.

8 DISPOSIÇÕES FINAIS

8.1 Caso o usuário venha a receber mensagens externas de conteúdo não apropriado, o mesmo deverá excluí-las no primeiro acesso à caixa postal após o recebimento das mesmas;

8.2 É permitida a criação de listas de correio eletrônico, com o objetivo de atender necessidades específicas de determinados grupos de usuários;

8.3 O envio de mensagens a todos os usuários é restrito a assuntos de interesse geral dos magistrados e servidores, sendo de responsabilidade das unidades administrativas e seus representantes;

8.4 É permitida a participação em Listas de Discussão com assuntos relacionados exclusivamente ao interesse do trabalho tanto profissional quanto educativo;

8.5 As mensagens ou arquivos eletrônicos com Assinaturas Digitais e cujos Certificados

forem emitidos por entidades certificadoras que façam parte da ICP-Brasil são considerados documentos oficiais no âmbito deste Tribunal.

Anexo VII - ATO TRT-GP Nº 296/2017

PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

1 OBJETIVO

Este documento faz parte dos instrumentos normativos de Segurança da Informação do Tribunal Regional do Trabalho da Sexta Região. Tem por objetivo dispor sobre as regras de segurança que nortearão a definição e a implantação de medidas para a proteção contra a ação de códigos maliciosos no ambiente de rede do Tribunal.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Antivírus**: ferramenta desenvolvida para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos de um computador. Pode incluir também a funcionalidade de *firewall* pessoal;

2.2 **Código malicioso**: termo genérico que se refere a todos os tipos de programas especificamente desenvolvidos para executar ações danosas em recursos de tecnologia da informação;

2.3 ***Firewall***: dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;

2.4 ***Firewall* pessoal**: tipo específico de *firewall*. Programa usado para proteger um computador contra acessos não autorizados vindos da Internet; e

2.5 ***Log***: registro de atividades gerado por programas e serviços de um computador. Termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo: de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

3 CONSIDERAÇÕES INICIAIS

3.1 Conforme estabelecido na Norma Institucional de Responsabilidades Quanto ao Uso de Senhas, Estações de Trabalho, *Softwares* e Rede; os usuários são responsáveis pelos recursos de tecnologia da informação por eles utilizados, devendo contribuir para seu funcionamento e segurança.

3.2 Códigos maliciosos são agentes potencialmente graves à segurança da informação, pois possibilitam o roubo de informações sigilosas e a paralisação dos serviços.

3.3 Convém que os recursos de tecnologia da informação estejamprotegidos por sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de

acesso não autorizado, tais como programas antivírus, programas de análise de conteúdo de correio eletrônico e *firewall*.

3.4 Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela Secretaria de Tecnologia da Informação.

4 CONTROLES

4.1 É vedada qualquer atividade, por parte dos usuários, que vise à criação ou distribuição de códigos maliciosos.

4.2 É vedada ao usuário a desativação ou a alteração de configuração de quaisquer de seus componentes de proteção contra códigos maliciosos (por ex.: antivírus, *firewall* pessoal etc.). Caso julgue necessário alguma modificação, o setor responsável deverá ser informado.

4.3 Antes de sua utilização, é conveniente que toda e qualquer mídia de armazenamento que tenha origem externa ao Tribunal seja verificada quanto à existência de códigos maliciosos.

4.4 Convém que todo e qualquer arquivo recebido por correio eletrônico ou Internet seja verificado de forma automática quanto à existência de códigos maliciosos.

4.5 Convém que todos os dispositivos de processamento do Tribunal devam estar configurados de acordo com os padrões de segurança mais adequados aos serviços previstos, de maneira que prestem apenas os serviços previstos.

4.6 Convém que todos os dispositivos de processamento do Tribunal estejam atualizados conforme as recomendações dos respectivos fabricantes e fornecedores.

4.7 Os dispositivos de processamento portáteis, sempre que tecnicamente possível, devem possuir *firewall* pessoal instalado e configurado de forma a possibilitar que o dispositivo seja utilizado somente para os fins previstos.

4.8 Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.

4.9 Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados, isolados ou removidos do sistema pelo programa antivírus. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o desempenho das atividades do Tribunal.

