ADC/7842/2018
Termo de Referência

Objetivo:
Qualificação e contratação de fornecedores de análise de segurança da informação para atendimento de Ordens de Serviço

Rede Nacional de Ensino e Pesquisa – RNP
Segurança da Informação Corporativa
Março/2018

1. INTRODUÇÃO

A Rede Nacional de Ensino e Pesquisa (RNP) é uma instituição privada, sem fins lucrativos, com sede no Rio de Janeiro (RJ), qualificada pelo Governo Federal como Organização Social e contratada pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) para atender aos seguintes objetivos estratégicos:

1) Promover o desenvolvimento tecnológico de novos protocolos, serviços e aplicações de redes;

2) Prover serviços de infraestrutura de redes IP (Protocolo Internet) avançadas para atividades de pesquisa e desenvolvimento científico e tecnológico, educação e cultura;

3) Promover a disseminação de tecnologias, através da implantação, em nível de produção de novos protocolos, serviços e aplicações de redes, da capacitação de recursos humanos e da difusão de informações;

4) Planejar e empreender projetos de tecnologia de informação e comunicação para o desenvolvimento e uso de aplicações e serviços inovadores.

A RNP promove o interesse público pelo desenvolvimento tecnológico da área de redes e suas respectivas aplicações, com o foco orientado para o suporte às ações estratégicas em educação, ciência, tecnologia e inovação, através de Programa Interministerial dos Ministérios da Ciência e Tecnologia e da Educação.

Para tanto, constitui-se como a infraestrutura de rede de comunicação e computação que garante o suporte à pesquisa brasileira, uma vez que propicia a integração de todo o sistema de pesquisa e ensino superior por uma rede nacional de alta capacidade, rica em serviços e aplicações. Nesta rede (ou *backbone*), também são realizadas pesquisas para o desenvolvimento e o teste de novas tecnologias de informação e comunicação (TIC). Estas tecnologias formam a base da nova

Sociedade do Conhecimento, e seu domínio e uso são essenciais para o desenvolvimento do país. Neste sentido, a própria rede constitui-se em um laboratório nacional onde os experimentos de TIC são realizados, de modo que seus resultados possam beneficiar mais rapidamente nossos clientes: as universidades, os centros de pesquisa e as agências federais.

2. ESCOPO

Esta Solicitação de Proposta versa sobre os processos de Qualificação e Contratação de Fornecedores para abertura de Ordens de Serviço (O.S.), de forma a esclarecer tais processos a todas as partes interessadas.

As Ordens de Serviço poderão contemplar atividades para identificação de vulnerabilidades e seus riscos associados, como por exemplo:

- Identificação dos controles existentes e sua suficiência para prevenir incidentes;
- Levantamento de informações sobre o ambiente, utilizando técnicas como (não restritas a):
  - Varredura de portas e *fingerprinting*
  - Clonagem (*mirroring*) de sites
  - Reconhecimento através de sites de busca
  - Análise de mensagens de erro
- Análise de vulnerabilidades baseada no modelo “gray box” (iniciando com “black box” e em seguida “white box”;
- Análise de todas as portas TCP/UDP;
- Análise de infraestrutura (sistema operacional e serviços);
- Análise de aplicação e bancos de dados, verificando a robustez contra fraudes e revelação de informações sigilosas, através de testes de (não restritas a):
  - Configuração;
  - Autenticação e autorização;
  - Gerenciamento de sessão;
  - Validação de dados;

  - Aumento de privilégios;
  - Teste de invasão (pentest);
- Realização de testes baseados nas versões mais recentes da OWASP, OSSTMM e ISSAF;
- Eliminação de falsos positivos;
- Elaboração da planilha técnica de riscos (padrão RNP), conforme apresentado no Anexo A.;
- Elaboração do plano de ação (padrão RNP), conforme apresentado no Anexo B;
- Elaboração de relatório técnico com as atividades realizadas e, minimamente, as seguintes informações:
  - Ativos afetados;
  - Descrição da vulnerabilidade, possíveis danos e ameaças;
  - Método ou forma de detecção;
  - Referência da vulnerabilidade;
  - Criticidade de vulnerabilidade, de acordo com o CVSS;
  - Evidência do problema encontrado;
  - Recomendações de possíveis soluções para mitigar a vulnerabilidade;
  - Data e hora da identificação da vulnerabilidade (fuso América/São Paulo).
- Elaboração de relatório gerencial, contendo minimamente as seguintes informações:
  - Percentual de vulnerabilidades por criticidade;
  - Percentual de vulnerabilidades por ativo;
- Validação da correção das vulnerabilidades pela RNP após a realização da análise de segurança.

