



MINISTÉRIO DA EDUCAÇÃO
FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO
DIRETORIA DE GESTÃO, ARTICULAÇÃO E PROJETOS EDUCACIONAIS

TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE PESSOA FÍSICA
- CONSULTOR POR PRODUTO -

TOR/FNDE/DIRTE/CGINF Nº 024/2014

1. Projeto

OEI - BRA09/004 - Aprimoramento da sistemática de gestão do Ministério da Educação - MEC em seus processos de formulação, implantação e avaliação do Plano Nacional da Educação – PNE.

2. Finalidade de Contratação

Contratar serviço especializado de consultoria para estruturar propostas técnicas alinhadas às melhores práticas de segurança da tecnologia da informação, visando à avaliação e agregação de tecnologias baseadas no Gerenciamento de Segurança da TI, com foco nas melhores práticas de segurança do mercado de tecnologia da informação nacionais e internacionais, assim como a definição de métricas operacionais adequadas relacionadas à consolidação do Plano Nacional da Educação – PNE, suprimindo as necessidades dos Sistemas utilizados pelo FNDE que atendem diretamente ao PNE.

3. Enquadramento nas ações do Projeto

3.1. Resultado

Resultado 1.1. Estudos diagnósticos concebidos e realizados para identificação das necessidades institucionais, das tipologias e dos delineamentos referentes aos novos sistemas tecnológicos aplicáveis à implantação do PDE.

3.2. Atividade

Atividade 1.1.2. Desenvolver processos de trabalho adequados aos novos sistemas e redes digitais utilizados na implantação do PDE.

4. Justificativa

O Ministério da Educação (MEC), por meio da adoção e operacionalização do Plano Nacional da Educação (PNE) vem desenvolvendo ações relativas a profusão e capilarização de recursos investidos na educação federal, com vistas a beneficiar a sociedade brasileira. O PNE tem sido difundido por meio da forte utilização da tecnologia da Informação (TI).

O Fundo Nacional de Desenvolvimento da Educação (FNDE), como Autarquia Federal vinculada ao Ministério da Educação (MEC), tem respondido, dentro de sua competência institucional, por ações que visam apoiar e difundir as políticas públicas

de educação, notadamente o PNE, por meio de constante avanço de seu parque tecnológico que apoia tais ações.

É de conhecimento geral que a tecnologia da informação, quer seja aplicada em ambiente privado, como empresas no geral, quer seja aplicada em âmbito público, como na Administração Pública, sempre sofreu com ameaças tecnológicas, como ataques de grupos hackers/crackers buscando vulnerabilidades e brechas encontradas em fraquezas deixadas por sistemas computacionais. Vulnerabilidades e brechas da tecnologia têm sido apresentadas e exploradas em diversos pontos do mundo, pois a sociedade tem evoluído, fortemente, com base na utilização de instrumentos diversos, como *tablets*, *smartphones*, *notebooks*, computadores de trabalho. Toda essa pulverização tecnológica tem chamado a atenção de grupos maliciosos, como aqueles acima mencionados, com o objetivo de causar prejuízos em organizações e instituições públicas.

Toda tecnologia da informação necessita ser avaliada, estudada, mecanismos, metodologia e ferramentas necessitam ser implementados, expertise e conhecimento necessitam ser aplicados para se mitigar os riscos advindos das ameaças em questão.

Para que o FNDE possa manter a qualidade e segurança evolutiva do seu parque de TI, prestando o apoio necessário para os programas educacionais como o PNE, segundo o pressuposto da segurança da informação e comunicação, faz-se necessário buscar no mercado brasileiro consultoria especializada, orientada na implementação de requisitos, melhores práticas nacionais/ internacionais e metodologias de segurança em TI aplicadas a cada plataforma computacional em operação na autarquia.

O papel fundamental dessa consultoria será recomendar, com base em expertise técnica, soluções e metodologias que envolvam a segurança da TI nos pilares: usuários, informação, dispositivos computacionais e sistemas corporativos a qual prestam suporte aos planos públicos de educação como o PNE.

Por fim, observa-se que as ações acima deverão ser realizadas por meio de 02 (duas) etapas, a fim de atender ao planejamento temporal e operacional da CGINF/DIRTE/FNDE quanto à avaliação, mensuração e devida implementação dos serviços de segurança em tecnologia da informação necessários para aumentar o nível de maturidade da organização nos pilares em questão.

