PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

PROJETO: IMPLANTAR PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Número do Projeto: 08/2011-5
Código do Projeto: CTI_SI_GESTAO_RISCOS
Versão: 3
Área demandante: Comitê de Planejamento e Gestão
Data da versão: 09/01/2013

COORDENADOR:	**Juíza Maria José Bighetti Ordoño Rebello** (NOME)		
GERENTE DE PROJETO:	**Ângela Tieko Tanaka Magrini** (NOME)	**3120-2000/2032** (TELEFONE/RAMAL)	**angela.tanaka@trtsp.jus.br** (ENDEREÇO ELETRÔNICO)

1. Identificação

Nome do projeto:	Implantar processo de Gestão de Riscos de Segurança da Informação
Número do projeto:	08/2011-5

2. Responsáveis

Área responsável pela execução	(CTI)
Parceiros na execução	Comissão de Treinamento e Capacitação

3. Cronograma	
Data de início do projeto	
4. Beneficiários	
Beneficiados diretos	Agentes do Judiciário
Área de abrangência	Todas as unidades judiciárias e administrativas do TRT da 2ª Região
5. Escopo	
Problematização (por quê?)	O TRT não conta com um mecanismo eficaz de gestão de riscos de segurança da informação
6. Meta	
Meta (para quê?)	Gerenciar e comunicar de forma consistente as fragilidades e eventos afetos à segurança da informação, permitindo a tomada de ação preventiva e corretiva no menor tempo possível
7. Metodologia	
Metodologia (como?)	- Dinâmica de grupo - Pesquisa normativa e bibliográfica - Pesquisa de campo
8. Embasamento conceitual	
Conceitos e normativos	**Recomendação do TCU:** “9.2.7 - em atenção ao disposto na Resolução nº 90/2009, art. 10, do CNJ, implemente processo de gestão de riscos de segurança da informação, a fim de, entre outros objetivos, avaliar regularmente a probabilidade e o impacto dos risco identificados, utilizando métodos qualitativos e quantitativos, observando as práticas contidas

	no Cobit 4.1, PO9.4 - Avaliar e gerenciar riscos de TI e na NBR 27005 - Gestão de Riscos de Segurança da Informação (item 3.18);" (Ac. TCU 2.938/2010, p. 3, item 9.2.7) Detalhamento na p. 20, item 3.18 do Ac. TCU 2.938/2010 **Normativos:** Resolução CNJ 90/2009 NBR - ISO/IEC 27005 ITGI – Cobit 4.1, PO 9.4 – Avaliação de riscos
9. Organização	
Atividades	1. Estabelecer plano de aceitação e tratamento de riscos 2. Estabelecer processo periódico de análise de risco 3. Efetuar análise de risco inicial 4. Analisar resultados da análise de risco inicial
10. Resultados	
Resultados esperados	Obter procedimentos padronizados e documentados para gestão de riscos de segurança, avaliando regularmente a probabilidade e o impacto dos riscos identificados
11. Custos	
Recursos financeiros previstos	A definir

Detalhamento das atividades

Atividade	Responsável	Início	Término
1. Estabelecer plano de aceitação e tratamento de riscos 1.1. Definir critérios para tratamento de riscos; 1.2. Definir critérios para aceitação de riscos.	Comitê de Segurança da Informação		
2. Estabelecer processo periódico de análise de risco 2.1. Definir periodicidade das análises de risco; 2.2. Definir escopo dos ativos, segundo critérios de classificação da informação; 2.3. Definir escopo das análises de risco.	Comitê de Segurança da Informação		
3. Efetuar análise de risco inicial 3.1. Inventariar ativos; 3.2. Efetuar análise de risco; 3.3. Informar resultados da análise de risco.	Setor de Segurança em Tecnologia da Informação		
4. Analisar resultados da análise de risco inicial 4.1. Analisar resultados da análise de risco; 4.2. Decidir que riscos serão aceitos e que riscos deverão ser tratados; 4.3. Priorizar riscos que devem ser tratados.	Comitê de Segurança da Informação		