Todas as análises e testes deverão ser realizadas na janela de tempo definida pela RNP para este fim.

Caso o fornecedor não tenha interesse em alguma Ordem de Serviço (por exemplo: devido à tecnologia a ser utilizada), poderá declinar ao convite através de justificativa formal.

2.1 QUALIFICAÇÃO DE FORNECEDORES

A RNP deseja selecionar 3 (três) fornecedores para atenderem as demandas de análise de segurança da RNP durante o período de 12 (doze) meses prorrogáveis por iguais períodos mediante termo aditivo. A qualificação técnica, seguirá os critérios de pontuação definidos no quadro abaixo:

Descrição	Pontuação	Como comprovar
Empresa certificada ISO 27001	5 (cinco) pontos para escopo certificado associado ao serviço a ser prestado. 3 (três) pontos para outro escopo. OBS: pontuação não cumulativa	Enviar cópia do documento oficial emitido por entidade competente constando a certificação
Realização de uma PoC de identificação de vulnerabilidades em um sistema da RNP.	3 (três) pontos por vulnerabilidade com CVSS acima de 8 no sistema da RNP 1 (um) ponto por vulnerabilidade identificada no sistema da RNP Limite de 5 vulnerabilidades por PoC. Bônus de 5 pontos para vulnerabilidade crítica (CVSS >= 8) identificada apenas pela empresa (exclusivamente).	Enviar vulnerabilidades no modelo de relatório técnico da empresa.
Apresentação de atestado de prestação de serviço para instituições financeiras.	2 (dois) pontos por atestado, até o máximo de 6 (seis) pontos	Enviar cópia do atestado
Apresentação de atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o nível de experiência e o bom desempenho da empresa na prestação de teste de invasão e análise de vulnerabilidades de segurança	2 (dois) pontos por atestado, até o máximo de 10 (dez) pontos	Enviar cópia do atestado de capacidade técnica

Apresentação de atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o nível de experiência e o bom desempenho da empresa na prestação de serviço de forense computacional.	2 (dois) pontos por atestado, até o máximo de 6 (seis) pontos	Enviar cópia do atestado de capacidade técnica
Apresentação de atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o nível de experiência e o bom desempenho da empresa na prestação de serviços de consultoria para implementação de *hardening* de segurança.	2 (dois) pontos por atestado, até o máximo de 6 (seis) pontos	Enviar cópia do atestado de capacidade técnica
Apresentar exemplos de relatórios técnicos e gerenciais produzidos (com dados sanitizados)	2 (dois) pontos por atestado, até o máximo de 6 (seis) pontos	Enviar relatórios
Apresentar evidências da realização de testes anteriores baseados na OWASP	2 (dois) pontos por relatório, até o máximo de 4 (quatro) pontos	Enviar relatórios
Apresentar evidências da realização de testes anteriores baseados na OSSTMM	2 (dois) pontos por relatório, até o máximo de 4 (quatro) pontos	Enviar relatórios
Apresentação de profissional com perfil de analista de segurança ou pentester certificado através do EC-Council Certified Ethical Hacker (CEH)	4 (três) pontos por profissional, até o máximo de 12 (doze) pontos	Enviar cópia do certificado de conclusão do treinamento e cerificação, e comprovante de que o profissional trabalha ou presta serviços para a empresa.
Apresentação de profissional com perfil de analista de segurança ou pentester certificado GIAC Penetration Tester (GPEN)	4 (três) pontos por profissional, até o máximo de 12 (doze) pontos	Enviar cópia do certificado de conclusão do treinamento e cerificação, e comprovante de que o profissional trabalha ou presta serviços para a empresa.
Apresentação de profissional com perfil de analista de segurança ou pentester certificado Certified Information Systems Security Professional (CISSP)	3 (três) pontos por profissional, até o máximo de 9 (nove) pontos	Enviar cópia do certificado de conclusão do treinamento e cerificação, e comprovante de que o profissional trabalha ou presta serviços para a empresa.

