PLANO DE PROJETO

REVISÕES

Data	Versão	Autor	Alterações
25.04.2018	1.0	Lucas Pozatti	Criação do plano
11.05.2018	1.1	Lucas Pozatti	Ajuste no escopo

1. IDENTIFICAÇÃO DO PROJETO

ID	490	**Classificação**	Complexo
Nome do Projeto	Avaliação de segurança do ambiente tecnológico		
Gerente do Projeto	Lucas Pozatti		
Data da Solicitação	13/12/2017		
Representante do Negócio	Natacha Moraes de Oliveira		
Unidade Organizacional	Secretaria de Tecnologia da Informação e Comunicações		
Áreas Beneficiadas	TRT como um todo, uma vez que o projeto visa aumentar o nível de segurança da TI.		

2. ALINHAMENTO ESTRATÉGICO

Área	Escritório de Segurança da Informação
PDTI	PDTI 2018
Objetivo Estratégico TIC	Aprimorar a segurança da informação
Objetivo Estratégico Institucional	Promover a inovação, integração e atualização dos sistemas de informação

3. JUSTIFICATIVA

O ESI executou em 2015 e 2017 ciclos do SGSI, cujo objetivo foi avaliar o nível de maturidade de segurança da informação, através da execução de análise de riscos do ambiente tecnológico e tratamento daqueles considerados como prioritários. Tais análises foram realizadas por meio de resposta de questionários específicos, relacionados às tecnologias que suportam a atividade de prestação jurisdicional.

Apesar de tal abordagem prover um bom panorama da situação de segurança da informação, verificou-se a necessidade de realizar uma avaliação de segurança do ambiente tecnológico de uma forma mais prática, ou seja, realizando a análise de vulnerabilidades e de fraquezas diretamente nos ativos, por meio de escaneadores

de vulnerabilidade. Esse tipo de software possui um banco de dados de vulnerabilidades e varre o ambiente em busca de pontos fracos, críticos ou não, encontrados em ativos e sistemas. O ponto positivo dessa abordagem é que ela não é subjetiva, não dependendo da interpretação que uma pessoa dá a um determinado questionário.

Outra forma prática de avaliar o ambiente tecnológico, bastante comum no mercado, é a realização de *pentest*, ou, em português, testes de invasão. Essa atividade é uma simulação onde uma pessoa executa os passos de um atacante que tenta invadir a rede, para ter acesso a dados confidenciais, escalar privilégios em serviços e sistemas, causar algum dano à empresa, dentre outras ações, por meio da exploração de vulnerabilidades encontradas no ambiente tecnológico. Além de testar os mecanismos de defesa do Tribunal, essa atividade permite avaliar se o monitoramento do ambiente está sendo executada de forma eficiente.

Os principais serviços do TRT são disponibilizados na web (PJe, consulta processual) e ainda há a tendência de migrar outros serviços para web. Entretanto, não são realizados testes para verificar as possíveis vulnerabilidades dos serviços e infraestrutura tecnológica por equipe diversa daquela que os desenvolve ou mantém. Embora no segundo ciclo do SGSI, tenha sido verificado um aumento da maturidade da segurança da informação (atingindo um percentual de aproximadamente 75% de nível de segurança), o foco foi mais a nível de gestão, diante do grande número de ativos envolvidos.

4. OBJETIVOS E BENEFÍCIOS ESPERADOS PARA O NEGÓCIO

Objetivo: Esse projeto tem por objetivo analisar as opções oferecidas pelo mercado para a realização da avaliação de segurança do ambiente tecnológico do TRT4, a fim de indicar qual seria a solução de melhor custo/benefício a se contratar, que atende aos requisitos desse Tribunal: a realização de uma quantidade limitada de pentests e/ou análise de vulnerabilidade; ou a contratação de um serviço de monitoramento de segurança, abrangendo, dentre outras coisas testes de invasão e análise de vulnerabilidade.
Depois, caso seja decidido pela realização da contratação, o projeto poderá abranger a contratação e a execução do objeto. Esse objetivo será discutido e avaliado posteriormente.

Benefício (descrição e seu valor esperado)	**Situação atual**	**Sugestão de como medir**
Melhorar o nível de segurança dos serviços de TIC (caso seja contratada alguma solução indicada no estudo)	A gestão de vulnerabilidades é feita de forma pontual, sem um processo e uma ferramenta definidos para tal.	Extração de relatório após a execução das análises

5. DESCRIÇÃO DO ESCOPO

O escopo do projeto abrange a pesquisa das soluções disponíveis no mercado e elaboração de um relatório para subsidiar a SETIC quanto à decisão de adotar ou não uma das soluções. Caso após a apresentação do relatório seja decidido pela contratação de uma das soluções apresentadas, será feita uma solicitação de mudança para aumentar o escopo do projeto, podendo abranger desde a contratação até o final da execução do objeto contratado.

Para tanto, serão necessárias as seguintes etapas:

- Estudo das soluções existentes no mercado;

- Entrevistas com os fornecedores;
- Estudo dos editais de licitação para esta área;
- Definição dos requisitos desejados para um serviço de monitoramento de segurança pelo TRT;
- Elaboração de um relatório final analisando as soluções estudadas e uma proposta de qual seria a mais adequada para o TRT.
- Decisão, por parte do Comitê Gestor de TIC, quanto à contratação ou não de uma das soluções propostas.