5. Atividades que deverão ser executadas

5.1 Consultor (linha técnica: Gestão de Segurança em TI)

- a) Realizar levantamento do parque computacional atual do FNDE que atende às políticas públicas de educação, notadamente ao PNE, com relação aos usuários da autarquia que utilizam esse parque, bem como com relação à proteção atual das informações veiculadas no ambiente computacional da entidade;
- b) Propor, com base no levantamento do item “a”, modificações técnicas de segurança para aumentar a maturidade da organização na segurança dos seus ativos de tecnologia da informação;
- c) Realizar levantamento dos dispositivos tecnológicos e sistemas que trafegam informações corporativas e que apoiam as políticas públicas de educação sob competência do FNDE;

- d) Propor, com base no levantamento do item “c”, modificações técnicas de segurança para aumentar a maturidade da organização na segurança dos seus ativos de tecnologia da informação;
- e) Elaborar proposta de construção de Termo de Referência no viés técnico, contemplando requisitos técnicos das modificações de segurança avaliadas e sugeridas nos itens “b” e “d”, com aderência à INSTRUÇÃO NORMATIVA Nº 04, de 12 de novembro de 2010, da Secretária de Logística e Tecnologia da Informação – SLTI, para suporte seguro do parque tecnológico do FNDE que apoia as políticas públicas de educação;
- f) Identificar e analisar as melhores práticas de TI relativas à segurança da informação para implementação em modelo SOC (*Security Operations Center*) como boa prática para aumento da maturidade de segurança do FNDE para aplicação no parque computacional que apoia as políticas públicas de educação sob competência da Autarquia.

6. Produtos ou resultados previstos / remuneração / cronograma de entrega

PRODUTO	DATA DE ENTREGA
<p>Documento Técnico A:</p> <ul style="list-style-type: none"> - Documento técnico contendo proposta de mecanismos de segurança em TI para usuários e informações corporativas, incluindo diagnóstico do parque computacional atual do FNDE que atende às políticas públicas de educação, notadamente ao PNE, com relação aos usuários da autarquia que utilizam esse parque, bem como, com relação à proteção atual das informações veiculadas no ambiente computacional da entidade, propondo modificações técnicas de segurança para aumentar a maturidade da organização na segurança dos seus ativos de tecnologia da informação. - Proposta de mecanismos de segurança em dispositivos tecnológicos corporativos e sistemas organizacionais, incluindo diagnóstico dos dispositivos tecnológicos e sistemas que trafegam informações corporativas e que apoiam as políticas públicas de educação sob competência do FNDE, bem como propor modificações técnicas de segurança para aumentar a maturidade da organização na segurança dos seus ativos de tecnologia da informação. 	50 dias

<p>Documento Técnico B:</p> <ul style="list-style-type: none"> - Documento técnico contendo proposta de requisitos técnicos para subsidiar a solução de segurança avaliada e sugerida nos documentos “Proposta de segurança em TI para usuários e informações corporativas” e “Proposta de segurança em dispositivos tecnológicos corporativos e sistemas organizacionais”, com aderência à INSTRUÇÃO NORMATIVA Nº 04, de 12 de novembro de 2010, da Secretária de Logística e Tecnologia da Informação – SLTI. - Estudo sobre melhores práticas de TI relativas à segurança da informação para implementação em modelo SOC, que trará melhores práticas de SOC. 	<p>135 dias</p>
--	-----------------

7. Requisitos mínimos de qualificação

a. Formação acadêmica

Curso superior completo na área de Computação OU qualquer área de formação acrescida de pós-graduação na área de Tecnologia da Informação OU Segurança da Informação com carga horária mínima de 360 horas. Os cursos deverão ser reconhecidos pelo MEC.

b. Experiência profissional

Mínimo de 03 (três) anos em atividades de implementação e execução de ações relacionadas à área de Segurança da Informação e Comunicações para TI.

c. Conhecimento desejável

- Certificações relativas à Segurança da Informação e Comunicações;
- Conhecimento em arquitetura de Segurança da Informação e Comunicações;
- Conhecimento em Gestão de Incidentes de Segurança da Informação e Comunicações;
- Experiência na implementação e execução de produtos e serviços de Segurança da Informação e Comunicações, tais como firewall, antivírus, biometria e outros tipos de hardware e software de segurança;
- Conhecimentos em gestão de Segurança da Informação e Comunicações baseado nas melhores práticas de mercado;
- Conhecimentos em elaboração de Editais de contratação de serviços de TI considerando as Instruções normativas do Ministério do Planejamento;
- Conhecimento sobre referências legais e normativas de Segurança da Informação e Comunicações: ISO27000, ISO31000, ISO22300, Instruções Normativas e Normas Complementares do GSIPR;
- Conhecimento sobre referências legais e normativas de governança de TI: ISO20000, COBIT, COSO.
- Consultoria profissional especificamente no âmbito da Administração Pública Federal.

OBS.: A formação e a experiência serão comprovadas por meio de apresentação de documentos tais como: contratos de trabalho e/ou de prestação de serviços, registro em carteira de trabalho ou documentos equivalentes.

As certificações/conhecimentos desejáveis serão pontuados para efeito de classificação e considerados em caso de empate entre os candidatos.

8. Processo Seletivo

8.1 O Processo Seletivo se dará em Brasília e os custos de transporte, hospedagem e alimentação, se necessários, são de responsabilidade do candidato.