Apresentação de profissional com perfil de analista de segurança ou pentester certificado Offensive Security Certified Professional (OCSP)	4 (três) pontos por profissional, até o máximo de 12 (doze) pontos	Enviar cópia do certificado de conclusão do treinamento e cerificação, e comprovante de que o profissional trabalha ou presta serviços para a empresa.
Apresentação de profissional certificado em Linux com a LPIC-1	1 (um) ponto por profissional, até o máximo de 3 (três) pontos	Enviar cópia do certificado LPIC-1 (LPI 101 e 102) e comprovante de que o profissional trabalha ou presta serviços para a empresa.
Apresentação de profissional certificado em Linux com a LPIC-2	3 (três) pontos por profissional, até o máximo de 6 (seis) pontos (não cumulativos se o profissional tiver a LPIC-1)	Enviar cópia do certificado LPIC-2 (LPI 201 e 202) e comprovante de que o profissional trabalha ou presta serviços para a empresa.
Apresentação de profissional certificado em Linux com a LPIC-3	5 (cinco) pontos por profissional, até o máximo de 10 (dez) pontos (não cumulativos se o profissional tiver a LPIC-1 ou LPIC-2)	Enviar cópia do certificado LPIC-3 (LPI 301 e 302) e comprovante de que o profissional trabalha ou presta serviços para a empresa.

Estará automaticamente desclassificado o fornecedor que obtiver pontuação inferior a 50 pontos.

Vale ressaltar que, a não pontuação em um dos critérios acima não elimina o fornecedor, pois o objetivo do processo é classificatório e não eliminatório.

Os fornecedores deverão enviar proposta técnica contemplando a pontuação que atingem. Tal pontuação será verificada através dos comprovantes enviados pelos fornecedores e a RNP reserva o direito de verificar através dos meios legais e/ou públicos a veracidade de cada informação apresentada. Caso seja comprovado que algum documento é inválido ou falsificado, o fornecedor estará automaticamente eliminado do processo seletivo ou do contrato de prestação de serviços para a RNP.

Os fornecedores também deverão enviar uma proposta comercial, contemplando o valor de cada hora de trabalho a ser praticada durante a vigência do contrato. Solicitamos que o valor seja discriminado de acordo com o tamanho (em termos de horas de trabalho) das futuras Ordens de Serviço, conforme tabela abaixo:

Tamanho da O.S.	**Valor/hora (R$)**
Até 40 horas	
Entre 40 e 80 horas	
Acima de 80 horas	

Após a qualificação dos 3 (três) fornecedores com melhores pontuações, será estabelecido um contrato de prestação de serviços e a RNP poderá enviar a qualquer tempo as Ordens de Serviço.

2.2 ABERTURA DE ORDENS DE SERVIÇO

As demandas de análise de segurança que fazem parte do escopo desta Solicitação de Proposta serão tratadas através de Ordens de Serviço, a serem enviadas aos 3 (três) fornecedores selecionados na etapa anterior.

As respostas às Ordens de Serviço deverão ser propostas técnica e comercial, com escopo fechado, detalhando a solução técnica a ser implementada, a quantidade de horas a serem consumidas, um cronograma de execução, a data de entrega da demanda e o cronograma físico-financeiro (os marcos de entregas alinhados aos faturamentos). Outros entregáveis serão definidos em cada Ordem de Serviço, de acordo com a demanda.

Cada proposta recebida pela RNP como retorno das Ordens de Serviço serão avaliadas da seguinte forma:

1. Será calculado o Índice de Preço (IP), de acordo com a faixa de horas (tamanho da O.S.). A fórmula utilizada será:

$$\text{Índice de Preço (IP)} = \frac{\text{Menor preço proposto}}{\text{Preço do fornecedor}}$$

Onde:

- Menor preço proposto: Será utilizado o menor preço entre as propostas recebidas para a Ordem de Serviço.

- Preço do fornecedor: Será utilizado o preço da proposta de cada fornecedor.

2. Será calcula do Índice do Prazo de Entrega (IPE), considerando a quantidade de dias da data de abertura da O.S. até a data final de entrega da demanda informada pelos fornecedores. A fórmula utilizada será:

$$\text{Índice do Prazo de Entrega (IPE)} = \frac{\text{Menor tempo para entrega}}{\text{Tempo do fornecedor}}$$

Onde:

- Menor tempo para entrega: Será utilizada a menor quantidade de dias para entrega da O.S. entre as propostas recebidas.
- Tempo do fornecedor: Será utilizada a quantidade de dias para entrega de cada fornecedor.

