PORTARIA TRT 18ª GP/DG Nº 076/2014
Aprova a Revisão 1.0 da Política de Segurança da Informação e Comunicações do Tribunal Regional do Trabalho da 18ª Região
A DESEMBARGADORA-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais e tendo em vista o que consta do Processo Administrativo SISDOC Nº 4001/2014;
Considerando a necessidade de estabelecer diretrizes e padrões para garantir o controle e a segurança da informação no âmbito do Tribunal, com observância dos princípios da integridade, da confidencialidade e da disponibilidade;
Considerando a Resolução nº 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário; e
Considerando que a segurança da informação constitui atividade estratégica da área de tecnologia da informação e comunicação, conforme artigo 2º, parágrafo 2º, inciso IV, da mencionada Resolução,
RESOLVE:
Art. 1º . Aprovar a Revisão 1.0 da Política de Segurança da Informação e Comunicações do Tribunal Regional do Trabalho da 18ª Região, conforme Anexo.
Art. 7º Esta Portaria entra em vigor na data de sua publicação.
Art. 8º Publique-se no Diário da Justiça Eletrônico e no Boletim Interno
Eletrônico.
Elza Cândida da Silveira
Desembargadora-Presidente
Goiânia, 11 de março de 2014.
[assinado eletronicamente]
ELZA CÂNDIDA DA SILVEIRA
DESEMB. PRES. DE TRIBUNAL

	Tribunal Regional do Trabalho da 18ª Região Comitê de Segurança da Informação Secretaria de Tecnologia da Informação Núcleo de Segurança da Informação	Código: **PO01**
		Revisão: **1.0**
		Vigência:
		Classificação: **PÚBLICO**
		Ato normativo:
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES		

1 OBJETIVO

Estabelecer as diretrizes da Política de Segurança da Informação e Comunicações do Tribunal Regional do Trabalho da 18ª Região, com observância dos princípios da integridade, da confidencialidade e da disponibilidade.

2 APLICAÇÃO

As disposições desta Política aplicam-se a todos os usuários de recursos de tecnologia da informação disponibilizados pelo Tribunal.

3 ALINHAMENTO

Resolução nº 90, de 29 de setembro de 2009 do CNJ;
ABNT NBR ISO/IEC 27001;
ABNT NBR ISO/IEC 27002;

4 DEFINIÇÕES

4.1 Confidencialidade: garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

4.2 Integridade: preservação da exatidão e completude da informação e dos métodos de processamento;

4.3 Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;

4.4 Ativo: a informação e todos os recursos e dispositivos que a manipulam;

4.5 Segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade da informação;

4.6 Recurso de Tecnologia da Informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como as instalações físicas que os abrigam;

4.7 Usuários: magistrados, servidores e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores e ainda os estagiários e menores aprendizes em atividade no Tribunal;

4.8 Plano de Continuidade do Negócio: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações;

4.9 Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação ou falhas de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]

4.10 Incidente de segurança da informação: é identificado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004]

5 CONTEÚDO

5.1 São de propriedade do Tribunal as informações geradas ou manipuladas pelos usuários identificados no item 4.7 desta política, no desempenho de suas funções, ainda que fora das dependências físicas do órgão e independentemente da forma de apresentação ou armazenamento com que tenham sido produzidas.

5.1.1 As informações de que trata o item 5.1 devem ser adequadamente protegidas e utilizadas exclusivamente para os fins relacionados às atividades institucionais no Tribunal.

5.1.2 Toda informação gerada ou manipulada no Tribunal deve ser classificada de acordo com norma a ser proposta pelo Comitê de Segurança da Informação e editada por meio de portaria da Presidência.

5.1.3 O Tribunal adotará dispositivos de proteção capazes de assegurar a autenticidade, integridade e disponibilidade da informação, conforme o seu nível de classificação e independentemente do suporte em que seja armazenada ou veiculada.

5.1.4 Compete à chefia imediata do usuário zelar, no âmbito de sua unidade, pela observância das disposições constantes desta Política, bem como pelas normas relativas à segurança da informação que vierem a ser editadas, comunicando à autoridade superior as eventuais irregularidades.

5.1.5 A inobservância das normas previstas nesta Política será devidamente apurada, podendo ensejar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurado aos envolvidos o contraditório e a ampla defesa.

5.1.6 Os contratos e convênios celebrados pelo Tribunal, cujo objeto envolva a utilização de recursos de tecnologia da informação, deverão conter cláusula exigindo a observância desta Política, que estará disponível no sítio eletrônico do Tribunal na internet.

5.1.7 A Secretaria de Tecnologia da Informação e Comunicações deverá constituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, conforme norma indicada no item 6.1.4 letra “f”.

6 COMPETÊNCIAS E RESPONSABILIDADES

6.1 Compete ao Comitê de Segurança da Informação:

6.1.1 Coordenar, implantar, divulgar e operacionalizar a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região, bem como propor e acompanhar planos de ação para aplicação desta política;

6.1.2 Propor a realização de campanhas de conscientização dos usuários quanto à política de segurança da informação;

6.1.3 Dirimir dúvidas e deliberar sobre questões não contempladas pela política de segurança da informação ou pelas normas a ela relacionadas, bem como sugerir as alterações necessárias;

6.1.4 Deliberar sobre as propostas de atos normativos apresentadas pelo Núcleo de Segurança da Informação, relativos às seguintes matérias, entre outras:
a)Acesso aos recursos de rede, inclusive internet;
b)Uso adequado de correio eletrônico (e-mail), estações de trabalho e dispositivos móveis fornecidos pelo Tribunal;
c)Uso e instalação de softwares;
d)Monitoramento e auditoria dos recursos de tecnologia da informação;

e)Plano de continuidade do negócio, em conformidade com o item 4.8 das Definições; e
f)Tratamento e resposta a incidentes em redes computacionais;

6.1.5 Deliberar sobre as iniciativas do Núcleo de Segurança da Informação relacionadas ao incremento da segurança da informação.

6.1.6 Os atos normativos de que trata o item 6.1.4 serão materializados por meio de Portarias da Presidência, numerados sequencialmente e publicados no órgão oficial de divulgação do Tribunal.

6.2 Compete ao Núcleo de Segurança da Informação:

6.2.1 Elaboração das normas previstas no item 6.1.4 e encaminhamento ao Comitê de Segurança da Informação, para fins de deliberação;

6.2.2 Assessoramento ao Comitê de Segurança da Informação, sempre que solicitado pelo seu Presidente, mediante esclarecimentos técnicos, prestação de informações ou encaminhamento de documentos;

6.2.3 Elaboração de programas de treinamento visando à capacitação dos proprietários e usuários da informação;

6.2.4 Monitoramento e auditoria dos recursos de tecnologia da informação do Tribunal;

6.2.5 Gestão do plano de continuidade do negócio de tecnologia da informação;

6.2.6 Análise periódica de riscos relacionados a tecnologia da informação e a seus ambientes, processos e pessoas;

6.2.7 Comunicação ao Comitê de Segurança da Informação dos incidentes de segurança tecnológica e do nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de risco.

6.3 A Equipe de Tratamento e Resposta a Incidentes de Informação em Redes Computacionais é responsável por:

6.3.1 Receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, além de armazenar registros para formação de séries históricas como subsídio estatístico.