5 COMPETÊNCIAS E RESPOSABILIDADES

Ficam definidas as seguintes competências e responsabilidades:

5.1 **À Secretaria de Tecnologia da Informação**:

a) auxiliar no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;
b) proceder com a instalação dos sistemas de detecção e bloqueio de códigos maliciosos nos equipamentos computacionais, mantendo-os atualizados conforme disponibilização do fabricante; e
c) monitorar os *logs* dos sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, com objetivo de atuar de forma proativa na identificação de ameaças.

5.2 **Ao usuário:**

a) utilizar somente programas homologados pela Secretaria de Tecnologia da Informação;
b) observar se o programa de antivírus está instalado, atualizado e ativo no equipamento computacional;
c) utilizar mídia de armazenamento que tenha origem externa à organização conforme disposto no item 4.2; e
d) notificar imediatamente à Secretaria de Tecnologia da Informação qualquer suspeita de ataque por código malicioso à dispositivo de processamento sob sua custódia, ou mesmo a sua rede local.

6 DISPOSIÇÕES FINAIS

6.1 As atualizações e as correções para os sistemas de detecção e bloqueio de códigos maliciosos devem ser homologadas pela Secretaria de Tecnologia da Informação antes de aplicadas ao ambiente de produção.

6.2 Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem, depois de homologadas, ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

6.3 Os casos omissos e as dúvidas surgidas na aplicação desta norma serão dirimidos pelo Comitê Gestor de Segurança da Informação.

7 VIGÊNCIA E ATUALIZAÇÃO

A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Anexo VIII - ATO TRT-GP Nº 296/2017

TRATAMENTO DE INCIDENTES

1 OBJETIVO

Este documento faz parte dos instrumentos normativos de Segurança da Informação do Tribunal Regional do Trabalho da Sexta Região. Tem por objetivo dispor sobre a criação e o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), no âmbito do Tribunal.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Agente Responsável**: servidor público ocupante de cargo efetivo de carreira do Tribunal Regional do Trabalho da Sexta Região incumbido de supervisionar o trabalho realizado pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

2.2 **Comunidade ou Público Alvo**: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;

2.3 **CTIR GOV**: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

2.4 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):** grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e de executar atividades relacionadas a incidentes de segurança em redes de computadores;

2.5 **Incidente de segurança**: evento adverso, confirmado ou sob suspeita, relacionado à informação ou aos sistemas de computação ou às redes de computadores;

2.6 **Serviço**: é um conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais; e

2.7 **Tratamento de Incidentes de Segurança em Redes Computacionais**: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas, e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

3 CONSIDERAÇÕES INICIAIS

3.1 O Tribunal Regional do Trabalho da Sexta Região possui a competência formal e a respectiva atribuição de administrar sua infraestrutura da rede de computadores.

3.2 O gerenciamento de incidentes de segurança em redes de computadores requer especial atenção da alta administração do Regional.

3.3 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais deve ser composta, preferencialmente, por servidores públicos ocupantes de cargo efetivo de carreira, com perfil técnico compatível.

4 MISSÃO

A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do Tribunal tem como missão prioritária facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, a fim de evitar que os serviços prestados pelo Tribunal sejam afetados negativamente e, desta forma, contribuindo para que a Justiça do Trabalho de Pernambuco cumpra sua missão institucional.

5 COMUNIDADE OU PÚBLICO ALVO

A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) atenderá internamente a seguinte comunidade, composta por: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando os recursos tecnológicos deste Regional.

Externamente, a ETIR se relacionará com o Centro de Tratamento e Resposta de Incidentes em Redes Computacionais (CTIR GOV) e outras equipes similares da organização pública da Administração Pública Federal, fornecendo informações acerca dos incidentes de segurança ocorridos na rede do Tribunal, alimentando as suas bases de conhecimentos e fomentando a troca de experiências e tecnologias.

A comunicação do tratamento dos incidentes de segurança para a comunidade interna e externa será efetuada através dos canais de comunicação oficiais do Tribunal Regional do Trabalho da 6ª Região.

6 MODELO DE IMPLEMENTAÇÃO

A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)

seguirá o Modelo 1 de implementação definido na Norma Complementar Nº 05 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República (05/IN01/DSIC/GSIPR), conforme detalhado a seguir.

6.1 Inicialmente, não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de segurança em rede. A equipe será formada a partir dos membros das equipes da Secretaria de Tecnologia da Informação do próprio Tribunal, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

6.2 As funções e serviços de tratamento de incidente deverão ser realizados, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

6.3 A Equipe desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém, que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.

7 ESTRUTURA ORGANIZACIONAL

7.1 Posicionamento e Composição

7.1.1 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ficará subordinada a Secretaria de Tecnologia da Informação do Tribunal Regional do Trabalho da Sexta Região, podendo, entretanto, envolver pessoas de outras áreas que se façam necessárias.

7.1.2 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) será formada preferencialmente por:

a) um servidor da área de Redes de Computadores;
b) um servidor da área de Banco de Dados;
c) um servidor da área de Suporte a Sistemas Operacionais e Aplicações;
d) um servidor da área de Backup e Recuperação;
e) um servidor da área de Segurança da Informação;
f) um servidor da área de Datacenter e Arquitetura de Hardware; e
g) um servidor da área de Monitoramento dos Serviços de TI.

7.1.3 Para cada uma das posições mencionadas no item 7.1.2, deverá ser designado um suplente que deverá ter condições de substituir o titular e executar todas as suas atribuições.

7.1.4 Caso necessário, servidores de outras áreas poderão ser convocados para comporem a Equipe de Tratamento e Resposta a Incidentes em Redes

Computacionais (ETIR): Assessoria Jurídica, área de Gestão de Pessoas, área de comunicação, infraestrutura elétrica e hidráulica, entre outras.

7.2 **Competências e Responsabilidades**

Ficam definidas as seguintes competências e responsabilidades:

7.2.1 **Ao Agente Responsável**:

a) definir, com auxílio da área de Segurança da Informação, o processo de gestão de resposta a incidentes, e supervisionar as atividades desempenhadas pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);
b) assegurar que os usuários que comuniquem incidentes de segurança da informação sejam informados dos procedimentos adotados;
c) auxiliar as áreas envolvidas na elaboração de relatórios, apresentando estatísticas e análise de tendências de incidentes; e
d) ser o interlocutor com organismos externos de resposta a incidentes, especialmente o CTIR GOV.

7.2.2 **Ao CGSI**: prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), bem como prover a infraestrutura necessária.

7.2.3 **À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)**:

a) recolher evidências imediatamente após a constatação de um incidente de segurança da informação na rede de computadores do Tribunal;
b) executar uma análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;
c) investigar as causas dos incidentes de segurança da informação na rede de computadores do Tribunal;
d) implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes; e
e) indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

7.2.4 **Ao diretor da Secretaria de Tecnologia da Informação**:

a) indicar, mediante portaria, o Agente Responsável, os servidores membros da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) e seus respectivos suplentes; e
b) estabelecer na portaria referida no item a), conforme Modelo 1 de

implementação definido na Norma Complementar 05/IN01/DSIC/GSIPR, o percentual de tempo de trabalho para cada membro da equipe.

8 AUTONOMIA

A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) possui autonomia compartilhada, e trabalhará em acordo com outros setores funcionais da organização a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas, observando as seguintes disposições:

a) a equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque, e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização.
b) o processo decisório será compartilhado entre o gestor do serviço impactado e o gerente funcional da área correspondente ao incidente;
c) para ações de alto impacto, o processo decisório contará também com a participação do Diretor da Secretaria de Tecnologia da Informação. Para que sejam tomadas as ações administrativas e judiciais necessárias é cabível que a decisão seja comunicada formalmente à Diretoria Geral e ao Secretário Geral, respectivamente.

9 SERVIÇOS

Os serviços a serem prestados pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) serão definidos com base no histórico de incidentes de segurança reportados e que necessitem de apoio/orientação para o tratamento. Inicialmente serão oferecidos os seguintes serviços:

Serviço	**Objetivo**	**Definição**	**Funções e procedimentos que compõem o serviço**	**Disponibilidade (quando, como e onde o serviço será oferecido)**	**Metodologia para execução**
Tratamento de Incidentes de Segurança em Redes	Analisar e extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação	Este Serviço consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança,	Análise, avaliação, classificação e tratamento das notificações de incidentes de segurança da informação.	Sempre que houver a notificação de um incidente.	Os serviços serão realizados com base nas orientações do CTIR Gov e nas boas práticas de mercado.