Dessa forma, cada fornecedor receberá um IP e IPE, que será utilizado para determinar o fornecedor vencedor da Ordem de Serviço, considerando aquele que obtiver maior pontuação no resultado. Por padrão a RNP utilizará peso 5 (cinco) para os dois índices, se fazendo do direito de alterar os pesos dos índices por ordem de serviço, divulgando a alteração na abertura da O.S.. O cálculo do resultado será realizado através da seguinte fórmula:

$$\text{Resultado do Fornecedor} = (IP*5) + (IPE*5)$$

Por exemplo:

- Cálculo do Índice de Preço (IP):

	Empresa A	**Empresa B**	**Empresa C**
Menor preço proposto (R$)	7	7	7
Preço da empresa (R$)	8	7	10
Índice de Preço (IP)	0,875	**1,000**	0,700

- Cálculo do Índice do Prazo de Entrega (IPE):

	Empresa A	**Empresa B**	**Empresa C**

Menor tempo para entrega (dias)	30	30	30
Tempo do fornecedor (dias)	30	45	35
Índice do Prazo de Entrega (IPE)	**1,000**	0,667	0,857

- Resultado:

	Empresa A	Empresa B	Empresa C
Resultado: (IP*5) + (IPE*5)	**9,375**	8,333	7,786

Neste exemplo a “Empresa A” venceu a Ordem de Serviço, pois obteve o maior valor no item ‘Resultado’ e, dessa forma, executará a demanda para a RNP.

OBS: Em caso de empate no resultado, o fornecedor com melhor pontuação técnica (definida na qualificação) será declarado o vencedor da Ordem de Serviço.

2.3 SLA – NIVEL DE SERVIÇO

O SLA será encaminhado juntamente com a Ordem de Serviço, pois dependerá do tipo de análise a ser contratado. Caso o fornecedor não tenha condições de atender o SLA apresentado, poderá declinar da OS através de justificativa formal.

3. CONSIDERAÇÕES GERAIS

- Cada Ordem de Serviço terá seu faturamento isolado;
- O faturamento da O. S. será realizado após o aceite formal da RNP, onde será avaliado o escopo solicitado e a qualidade da entrega;
- Quando uma O.S. contemplar trabalho para mais de um mês, o fornecedor deverá apresentar um cronograma físico-financeiro atrelando o faturamento às entregas respeitando o limite máximo de uma Nota Fiscal e respectivo pagamento por mês.

- O faturamento deverá ter vencimento de 20 dias após o aceite formal da RNP.

Resultado da análise técnica | Levantamento de vulnerabilidades

Sistema: XXXX

#ID	Ativo	Localização	Vulnerabilidade	Descrição	Como a vulnerabilidade foi encontrada?	Recomendação	Referência	Observações	Requis.					
	Onde existe a vulnerabilidade: Ex. Servidor web	Onde está a vulnerabilidade: Ex. www.rnp.br / IP	Nome da vulnerabilidade Ex.Permissão de root	Detalhes da vulnerabilidade	Ex. Nexpose, teste no servidor, checklist xyz, comando x	Como fazer para resolver a vulnerabilidade	Referência para recomendação Ex.Site do fabricante	-	CVS	Impacto	Probabilidade - calc	Probabilidade	Risco - calc	Risco

Requisitos de segurança:
C - Confidencialidade
I - Integridade
D - Disponibilidade

Escala para preenchimento:
3 - Afeta muito
2 - Afeta parcialmente
1 - Afeta pouco

Plano de ação
Análise de segurança - Sistema: xxxxx

Informações adicionais para preenchimento do campo Tratamento dos Riscos	
Reter	Na impossibilidade de implementar ações para corrigir a vulnerabilidade, o risco deve ser ***Aceito formalmente*** pelo responsável do ativo
Modificar	Ações implementadas que diminuem o nível de risco
Evitar	Atividade ou condição que da origem a um determinado risco seja evitado. Eliminação de uma atividade planejada

ID	Ativo	Localização	Vulnerabilidade	Descrição da Vulnerabilidade	Ação	Referência	Observações	Nível	Tratamento dos Riscos	Justificativa para riscos retidos	Responsável	Dt. Início	Dt. Término	Status	Observações Cliente	Observações Técnicas - Validação