1. Número e Título do Projeto:

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

2. Objetivo / Finalidade da Consultoria

Realizar estudos e proposições de atualização e aperfeiçoamento dos processos tecnológicos utilizados pelo Inep no que tange ao processo de respostas a incidentes, de forma a tornar a infraestrutura mais segura, por meio da criação de ambiente NOC/SOC (Network Operation Center/ Security Operation Center) institucional.

3. Enquadramento das Ações no Projeto

3.1 Resultados:

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 Atividades:

1.1.1. Formular pesquisa diagnóstica sobre níveis de adequabilidade tecnológica dos sistemas e redes digitais utilizados na implantação do PDE.

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

1.1.3. Diagnosticar as novas exigências tecnológico/informacionais para a implantação do PDE.

1.1.5. Realizar estudos para identificar e relacionar as possibilidades de adequação (customização) dos atuais sistemas digitais em uso no MEC.

4. Justificativa

Com o objetivo de dar celeridade à execução das opções das ações do Plano de Desenvolvimento de Educação – PDE, o MEC firmou parceria com a Organização dos Estados Ibero-americanos, para Educação, a Ciência e a Cultura – OEI para executar o Projeto "Aprimoramento da sistemática de gestão do Ministério da Educação - MEC em seus processos de formulação, implantação e avaliação do Plano de Desenvolvimento da Educação – PDE".

O Programa de Desenvolvimento da Educação - PDE está sustentado em seis pilares: i) visão sistêmica da educação, ii) territorialidade, iii) desenvolvimento, iv) regime de colaboração, v) responsabilização e vi) mobilização social – que são desdobramentos consequentes de principio e objetivos constitucionais, com a finalidade de expressar o enlace necessário entre educação, território e desenvolvimento, de um lado, e o enlace entre equidade e potencialidade, de outro.

Tal concepção implica, adicionalmente, em melhorar, ampliar e disponibilizar aos estados, o Distrito Federal, e aos municípios instrumentos eficazes necessários à implementação de políticas públicas e de melhoria da qualidade da educação e, inclusive, viabilizar acesso pela sociedade a informações transparentes que promovam o debate em torno das políticas de desenvolvimento da educação de modo a permitir o efetivo acompanhamento e fiscalização do cumprimento dos deveres do Estado e o engajamento consciente em defesa da educação.

Visando subsidiar o MEC na consecução dos objetivos do PDE e voltado à sua missão institucional de retratar e oferecer aos agentes públicos e à sociedade em geral informações educacionais fidedignas a partir de estudos, avaliações e pesquisas, o Inep necessita incrementar sua performance mediante o aprimoramento de sua estrutura tecnológica.

Hoje, o Inep suporta sistemas como o EducaCenso (Censo da Educação básica por aluno), Censo da Educação Superior, ENEM (Exame Nacional do Ensino Médio), ENADE (Exame Nacional de Desempenho de Estudantes), Prova Brasil, Sistema Sinaes (Sistema Nacional de Avaliação da Educação Superior). Em virtude disto é necessária uma infraestrutura que garanta estabilidade, segurança, alta-disponibilidade e agilidade na utilização e no armazenamento de dados provenientes desses sistemas.

Para o perfeito funcionamento de toda rede computacional e a integridade e sigilo dos serviços e dados que utilizam essa rede é primordial garantir e melhorar os processos de segurança, em especial o de monitoração, garantindo a disponibilidade e segurança das informações, dos ambientes e das ferramentas de trabalho que compõem a infra-estrutura do Inep.

Como ponto fundamental ao atendimento do objetivo descrito torna-se necessária a implantação de uma sistemática de gerência de incidentes envolvendo ativos que compõem a rede de dados e voz do Inep. Atualmente, as melhores práticas de mercado estabelecem como ponto pacífico de discussões a criação de um ambiente de NOC/SOC (Network Operation Center/

Security Operation Center). Esta estrutura objetiva consolidar dados provenientes da gerência e monitoração realizada sobre os ativos existentes através de ferramentas diversas – como Checkpoint SmartCenter, SourceFire Defence Center, F5 Manager e Zabbix – bem como o tratamento destes dados, criando ações de respostas aos incidentes constatados no ambiente.

O Ambiente de NOC/SOC utiliza os dados gerados pela monitoração de disponibilidade de ativos e provê insumos para respaldar decisões em momentos de alta criticidade. Ele também garante documentação exaustiva do incidentes de segurança.

A criação deste ambiente envolve investimento em geração de projetos contendo infraestrutura, metodologias, normas e consolidação do ambiente tecnológico levando em consideração as variáveis de implementação existentes. O conhecimento profundo em tecnologia é fundamental e deve basear-se em segurança da informação.