6. LIMITES

Não fazem parte do escopo **inicial** deste projeto:

- A aquisição de nenhum produto;
- A geração dos documentos exigidos no processo de aquisição formal do TRT;
- A instalação permanente de algum software na infraestrutura do TRT.

7. ENTREGAS DO PROJETO

- Elaboração e aprovação do Plano de Projeto;
- Estudo das soluções disponíveis no mercado
- Decisão de adoção de solução
- Encerramento do projeto

8. PREMISSAS

- Os fornecedores contatados estarão disponíveis para as reuniões de apresentação das soluções;
- Apoio da SETIC e suas áreas para avaliação das soluções e definição daquilo que seria necessário para o atendimento de suas necessidades relacionadas ao objeto do estudo;

9. RESTRIÇÕES

- O código do PJe não será considerado para o estudo das soluções de análise de vulnerabilidades e pentest e nem na ocorrência de contratação de serviços de pentest ou serviço de monitoramento de segurança;
- Para fins de estudos e realização de estimativas de orçamento, será informado aos fornecedores que a intenção do TRT é que a gestão dos ativos de infra e implementação de possíveis correções de vulnerabilidades fiquem sob responsabilidade da SETIC.

10. CRONOGRAMA

	Título	Duração	Início	Fim	Prede...	Responsáveis
1	**Avaliação de Segurança do Ambiente Tecnológico**	101 Dias	19/01/2018	20/06/2018		LUCAS POZATTI
2	Gerenciamento do Projeto	101 Dias	19/01/2018	20/06/2018		LUCAS POZATTI
3	Planejamento	80 Dias	19/01/2018	21/05/2018		LUCAS POZATTI
10	Monitoramento	1 Dias	19/01/2018	19/01/2018		LUCAS POZATTI
12	Gestão de Mudança	2 Dias	29/05/2018	30/05/2018		LUCAS POZATTI
13	Mudança 1 - Replanejamento do projeto, conforme solução a ser contratada	2 Dias	29/05/2018	30/05/2018		LUCAS POZATTI
14	Anexar registro de mudança e plano de projeto atualizado	1 Dias	29/05/2018	29/05/2018	35	LUCAS POZATTI
15	Gerar nova linha de base do cronograma	1 Dias	30/05/2018	30/05/2018	14	LUCAS POZATTI
16	**Encerramento do projeto**	**16 Dias**	**29/05/2018**	**20/06/2018**		**LUCAS POZATTI**
24	**Estudo das soluções disponíveis no mercado**	**77 Dias**	**23/01/2018**	**18/05/2018**		**LUCAS POZATTI**
25	Reunião 01 - On-Security	1 Dias	23/01/2018	23/01/2018		LUCAS POZATTI
26	Reunião 02 - DropReal	1 Dias	23/01/2018	23/01/2018		LUCAS POZATTI
27	Reunião 03 - On-Security	1 Dias	02/04/2018	02/04/2018		LUCAS POZATTI
28	Reunião 04 - Agility Networks	1 Dias	11/04/2018	11/04/2018		LUCAS POZATTI
29	Reunião 05 - On-Security - Apresentação de proposta	1 Dias	12/04/2018	12/04/2018		LUCAS POZATTI
30	Reunião 06 - Service IT	1 Dias	18/04/2018	18/04/2018		LUCAS POZATTI
31	Reunião 07 - Agility Networks	1 Dias	02/05/2018	02/05/2018		LUCAS POZATTI
32	Elaborar relatório de estudo das soluções	10 Dias	07/05/2018	18/05/2018		LUCAS POZATTI
33	**Decisão de adoção de solução**	**6 Dias**	**21/05/2018**	**28/05/2018**		**LUCAS POZATTI**
34	Apresentar sugestão de solução a ser contratada	1 Dias	21/05/2018	21/05/2018	32	LUCAS POZATTI
35	Decidir contratação de solução	5 Dias	22/05/2018	28/05/2018	34	LUCAS POZATTI

11. MAPA DAS RESPONSABILIDADES

Nome	Área/Cargo	Responsabilidades
Lucas Pozatti	ESI	Gerente do projeto / Execução do projeto
Alberto Muller	CGTIC	Apoiar execução do projeto / Avaliar proposta contida no relatório
André Farias	CDS	Avaliar proposta contida no relatório
Paulo Mendes	CIT	Avaliar proposta contida no relatório
Natacha Moraes	SETIC	Avaliar proposta contida no relatório

12. ESTIMATIVAS DE CUSTOS

Tipo do Custo *	Aquisição é escopo do Projeto (S/N)	Custo Previsto (R$)	Custo Realizado (Empenhado) (R$)
Projeto não possui custos (de acordo com o escopo inicial)	N	0	0
Total dos Custos		**0**	**0**

*** Custos com recursos humanos internos não são contabilizados.**
*** Custo previsto do projeto deve estar contido e aprovado no Plano de Contratações de TIC (CGTIC).**

13. RISCOS

ID 01	**TÍTULO : Impossibilidade de conhecer as soluções disponíveis no mercado**		
Estado	**Causa**		
Identificado	Inexistência de fornecedores para apresentar as soluções disponíveis no mercado		
Probabilidade	**Impacto / efeito**		**Criticidade**
Baixa	**Nível**	**Descrição**	Média
	Alto	Impossibilidade de avaliação das soluções, dificultando sobremaneira a redação do relatório	
Resposta	**Tipo**	Aceitar	
	Ação	Reportar no relatório	

14. CONSIDERAÇÕES ADICIONAIS

N/A

15. APROVAÇÃO

Nome	Papel no Projeto/Área	Assinatura