PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 230/2013 (*)

Aprova a Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações.

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

CONSIDERANDO as boas práticas de Governança de TI que visam garantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;

CONSIDERANDO a necessidade de implementar mecanismos de controle da gestão de risco de segurança da informação,

RESOLVE:

Art. 1º Aprovar a Norma Complementar nº 04/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre a gestão de riscos de segurança da informação e comunicações, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 29 de maio de 2013.
MARIA ROSELI MENDES ALENCAR
Presidente

(*) Revogado pelo Ato TRT7.GP Nº 106/2018 disponibilizado no Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2519, 17 julho 2018. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1237, 03 jun. 2013.
Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 5.

Anexo Revogado

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação Escritório de Segurança da Tecnologia da Informação	Número da Norma Complementar	Revisão	Emissão	Folha
	04/NC/STI/SESTI	00	00/00/00	1/1
	Gestão de Riscos de Segurança da Informação e Comunicações			

1 OBJETIVO
Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) no Tribunal Regional do Trabalho da 7ª Região.
2 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR
2.1 Decreto nº 3.505, de 13 de junho de 2000, que "*Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*".
2.2 Art. 10, da Resolução nº 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, estabelece que "*a estrutura organizacional, o quadro de pessoal, a gestão de ativos e os processos do setor responsável pela gestão de trabalho da área de TIC do Tribunal deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as áreas de governança e de gerenciamento de serviços de TIC*".
2.3 Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008, que "*disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências*".
2.4 Norma Complementar 04/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional, de 14 de agosto de 2009, Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC), que "*estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF*".
2.5 Norma ABNT NBR ISO/IEC 27002:2005, que trata de Código de Pratica para a gestão da Segurança da Informação.
2.6 Norma ABNT NBR ISO/IEC 27005:2011, que trata de Gestão de riscos de segurança da Informação.
2.7 Norma ABNT ISO Guia 73, Gestão de riscos – Vocabulário.
2.8 Norma ABNT NBR ISO 31000:2009, Gestão de risco - Princípios e Diretrizes.
3 CONCEITOS E DEFINIÇÕES
3.1 Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:
a) ameaça - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
b) 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;
c) comunicação do risco - troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;
d) estimativa de riscos - processo utilizado para atribuir valores à probabilidade e consequências de um risco;
e) gestão de Riscos de Segurança da Informação e Comunicações - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
f) riscos de Segurança da Informação e Comunicações - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
g) tratamento dos riscos - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;
h) vulnerabilidade - é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.
4 PRINCÍPIOS E DIRETRIZES
4.1 As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) considera, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do Tribunal Regional do Trabalho da 7ª Região, além de estarem alinhadas à Política de Segurança Institucional.
4.2 O processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) é contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações no âmbito do Tribunal Regional do Trabalho da 7ª Região.
4.3 O processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) está alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, publicada no Diário Oficial da União nº 199, Seção 1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua.
4.4 A Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) produzirá subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios do Tribunal Regional do Trabalho da 7ª Região.
5 PROCEDIMENTOS
5.1 Será abordado de forma sistemática o processo Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC), com o objetivo de manter os riscos em níveis aceitáveis. O processo é composto pelas seguintes etapas:
a) definições preliminares;
b) análise/avaliação dos riscos;
c) plano de tratamento dos riscos;
d) aceitação dos riscos;
e) implementação do plano de tratamento dos riscos;
f) monitoração e análise crítica;
g) melhoria do processo de Gestão de Riscos de Segurança da Informação e Comunicações;
h) comunicação do risco.
5.2 Conforme apresentado no Anexo (A) desta Norma.
5.3 Definições preliminares - nesta fase, será realizada uma análise do TRT da 7ª Região, visando estruturar o processo de gestão de riscos de segurança da informação e comunicações, sendo consideradas as características do Regional e as restrições a que esta sujeita. Esta análise inicial permite que os critérios e o enfoque da Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) sejam os mais apropriados para o Regional, apoiando-o na definição do escopo e na adoção de uma metodologia. As tarefas a seguir deverão ser executadas:

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1237, 03 jun. 2013.
Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 5.

a) definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) a fim de delimitar o âmbito de atuação. Esse escopo pode abranger o TRT da 7ª Região como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação;
b) adotar uma metodologia de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.
5.4 Análise/avaliação dos riscos - nesta fase, inicialmente serão identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados. As tarefas a seguir deverão ser executadas:
a) identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido;
b) identificar os riscos associados ao escopo definido, considerando:
- as ameaças envolvidas,
- as vulnerabilidades existentes nos ativos de informação,
- as ações de Segurança da Informação e Comunicações (SIC) já adotadas;
c) estimar os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados;
d) avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos no item 5.1.2;
e) relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo TRT da 7ª Região.
5.5 Plano de Tratamento dos Riscos
5.5.1 Determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, observando:
a) a eficácia das ações de Segurança da Informação e Comunicações (SIC) já existentes;
b) as restrições organizacionais, técnicas e estruturais;
c) os requisitos legais;
d) a análise custo/ benefício.
5.5.2 Formular um plano para o tratamento dos riscos, relacionando, no mínimo, as ações de Segurança da Informação e Comunicações (SIC), responsáveis, prioridades e prazos de execução necessários à sua implantação.
5.6 Aceitação do Risco - verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.
5.7 Implementação do Plano de Tratamento dos Riscos - executar as ações de Segurança da Informação e Comunicações (SIC) incluídas no Plano de Tratamento dos Riscos aprovado.
5.8 Monitoração e análise crítica - detectar possíveis falhas nos resultados, monitorar os riscos, as ações de Segurança da Informação e Comunicações (SIC) e verificar a eficácia do processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC).
5.8.1 Do processo de gestão - monitorar e analisar criticamente o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades do órgão ou entidade.
5.8.2 Do risco - manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:
a) nos critérios de avaliação e aceitação dos riscos;
b) no ambiente;
c) nos ativos de informação;
d) nas ações de Segurança da Informação e Comunicações (SIC);
e) nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).
5.9 Melhoria do Processo de GRSIC
5.9.1 Propor à Comissão Permanente de Informática a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica.
5.9.2 Executar as ações corretivas ou preventivas aprovadas.
5.9.3 Assegurar que as melhorias atinjam os objetivos pretendidos.
5.10 COMUNICAÇÃO DO RISCO
Manter as instâncias superiores informadas a respeito de todas as fases da gestão de risco, tornando as informações disponíveis.
6 RESPONSABILIDADES
6.1 Cabe à Presidência do Tribunal Regional do Trabalho da 7ª Região aprovar as diretrizes gerais e o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) observada, dentre outras, a respectiva Política de Segurança Institucional.
6.2 A Secretaria de Tecnologia da Informação, no âmbito de suas atribuições, é responsável pela coordenação da Gestão de Riscos de Segurança da Informação e Comunicações no Tribunal Regional do Trabalho da 7ª Região.
6.3 O Setor de Escritório de Segurança de TI é responsável pelo gerenciamento das atividades, com as seguintes atribuições:
a) análise/avaliação e tratamento dos riscos;
b) elaboração sistemática de relatórios para a Secretaria de Tecnologia da Informação, em cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Presidência.
7 VIGÊNCIA
Esta Norma Complementar entra em vigor na data de sua publicação.

8 ANEXO
Processo de gestão de riscos de segurança da informação e comunicações.

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES