TRIBUNAL REGIONAL DO
TRABALHO DA 2ª REGIÃO

TERMO DE ABERTURA DO PROJETO

1. INFORMAÇÕES DO PROJETO

Código	PDTIC 007-2019
Nome	PDTIC 007-2019 - Autoridade Certificadora Interna
Nome do Demandante	CSIC
Área do Demandante	CSIC
Gerente do Projeto	Edson Ribeiro da Silva
Substituto do Gerente do Projeto	Ramon Chiara

2. JUSTIFICATIVA

Durante os trabalhos de tratamento dos riscos identificados pela Análise de Riscos realizada em 2016, foi identificado que a verificação de autenticidade das requisições de servidores deve ser habilitada. Com este recurso, será realizada uma verificação do nome da máquina que faz a requisição. Caso esse nome não corresponda ao "cn" do certificado, mensagens de erro e de auditoria apropriadas serão registradas. É recomendado habilitar esta opção para proteger as conexões "SSL" de saída do "Directory Server" contra um ataque de "man-in-the-middle". No caso do TRT2, o "Directory Server" é implementado por meio de servidores "LDAP". Para que se possa verificar o certificado de clientes, cada um deve ter um certificado único. Isso é possível se forem instalados certificados digitais para cada servidor ou aplicação cliente do LDAP. Em reunião ocorrida no dia 04/12/2017, o risco foi considerado aceito pelo CSIC. Entretanto, o Comitê solicitou que fosse realizado um estudo de custo para implementação de uma Autoridade Certificadora Interna ou aquisição dos certificados, com o objetivo de avaliar se é um risco que pode ser tratado futuramente. Após pesquisa da equipe técnica e consulta aos demais Regionais que já têm a autoridade certificadora, a dificuldade técnica para implementação da solução estaria superada. Desta forma, o Comitê determinou, em reunião ocorrida em 26/03/2018, a criação da Autoridade Certificadora, de modo que a verificação de autenticidade das requisições de servidores possa ser habilitada e o risco seja tratado.

3. OBJETIVO

Criação da Autoridade Certificadora Interna do TRT2 no ambiente de produção (com certificado raiz e certificados intermediários), na qual serão hospedados o serviço Online Certificate Status Protocol (OCSP) - Serviço que responde com o status de revogação de certificados e a lista de certificados revogados. O funcionamento em produção será demonstrado com a emissão do certificado digital para uma única máquina.

4. ASPECTOS ESTRATÉGICOS

PETIC – OE3 - Aprimorar a gestão de riscos de TIC e PETIC – Ação 9: Garantir que todos os processos críticos de negócio tenham seus riscos de TIC identificados, avaliados e tratados

5. PROJETOS RELACIONADOS

Não há

6. DECLARAÇÃO DO ESCOPO

Fase 1 - Pesquisa.
Pesquisar padrões de mercado para criação e gerenciamento de certificados digitais.
Definir Autoridade Certificadora Interna em ambiente de homologação e forma de validação de certificados revogados.
Pesquisa de padrões criptográficos e prazos de validade.
Documentar as informações obtidas na pesquisa.

Fase 2 - Homologação.
Criação da Autoridade Certificadora e geração de certificados em ambiente de homologação com OpenSSL e EJBCA
Geração da Lista de Certificados Revogados (LCR) e hospedagem em ambiente de homologação.
Testar os servidores LDAP para receber pedidos com criptografia na autenticação.
Executar testes para verificar se mensagens de erro e de auditoria apropriadas são registradas quando há falha na autenticidade dos pedidos para o LDAP.
Executar testes para verificar se mensagens de erro e de auditoria apropriadas são registradas quando há pedidos de servidores que tenham certificados revogados.
Documentar as atividades envolvidas na criação da Autoridade Certificadora Interna em ambiente de homologação.

Fase 3 - Produção.
Definir padrões criptográficos
Emitir Certificado Raiz
Emitir Certificado Intermediário
Emitir Certificado Final
Garantir o funcionamento da Lista de Certificados revogados (LCR) e Online Certificate Status Protocol (OCSP) - Serviço que responde com o status de revogação de certificados.
Elaborar manual para solicitação de certificados.

7. EXCLUSÃO DE ESCOPO

Instalação de certificados finais nos equipamentos e servidores de homologação ou produção. Esta atividade será desempenhada de acordo com a disponibilidade das equipes da CITIC para o tratamento do risco.
Configuração dos servidores LDAP para receber pedidos com criptografia na autenticação. Esta atividade depende da instalação de certificados para equipamentos do ambiente de produção, uma vez que, configurados os servidores LDAP, eles só passarão a atender as requisições com certificados válidos.

8. PREMISSAS

Disponibilidade do responsável realizar pesquisas, testes e execução dentro dos prazos previstos neste projeto.
Participação efetiva das equipes e áreas envolvidas no projeto, fornecendo todas as informações necessárias à execução das atividades e a executando as tarefas dentro do cronograma do projeto

9. RESTRIÇÕES

Não foram identificadas restrições específicas.

10. ESTIMATIVAS INICIAIS

Duração (em meses)	7
Custos externos (R$)	

11. PRINCIPAIS ETAPAS

Relatório da pesquisa.
Relatório de testes em ambiente de homologação.
Manual de instalação e configuração da AC em produção.
Manual de solicitação de certificado.
Definição de processo de solicitação de certificado.
Relatório de instalação do serviço EJBCA com OCSP.
Manual de solicitação de certificado com a nova solução.

12. RISCOS INICIAIS

Ausência de conhecimento em EJBCA e Wildfly que possuem suporte pago que não será contratado.
Ausência de capacitação nas ferramentas OpenLDAP, OpenSSL, EJBCA, Apache, OCSP, Algorítimos de criptografia.
Ausência de suporte especializado, para o OpenLDAP e Apache que são ferramentas Open Source.
Disponibilidade das equipes de infraestrutura na fase de homologação, produção e execução.
Dificuldades nos testes que podem indicar trabalho de pesquisa insuficiente.

13. APROVAÇÃO

Des. Jucirema Maria Godinho Gonçalves

Comitê de Segurança da Informação e Comunicação