É nesse contexto que se propõe a contratação objeto deste termo de referência, que visa a construção de um plano detalhado para construção de um GRI (Grupo de Respostas a Incidentes) institucional, de forma a operacionalizar as ações a serem tomadas em razão da ocorrência de incidentes, reestruturando e redefinindo diversos procedimentos para que a rede computacional do Inep suporte as aplicações e os sistemas que precisam ser disponibilizados aos respectivos usuários, garantindo sempre a manutenção da confidencialidade, integridade e disponibilidade das informações, além de obter ganhos em segurança, performance e flexibilidade.

5. Atividades que deverão ser executadas

5.1 Consultor 1:

ATIVIDADES E PRODUTO 1:
Atividade 1:

- Identificar, dentre os ativos existentes na infraestrutura do Inep, aqueles que serão inseridos no NOC/SOC (Network Operation Center/ Security Operation Center) para monitoração e gerenciamento dos ativos e sistemas de segurança computacional do Inep;
- Especificar critérios de monitoração para cada ativo de segurança;
- Elaborar proposta de otimização dos recursos de segurança disponíveis no Inep e sugerir, se necessário, aquisição de novos ativos para melhoria da infraestrutura, com respectivas especificações técnicas.

Produto 1:
Documento técnico (A) contendo mapeamento e critérios de monitoração dos ativos de segurança a serem inseridos no NOC/SOC (Network Operation Center/ Security Operation Center), contemplando os critérios e recursos de segurança necessários.

ATIVIDADES E PRODUTO 2:
Atividade 2:

- Definir arquitetura, metodologia e aplicabilidade para criação do NOC/SOC (Network Operation Center/ Security Operation Center) para monitoração e gerenciamento dos ativos e sistemas de segurança computacional do INEP;
- Definir os critérios para integração da monitoração, gerenciamento e identificação de incidentes de disponibilidade, decréscimos de performance, segurança e redimencionamento de recursos;
- Elaborar proposta de projeto para criação do NOC/SOC, contemplando projeto físico, lógico e vinculação legal para integração dos recursos mínimos de Firewall (Checkpoint), IPS (SourceFire), Balanceadores de Carga (F5), sistemas de Armazenamento (Netapp) e Sistemas Operacionais (Linux e Windows).

Produto 2:
Documento técnico (B) contendo proposta de projeto para criação de um NOC/SOC, que integre a monitoração, o gerenciamento e a identificação de incidentes, contemplando projeto físico, lógico e legal para integração dos recursos.

ATIVIDADES E PRODUTO 3:
Atividade 3:

- Identificar normas para criação e suporte de equipe a compor o GRI (Grupo de resposta a incidentes);
- Elaborar proposta metodológica para operacionalização de GRI a ser implementado no Inep;

- Elaborar fluxograma de execução de procedimentos e responsabilidades em caso de incidentes;
- Mapear organograma funcional do GRI.

Produto 3:
Documento técnico (C) contendo proposta de projeto para implantação e operacionalização do GRI (Grupo de resposta a incidentes) a ser implementado no Inep, contemplando estrutura e fluxogramas necessários para execução de procedimentos em caso de incidentes, bem como definição de atribuições e responsabilidades de cada componente.

ATIVIDADES E PRODUTO 4:
Atividade 4:
– Identificar técnicas de correlação de eventos (incidentes) segundo modelo ITIL (Event Management process - *correlation engine*), a serem utilizadas no Inep;
- Elaborar, procedimentos adequados de correlação de eventos e de decomposições das correlações;
- Desenvolver proposta de projeto de correlação de eventos, seguindo modelo ITIL, de forma a especificar e detalhar os procedimentos de correlação de eventos (incidentes) e os respectivos responsáveis (do GRI).

Produto 4:
Documento técnico (D) contendo proposta de projeto, seguindo o modelo ITIL (*correlation engine)*, para implantação e operacionalização de metodologia baseada em operações de serviço e procedimentos de correlação de eventos para os componentes do GRI.

ATIVIDADES E PRODUTO 5:
Atividade 5:
- Criar Metodologia de Teste de Intrusão para Avaliação da eficiência da infra-estrutura do NOC/SOC e GRI proposto para o Inep;
- Executar Teste de Intrusão para Avaliação da eficiência da infra-estrutura do NOC/SOC e GRI;
- Avaliar resultado dos testes realizados, identificando falhas, lições aprendidas e pontos positivos.

Produto 5:
Documento técnico (E) contendo resultado da avaliação dos Testes de Intrusão, contemplando o descritivo da metodologia dos testes aplicados, a avaliação das respostas e ações do GRI e recomendações técnicas.

