PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 232/2013

Aprova a Norma Complementar de Procedimentos para Inventariar Ativos de Tecnologia da Informação.

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 prover o Tribunal de informações precisas sobre os ativos de tecnologia da informação, com identificação dos responsáveis, descrição do local de armazenamento, do processamento e do transporte e com informações básicas sobre os requisitos de segurança da informação e comunicações,

RESOLVE:

Art. 1º Aprovar a Norma Complementar nº 06/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre os procedimentos para inventariar os ativos de tecnologia da informação, 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

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1236, 31 mai. 2013.
Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 11.

1 OBJETIVO

O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o Tribunal Regional do Trabalho da 7ª Região:
a) de um entendimento comum, consistente e inequívoco de seus ativos de informação;
b) da identificação clara de seu(s) responsável(eis) - proprietário(s) e custodiante(s);
c) de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação;
d) de uma descrição do contêiner de cada ativo de informação;
e) da identificação do valor que o ativo de informação representa para o negócio do Tribunal Regional do Trabalho da 7ª Região.

2 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

2.1 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".
2.2 Item I, Art. 3º, do Decreto nº 3.505, de 13 de Junho de 2000, que institui a Política de Segurança da Informação nos Órgãos da Administração Pública Federal, que estabelece "dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis".
2.3 ABNT NBR ISO/IEC 27002:2005 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão de Segurança da Informação.
2.4 Norma Complementar 10/IN01/DSIC/GSIPR, do Departamento de Segurança da Informações e Comunicações, do Gabinete de Segurança Institucional, da Presidência da República, que trata de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
2.5 Diretrizes para Gestão de Segurança da Informação no âmbito do Poder Judiciário, de junho de 2012, do CNJ, que estabelece "Implantação de um Sistema de Gestão de Segurança da Informação (SGSI), a partir dos processos do Modelo de Gestão, que permita: Inventário e gestão, principalmente, dos ativos críticos de Tecnologia da Informação e da Comunicação".

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:
3.1 Ativos de Informação - aquilo que tem valor, seja tangível ou intangível, tais como informações, softwares, equipamentos, instalações, serviços, pessoas e imagem institucional.

3.2 Agente Responsável - Servidor Público ocupante de cargo efetivo ou em comissão da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação.
3.3 Ameaça - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
3.4 Autenticidade - propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
3.5 Confidencialidade - propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
3.6 Contêineres dos Ativos de Informação - o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.
3.7 Continuidade de Negócios - capacidade estratégica e tática de um órgão ou entidade 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.
3.8 Custodiante - refere-se a qualquer indivíduo ou estrutura do Tribunal Regional do Trabalho da 7ª Região que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação.
3.9 Disponibilidade - propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
3.10 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.
3.11 Proprietário do ativo de informação - refere-se a parte interessada do Tribunal Regional do Trabalho da 7ª Região, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades:
a) descrever o ativo de informação;
b) definir as exigências de segurança da informação e comunicações do ativo de informação;
c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;
d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento;
e) indicar os riscos que podem afetar os ativos de informação.
3.12 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.

3.13 Segurança da informação e comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
3.14 Serviços - Serviços de computação e comunicação, utilidades gerais (ex. Aquecimento, iluminação, eletricidade e refrigeração).
3.15 Valor do Ativo de Informação - valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um Tribunal Regional do Trabalho da 7ª Região, quanto cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.
3.16 Vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais do processo de Inventário e Mapeamento de Ativos de Informação considera,
prioritariamente, os objetivos estratégicos, os processos, os requisitos legais, e a estrutura do Tribunal Regional do Trabalho da 7ª Região, bem como à Política de Segurança Institucional do Tribunal Regional do Trabalho da 7ª Região.
4.2 Que deve subsidiar o Tribunal Regional do Trabalho da 7ª Região a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio.
4.3 E produz subsídios tanto para a Gestão de Segurança da Informação e Comunicações, a Gestão de Riscos de Segurança da Informação e Comunicações, e a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, do Tribunal Regional do Trabalho da 7ª Região, quanto para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação.
4.4 Sendo dinâmico, periódico, e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

5 PROCEDIMENTOS

5.1 Deverá ser adotada uma abordagem sistemática do processo de Inventário e Mapeamento de Ativos de Informação, a qual é composto por 3 (três) subprocessos:
a) identificação e classificação de ativos de informação;
b) identificação de potenciais ameaças e vulnerabilidades;
c) avaliação de riscos.
5.2 O subprocesso “a” é apresentado a seguir, e os subprocessos “b” e “c” são objetos tratados na Norma Complementar 04/NC/STI/SESEG, Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações e no Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (Brasil/GSIPR, 2010).