	de tendências.	procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.			
Emissão de alertas e advertências	Advertir a comunidade sobre incidentes de segurança da informação.	Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.	Aviso nos sites institucionais e emissão de e-mails aos usuários.	Sempre que se fizer necessário.	Os serviços serão realizados com base nas orientações do CTIR Gov e nas boas praticas de mercado.
Geração de relatórios mediante estatísticas e análise de tendências	Elaborar e publicar relatórios sobre os resultados alcançados com o tratamento de	Este serviço consiste em elaborar relatórios com base nos incidentes de segurança em redes de computadores	Coletar, processar, e publicar informações relacionadas aos incidentes de segurança ocorridos.	Semestralmente ou sempre que se fizer necessário.	Os serviços serão realizados com base nas orientações do CTIR Gov e nas boas

	incidentes.	registrados, possibilitando a análise de tendência.			praticas de mercado.

10 DISPOSIÇÕES FINAIS

10.1 Os incidentes de segurança da informação deverão ser reportados à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) por meio do e-mail incidenteseg-l@trt6.jus.br.

10.2 O Tribunal Regional do Trabalho da 6ª Região, que inicialmente optou pela implantação do Modelo I de implementação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), deverá, assim que possível, migrar para um dos outros modelos, Centralizado; Descentralizado; ou Misto, conforme a Norma Complementar 05/IN01/DSIC/GSIPR.

10.3 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede, orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

10.4 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar e com a legislação em vigor.

10.5 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) deverá comunicar a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse Órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

10.6 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) têm como dever, sem prejuízo do disposto no item 10.5 desta Norma Complementar e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR:

a) acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;
b) observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme orientações do GSIPR;
c) priorizar a continuidade dos serviços da ETIR e da missão institucional da

organização, observando os procedimentos previstos no item b).

10.7 Os casos omissos e as dúvidas surgidas na aplicação desta norma serão dirimidos pelo Comitê Gestor de Segurança da Informação.

11 VIGÊNCIA E ATUALIZAÇÃO

Esta norma entra em vigor a partir da publicação da portaria que nomeie os membros da ETIR e do processo de gestão de resposta a incidentes de segurança da informação, e sua atualização ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Anexo IX - ATO TRT-GP Nº 296/2017

GERAÇÃO E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

1. OBJETIVO

Esta norma tem por objetivo estabelecer as diretrizes para a geração de cópias de segurança das informações e sua restauração em tempo proporcional à criticidade do serviço afetado.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Arquivo ativo:** arquivo em uso (atual);

2.2 **Controle de acesso lógico:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso, utilizando para isto barreiras lógicas.

2.3 **Controle de acesso físico:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso, utilizando para isto barreiras físicas.

2.4 **Cópia de segurança das informações (backup):** é a cópia das informações fundamentais para a continuidade da prestação jurisdicional armazenadas em recursos de tecnologia da informação que permitem a recuperação após um desastre ou falha de uma mídia;

2.5 **Informação sigilosa:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

2.6 **Recursos de tecnologia da informação:** qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação e as instalações físicas que os abrigam;

2.7 **Sistemas críticos:** sistemas fundamentais para a continuidade da prestação jurisdicional do Tribunal; e

2.8 **Tipos de backup:** completo (copia todos os arquivos selecionados e os marca como arquivos que passaram por backup), incremental (copia somente os arquivos criados ou alterados desde o último backup completo ou incremental e os marca como arquivos que passaram por backup) e diferencial (copia arquivos criados ou alterados desde o último backup completo ou incremental, mas não marca os arquivos como arquivos que passaram por backup).

Anexo IX - ATO TRT-GP Nº 296/2017

3. CONSIDERAÇÕES INICIAIS

3.1 A realização de cópias de segurança das informações é fundamental para a continuidade da prestação jurisdicional, em caso de perda de dados ou desastres.

3.2 As cópias de segurança das informações devem ser efetuadas e testadas regularmente pela secretaria de Tecnologia da Informação.

3.3 A infraestrutura para a geração de cópias de segurança deve ser adequada para garantir que toda informação essencial possa ser recuperada.

4. PROCEDIMENTOS

4.1 Cabe à Secretaria de Tecnologia da Informação definir procedimentos para a geração e restauração das cópias de segurança, mantendo os registros completos e fidedignos das cópias.

4.2 Para sistemas críticos, os procedimentos de geração e restauração das cópias devem abranger todas as aplicações, dados, configurações e informações essenciais para a completa recuperação do sistema em caso de necessidade.

4.3 Os procedimentos de restauração de cópias de segurança devem ser verificados regularmente, de forma a garantir que estes são efetivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação.

4.4 Os procedimentos de cópia de segurança das informações devem ser automatizados para facilitar o processo de geração e recuperação das cópias.

4.5 Deve ser implantado um controle de acesso físico e lógico para as informações das cópias de segurança.

5. CÓPIAS DE SEGURANÇA DA INFORMAÇÃO

5.1 A Secretaria de Tecnologia da Informação é a responsável pelo processo de cópias de segurança das informações no âmbito do Regional.

5.2 A frequência, tipo (completa, diferencial e incremental) e tempo de retenção das cópias de segurança das informações geradas serão definidos pela Secretaria de Tecnologia da Informação, considerando os requisitos legais e a criticidade dos dados envolvidos com as atividades da Instituição.

5.3 Os equipamentos envolvidos no processo de cópias de segurança devem garantir que os dados das cópias de segurança sejam gravados na sua totalidade.

5.4 As informações sigilosas devem ser salvaguardadas criptografadas nas cópias de segurança.

5.5 A Secretaria de Tecnologia da Informação não realizará cópias de informações armazenadas em estações de trabalho do Regional.

6. Horário para a realização das cópias

As cópias de segurança serão realizadas em horário de baixa utilização das informações, preferencialmente fora do horário de expediente.

Sendo inevitável a realização de cópias de segurança no horário do expediente, deverá ser justificado antecipadamente caso haja necessidade de parada do serviço ou queda substancial no desempenho dos recursos de Tecnologia da Informação.

Na situação de erro de cópia de segurança das informações, é necessário que ela seja refeita logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

7. TESTES

7.1 A Secretaria de Tecnologia da Informação deve realizar testes periódicos de restauração das cópias de segurança, visando a garantir que as cópias geradas são confiáveis para uso em caso de necessidade.

7.2 Os registros das evidências dos testes devem ser devidamente documentados.

7.3 Por se tratar de uma simulação, as informações devem ser restauradas em local diferente do original, para que assim não sobreponha os arquivos ativos.

8. RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

8.1 A Secretaria de Tecnologia da Informação é a responsável pelo processo de restauração de segurança das informações no âmbito do Regional.

8.2 Solicitações de restauração de cópias de segurança devem ser encaminhadas formalmente à Secretaria de Tecnologia da Informação para as devidas providências.

8.3 Na situação de erro de restauração de cópia de segurança das informações é

necessário que ela seja refeita logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

9. MANUSEIO DE MÍDIAS

Para cada tipo de mídia devem ser observadas as recomendações dos fabricantes quanto aos seus requisitos de utilização.

9.1. Armazenamento

As mídias com cópias de segurança devem ser armazenadas em local remoto, que possua um nível apropriado de proteção física e ambiental, a distância do local principal suficiente para evitar danos ocasionados por um eventual sinistro.

O local onde as mídias devem ser armazenadas deve ter acesso restrito e controlado somente a usuários autorizados.

As mídias devem ser devidamente identificadas de forma a permitir sua rápida localização e recuperação.

9.2. Transporte

Quando necessário, as mídias serão transportadas por um colaborador autorizado pela Secretaria de Tecnologia da Informação, para um local seguro, dentro de embalagem lacrada que proteja adequadamente seu conteúdo.

9.3. Descarte e Substituição de mídias

9.3.1. Deverão ser adotados mecanismos seguros para o descarte de mídias (incineração, trituração, etc.) a fim de garantir que informações armazenadas e sem uso sejam irrecuperáveis, observando as legislações pertinentes.

9.3.2. Mídias a serem descartadas devem ser registradas e suas informações de identificação devem ser removidas.

9.3.3. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

10. MONITORAMENTO

10.1. Para formalizar o controle de execução de cópias de segurança de informações e

restaurações, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado nos termos desta Norma e dos procedimentos dela derivados.

10.2. Nos processos automatizados, o formulário poderá ser substituído por relatórios devidamente assinados pelos responsáveis.

11. DISPOSIÇÕES FINAIS

11.1. A Secretaria de Tecnologia da Informação deverá comunicar ao Comitê Gestor de Segurança da Informação qualquer irregularidade concernente a falhas de segurança, a fim de que sejam tomadas as providências cabíveis.

11.2. É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.