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

ATO TRT-GP Nº 314/2013

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 no anexo a este Ato.

Art. 2º Ficam revogadas as disposições em contrário.

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

Recife, 4 de julho de 2013.

IVANILDO DA CUNHA ANDRADE
Desembargador Presidente do TRT da Sexta Região

Anexo ATO TRT-GP Nº 314/2013

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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 a 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 promoção da cultura de Segurança da Informação no âmbito do Tribunal.

7.3 **À Área de Segurança da Informação compete**:

a) fornecer subsídios para as atividades do CGSI do Tribunal;
b) elaborar um Plano Diretor de Segurança da Informação com base nas definições estratégicas estabelecidas pelo Comitê;
c) gerir a Segurança da Informação e o Plano de Continuidade do Negócio;
d) coordenar as ações do Plano Diretor de Segurança da Informação e dos projetos a ele relacionados;
e) promover palestras e treinamentos para conscientização dos usuários e atualização das ações de segurança;
f) realizar análises de riscos periódicas no que tange à tecnologia, ambientes, processos e pessoas;
g) manter os registros de monitoramento sobre o uso dos recursos de tecnologia;
h) realizar auditorias ordinárias e extraordinárias, com emissão de relatórios sobre a utilização dos recursos de tecnologia, apontando, quando existentes, irregularidades e ausência de adequação em seu uso;

i) coordenar ações que se fizerem necessárias na ocorrência de incidentes de segurança da informação;
j) atuar de forma coordenada com outras áreas nos assuntos de segurança da informação;
k) 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.
l) gerir o Sistema de Gestão da Continuidade do Negócio do Tribunal (SGCN):
   - realizar Análises de Impacto no Negócio (AIN) de acordo com o escopo definido;
   - propor estratégias de continuidade a partir dos resultados fornecidos pela (AIN) e pela análise/avaliação de riscos, e submetê-las ao Comitê de Segurança da Informação para aprovação;
   - elaborar e manter os planos de continuidade do negócio;
   - coordenar a execução dos testes dos planos e de treinamentos dos participantes de atividades relativas à Gestão de Continuidade do Negócio;
   - conduzir a revisões e auditorias periódicas no SGCN.

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 Recursos Humanos 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 Coordenação de Desenvolvimento de Pessoas compete**: promover ações de capacitação em segurança da informação aos servidores deste Tribunal.

7.7 **À Assessoria de Comunicação 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.