ATIVIDADES E PRODUTO 6:
Atividade 6:
- Elaborar de material para seminários e treinamento específicos a equipe do GRI sobre ações em momentos de alta criticidade;
- Elaborar documentação para manutenção e gestão do NOC/SOC;

- Realizar transferência de conhecimento para equipe técnica responsável sobre a escalabilidade e novas integrações ao ambiente de NOC/SOC (Network Operation Center/ Security Operation Center) criado no INEP, garantindo assim a continuidade da integrabilidade do ambiente de NOC/SOC (Network Operation Center/ Security Operation Center) e o ambiente de produção dos sistemas que envolvem o Inep.

Produto 6:
Documento técnico (F) contendo consolidação da documentação desenvolvida, bem como descritivo das capacitações e seminários realizados.

6. Produtos ou Resultados previstos

PRODUTOS – Consultor 1	DATA DE ENTREGA
Produto 1: Documento técnico (A) contendo mapeamento e critérios de monitoração dos ativos de segurança a serem inseridos no NOC/SOC (Network Operation Center/ Security Operation Center), contemplando os critérios e recursos de segurança necessários.	14/05/2010
Produto 2: Documento técnico (B) contendo proposta de projeto para criação de um NOC/SOC, que integre a monitoração, o gerenciamento e a identificação de incidentes, contemplando projeto físico, lógico e legal para integração dos recursos.	02/07/2010
Produto 3: Documento técnico (C) contendo proposta de projeto para implantação e operacionalização do GRI (Grupo de resposta a incidentes) a ser implementado no Inep, contemplando estrutura e fluxogramas necessários para execução de procedimentos em caso de incidentes, bem como definição de atribuições e responsabilidades de cada componente.	24/09/2010
Produto 4: Documento técnico (D) contendo proposta de projeto, seguindo o modelo ITIL (*correlation engine)*, para implantação e operacionalização de metodologia baseada em operações de serviço e procedimentos de correlação de eventos para os componentes do GRI.	19/11/2010
Produto 5: Documento técnico (E) contendo resultado da avaliação dos Testes de Intrusão, contemplando o descritivo da metodologia dos testes aplicados, a avaliação das respostas e ações do GRI e recomendações técnicas.	03/01/2011
Produto 6: Documento técnico (F) contendo consolidação da documentação desenvolvida, bem como descritivo das capacitações e seminários realizados.	01/04/2011

7. PERFIL: Consultor em Segurança de Informações / Infraestrutura / Convergência

8. Requisitos Mínimos de Qualificação

Descrição:

A - FORMAÇÃO:

- Diploma de conclusão de curso de nível superior, devidamente reconhecido pelo MEC, em pelo menos um dos seguintes cursos: Análise de Sistemas, Processamento de Dados, Ciência da Computação ou áreas afins a Tecnologia da Informação, ou diploma de conclusão de curso de nível superior, devidamente reconhecido pelo MEC, em qualquer área, acompanhado de certificado de curso de pós-graduação stricto e/ou lato senso na área de Tecnologia da Informação de, no mínimo, 360 horas, fornecido por instituição reconhecida pelo MEC.

B – EXIGÊNCIAS ESPECÍFICAS

B1 - EXPERIÊNCIA PROFISSIONAL

- No mínimo 5 anos em atividades comprovadas relacionadas segurança da Informação;
- No mínimo 3 anos de experiência com produtos de Firewall Checkpoint
- No mínimo 3 anos de experiência com produtos de IPS SourceFire
- No mínimo 3 anos de experiência com balanceadores de Carga F5

B2 - Experiências / Certificações desejáveis:

- No mínimo 3 anos de experiência com sistemas de armazenamento Netapp
- No mínimo 3 anos de experiência com sistemas operacionais Linux e Windows
- Experiência em auditoria de sistemas de infraestrutura e/ou diagnósticos relacionados à segurança de redes;
- Conhecimentos ou experiência no modelo ITIL;
- Design de ambientes Críticos sob a manutenção da integridade, confidencialidade e Disponibilidade dos sistemas envolvidos;
- Implementação de serviços de rede voltados ao atendimento em Alta Performance;
- Profundos conhecimentos em um solução de correlacionamento de eventos e incidentes (SIEM);
- Certificação em:
    - BigIP (F5);
    - Firewall Checkpoint;
    - IPS SourceFire;

9. Vigência do Contrato

12 (doze) meses a partir da assinatura do contrato

10. Local de Trabalho

REGIÃO: Centro-Oeste
UF: DF
MUNICÍPIO: Brasília

Não serão reembolsadas as despesas referentes ao deslocamento dos profissionais até o local de trabalho, exceto se sobrevier a necessidade dos consultores prestarem serviços em outro local que não o acima especificado.

11. Número de Vagas: 1 (uma) vaga

Local/Data,

Nome responsável área contratante
cargo