5.3 O subprocesso de Identificação e Classificação de Ativos de Informação é composto por 6 (seis) etapas:
a) coleta de informações gerais dos ativos de informação;
b) detalhamento dos ativos de informação;
c) identificação do(s) responsável(is) - proprietário(s) e custodiante(s) de cada ativo de informação;
d) caracterização dos contêineres dos ativos de informação;
e) definição dos requisitos de segurança da informação e comunicações;
f) estabelecimento do valor do ativo de informação.
5.4 Etapa de Coleta de informações gerais dos ativos de informação.
5.4.1 Caberá a Secretaria de Tecnologia da Informação levantar as informações dos ativos de informação no prazo de 90 (noventa) dias a contar da data da publicação desta Norma Complementar, e anualmente as informações deverão ser atualizadas.
5.4.2 O levantamento deverá abranger o Tribunal Regional do Trabalho da 7ª Região como um todo.
5.4.3 Deverão ser adotadas metodologias de Gestão de Riscos de Segurança da Informação e Comunicações e de Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC, que incorporem o processo de Inventário e Mapeamento de Ativos de Informação.
5.5 Etapa de Detalhamento dos ativos de informação.
5.5.1 O detalhamento inicial dos ativos de informação, contemplará no mínimo um conjunto de informações, e deve:
a) determinar com clareza e objetividade o conteúdo do ativo de informação;
b) identificar o(s) responsável(is) - proprietário(s) e custodiante(s) - de cada ativo de informação;
c) identificar o valor de cada ativo de informação;
d) identificar os respectivos requisitos de segurança da informação e comunicações dos ativos de informação.
5.5.2 Identificar as interfaces e as interdependências internas e externas dos ativos de informação considerados críticos.
5.5.3 Identificar impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender os interesses da sociedade e do Estado.
5.6 Etapa de Identificação do(s) responsável(is) - proprietário(s) e custodiante(s) - de cada ativo de informação.
5.6.1 O proprietário do ativo de informação é a parte interessada do Tribunal Regional do Trabalho da 7ª Região, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.
5.6.2 O proprietário do ativo de informação possui as seguintes atividades:
a) descrever o ativo de informação;
b) definir as exigências de segurança da informação e comunicações do ativo de informação;
c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;
d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo;

e) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação.
5.6.3 O custodiante do ativo de informação deve proteger um ou mais ativos de informação do Tribunal Regional do Trabalho da 7ª Região, velando pelo armazenamento, transporte e processamento, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. Deve proteger os contêineres dos ativos de informação, e, consequentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo(s) proprietário(s) do(s) ativo(s) de informação.
5.7 Etapa de Caracterização dos contêineres dos ativos de informação.
5.7.1 O contêiner é o local onde "vive" o ativo de informação, será caracterizado com as seguintes informações: lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes.
5.7.2 Será definido os limites do ambiente que deve ser examinado para o risco, quanto descrever os relacionamentos que devem ser compreendidos para atendimento das exigências de segurança da informação e comunicações, caracterizam, também, o(s) contêiner(s) do(s) ativo(s) de informação.
5.8 Etapa de Definição dos requisitos de segurança da informação e comunicações dos ativos de informação.
5.8.1 Os requisitos de segurança da informação e comunicações dos ativos de informação devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.
5.8.2 Os requisitos de segurança da informação e comunicações dos ativos de informação serão categorizados, no mínimo, em 5 categorias de controle:
a) tratamento da informação;
b) controles de acesso físico e lógico;
c) gestão de risco de segurança da informação e comunicações;
d) tratamento e respostas a incidentes em redes computacionais;
e) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.
5.9. Etapa de Estabelecimento do valor do ativo de informação.
5.9.1 Cabe ao(s) proprietário(s) dos ativos de informação indicar o valor do ativo para o negócio do Tribunal Regional do Trabalho da 7ª Região, considerando fatores do(s) risco(s) os quais os ativos possam estar expostos, como ameaça, vulnerabilidade e impacto.
5.9.2 O proprietário do ativo da informação indicará o valor do ativo, o qual deve refletir o quão cada ativo de informação é importante para a que organização alcance seus objetivos estratégicos, e o quão o ativo de informação é imprescindível aos interesses da sociedade e do Estado.

6 RESPONSABILIDADES

6.1 O Diretor da Secretaria de Tecnologia da Informação, no âmbito de suas atribuições, é responsável pela coordenação do Inventário e Mapeamento de Ativos de Informação no do Tribunal Regional do Trabalho da 7ª Região bem como pela indicação de Agente Responsável pela gerência de tais atividades.

6.2 É responsável, também, pela análise quanto aos resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação, e consequente, proposição de ajustes e de medidas preventivas e pró ativas à Alta Direção.
6.3 Cabe ao Agente Responsável, no mínimo, as seguintes atividades:
a) o processo de identificação e classificação de ativos de informação;
b) o monitoramento dos níveis de segurança dos ativos de informação junto aos proprietários e custodiantes dos ativos de informação;
c) a elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações.

7 DISPOSIÇÕES GERAIS

7.1 Os casos omissos serão analisados pelo Comitê de Segurança da Institucional, que submeterá relatório conclusivo à Presidência, para a apreciação e decisão.

8 VIGÊNCIA

8.1 Esta Norma Complementar entra em vigor na data de sua publicação.