8.2 A etapa de entrevista **não** poderá ocorrer por vídeo-conferência ou teleconferência.

8.3 A participação no processo seletivo implica na aceitação integral e irrevogável dos termos deste edital.

8.4 O processo seletivo terá validade até 31/12/2014.

8.5 A seleção simplificada é pautada pela análise de currículos e entrevista, conforme segue:

I - PRIMEIRA ETAPA – Análise de Currículos

a) Serão eliminados os currículos inscritos que não atenderem integralmente os requisitos obrigatórios exigidos divulgados no edital.

b) Nesta etapa será aferida pontuação para os currículos inscritos que atendem aos requisitos obrigatórios.

c) A pontuação será atribuída conforme quadro abaixo.

d) Serão indicados para a etapa de entrevistas os candidatos que atenderam aos requisitos obrigatórios mínimos exigidos no edital.

e) O total de pontos recebidos nesta etapa irá compor a pontuação total recebida pelo candidato. PT (Pontuação Total) = PC (Pontuação de Currículo) + PE (Pontuação de Entrevista).

II - SEGUNDA ETAPA – Pontuação de Entrevistas

a) Serão indicados para a etapa de entrevistas os candidatos que atenderam integralmente aos requisitos obrigatórios mínimos exigidos no edital

b) Poderá ser aplicada avaliação para mensurar o conhecimento do candidato.

Critérios de avaliação e seleção

A. Formação acadêmica (Pontuação escalar - Máximo de 05 pontos)		Pontuação
A1	Curso superior completo na área de Computação OU qualquer área de formação, acrescida de pós-graduação na área de Tecnologia da Informação OU Segurança da Informação com carga horária mínima de 360 horas.	5,0

B. Experiência profissional (Pontuação escalar - Máximo de 05 pontos)		Pontuação
B1	Mínimo de 03 (três) anos em atividades de implementação e execução de ações relacionadas à área de Segurança da Informação e Comunicações para TI.	5,0

C. Entrevista (Pontuação cumulativa - Máximo de 60,0 pontos)		Pontuação
C1	Se expressa com polidez, objetividade e fluência verbal e demonstra boa capacidade de raciocínio.	1,0 a 5,0 pontos
C2	Apresenta Certificações relativas à Segurança da Informação e Comunicações.	10,0 pontos
C3	Apresenta conhecimento em arquitetura de Segurança da Informação e Comunicações.	5,0 pontos
C4	Apresenta conhecimento em Gestão de Incidentes de Segurança da Informação e Comunicações.	5,0 pontos
C5	Apresenta experiência na implementação e execução de produtos e serviços de Segurança da Informação e Comunicações, tais como firewall, antivírus, biometria e outros tipos de hardware e software de segurança.	5,0 pontos
C6	Apresenta conhecimento em gestão de Segurança da Informação e Comunicações baseado nas melhores práticas de mercado.	5,0 pontos
C7	Apresenta conhecimentos em elaboração de Editais de contratação de serviços de TI considerando as Instruções normativas do Ministério do Planejamento.	5,0 pontos
C8	Apresenta conhecimentos sobre referências legais e normativas de Segurança da Informação e Comunicações: ISO27000, ISO31000, ISO22300, Instruções Normativas e Normas Complementares do GSIPR.	5,0 pontos
C9	Apresenta conhecimentos sobre referências legais e normativas de governança de TI: ISO20000, COBIT, COSO.	5,0 pontos
C10	Atuou em prestação de serviços de consultoria profissional especificamente no âmbito da Administração Pública Federal	1,0 a 10,0 pontos
Na entrevista pessoal serão exigidos os documentos comprobatórios dos itens A e B.		

9. Vigência do contrato: Em até 04 (quatro) meses e 15 dias a partir da assinatura do contrato.

10. Número de vagas: 01 (uma) vaga.

11. Local de Trabalho: as atividades serão desenvolvidas na CGINF/DIRTE/FNDE/MEC, situada no SBS Quadra 02 – Brasília – DF.

12. Considerações gerais

Os produtos deverão ser entregues à Coordenação Geral de Infraestrutura Tecnológica – CGINF/DIRTE/FNDE, Brasília/DF, em versão preliminar e, após aprovação, em sua forma definitiva, com as devidas referências bibliográficas (quando necessário), em 2 (dois) exemplares gravados em CD ROM, na versão MS Word 2000 ou Open Office, contendo a identificação do consultor na capa dos exemplares.

A execução dos trabalhos previstos neste TOR – Termo de Referência – não implica qualquer relação de emprego ou vínculo trabalhista, sendo, portanto, regido

sem subordinação jurídica, conforme prevê o parágrafo 9º do Art. 4º do Decreto nº 5.151/2004.

O(a) consultor(a) deve ter disponibilidade para executar atividades no Ministério da Educação e/ou no Fundo Nacional de Desenvolvimento da Educação, em horário comercial, para que tenha acesso à plataforma de desenvolvimento dos Sistemas, que só pode ser acessada nas dependências do Ministério da Educação – e às informações necessárias à elaboração dos produtos propostos.

Os direitos autorais ou quaisquer outros direitos, de qualquer natureza, sobre materiais produzidos no âmbito desse trabalho pertencerão exclusivamente ao Ministério da Educação, e sua utilização e/ou reprodução total ou parcial requererá autorização prévia do Ministério da Educação.

Caso ocorra interrupção do contrato durante a sua vigência, os serviços de consultoria poderão ser conduzidos pelo próximo candidato selecionado, conforme cadastro reserva e necessidade da área demandante.

Brasília, 23 de julho de 2014.