

Objeto: CONTRATAÇÃO DE CONSULTORIA ESPECIALIZADA PARA REALIZAÇÃO DE “DIAGNÓSTICO DE ESTRATÉGIA DE CIBERSEGURANÇA”, A PARTIR DA AVALIAÇÃO DA INFRAESTRUTURA, CONTROLES E PROCESSOS DE SEGURANÇA DA INFORMAÇÃO DA PRODEMGE (GESTÃO DE SEGURANÇA E SEGURANÇA CIBERNÉTICA).

Solicitação enviada no dia 11/06/2024 às 16:40 enviada pela licitante YSSY Soluções S.A.

Questionamentos

ANEXO I - Termo de Referência

Analisar a maturidade da segurança cibernética do ambiente on-premise da PRODEMGE, com o objetivo de identificar lacunas ou oportunidades de melhoria (incremento de maturidade), com foco nos controles de:

QUESTÃO 1: Qual é o tamanho do ambiente On premises?

Segurança de rede: avaliação das melhores práticas de segurança cibernética do framework NIST-CSF para a segurança de rede, sua arquitetura, tecnologias utilizadas, segmentação, controle de acesso à rede e seus recursos, filtro de conteúdo e proteção da informação em trânsito;

Resposta Técnica: A PRODEMGE é a Companhia de Tecnologia da Informação do Estado de Minas Gerais. É responsável por manter e administrar os mais diversos tipos de aplicações dos órgãos e organizações relacionados ao Governo do Estado de MG. De acordo com seu sistema de CMDB, a Companhia atualmente conta com 665 aplicações ativas e por volta de 3.500 servidores (entre físicos e virtuais) além de diversos ativos de rede e de segurança sob a sua responsabilidade. Por se tratar de informação estratégica e de negócio da Companhia, esse detalhamento não poderá ser divulgado neste momento. Tais informações somente serão fornecidas a empresa vencedora da licitação.

QUESTÃO 2: Qual é a arquitetura do sistema? É possível disponibilizar a topologia de rede e segurança? Detalhamento do parque tecnológico que faz parte do escopo de serviço.

Segurança de dados: avaliação das melhores práticas de segurança cibernética do framework NIST-CSF para a segurança da informação avaliando a proteção dos dados em repouso, ciclo de vida da informação, proteções criptográficas, gestão de identidades, de acesso e de auditoria.

Resposta Técnica: A PRODEMGE conta com diversas aplicações com arquiteturas específicas bem como diversos ativos de rede e segurança em sua infraestrutura. Por se tratar de informação estratégica e de negócio da Companhia, as informações não poderão ser divulgadas neste momento. O detalhamento dessas somente será fornecido a empresa vencedora da licitação.

QUESTÃO 3: Quais são as soluções atuais utilizadas pela Prodemge no que tange a segurança de dados?

ANEXO I - Termo de Referência 26.03.

No ato da assinatura do contrato, a CONTRATADA deverá apresentar a relação dos profissionais certificados que serão os responsáveis por realizarem os serviços de Diagnóstico e Avaliação de Maturidade em Segurança da Informação. Será aceita, no mínimo, as seguintes certificações ou equivalentes: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Implementer e CCISO: Certified Chief Information Security Officer.

Resposta Técnica: Por se tratar de informação estratégica e de negócio da Companhia, as informações detalhadas relacionadas a segurança dos dados administrados, mantidos e hospedados pela PRODEMGE somente serão fornecidas a empresa vencedora da licitação.

QUESTÃO 4: Devem ser todas ou no mínimo uma destas certificações?

Resposta Técnica: Não. Conforme item 26.03 do Termo de Referência anexo ao Edital, serão aceitas no mínimo, as seguintes certificações ou equivalentes: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Implementer e CCISO: Certified Chief Information Security Officer. Ou seja, pelo menos uma delas deve constar no rol de certificações da equipe que executará as atividades pretendidas.

QUESTÃO 5: Existe um mínimo de profissionais que prestarão o serviço ?

Resposta Técnica: Não existe a obrigatoriedade de dedicação exclusiva a projeto. Porém, conforme item 4.2.5 do Termo de Referência anexo ao Edital, é importante esclarecer que a CONTRATADA terá 100 (cem) dias corridos, a partir da reunião inicial de planejamento, para realização dos serviços de análise e mapeamento que subsidiarão a construção do Diagnóstico e dos demais entregáveis pretendidos. A CONTRATADA é quem o número de profissionais e sua forma de trabalho, logo a mesma deve se organizar para que as atividades sejam executadas estejam dentro do prazo determinado.

QUESTÃO 6: Os profissionais devem ter dedicação exclusiva ao projeto ?

Resposta Técnica: Não existe a obrigatoriedade de dedicação exclusiva a projeto. Porém, conforme item 4.2.5 do Termo de Referência anexo ao Edital, é importante esclarecer que a CONTRATADA terá 100 (cem) dias corridos, a partir da reunião inicial de planejamento, para realização dos serviços de análise e mapeamento que subsidiarão a construção do Diagnóstico e dos demais entregáveis pretendidos. A CONTRATADA é quem define sua forma de trabalho, logo a mesma deve se organizar para que as atividades sejam executadas estejam dentro do prazo determinado.

QUESTÃO 7: Existe um número mínimo de dias/horas de trabalho presencial ?

Resposta Técnica: Não existe uma definição mínima de dias e/ou horas para o trabalho presencial. Conforme os itens 4.2.4 e 4.2.5 do Termo de Referência anexo ao Edital, a CONTRATADA terá 100 (cem) dias corridos, a partir da reunião inicial de planejamento, para realização dos serviços de análise e mapeamento que subsidiarão a construção do Diagnóstico e dos demais entregáveis pretendidos. Na maior parte do tempo a CONTRATADA poderá realizar suas atividades de forma remota, mas há a necessidade da avaliação dos controles de segurança física da PRODEMGE e essa avaliação só poderá ser realizada de forma presencial. Caso a CONTRATADA identifique que outras atividades de análise e mapeamento também devam ser realizadas de forma presencial, a mesma é quem deve se programar para executá-la dentro desse intervalo de tempo de 100 (cem) dias.

QUESTÃO 8: Existe obrigação de fornecimento de algum tipo de ferramenta para prestação dos serviços ?

Resposta Técnica: Não. Não existe essa obrigação. A CONTRATADA é quem define sua forma de trabalho, desde que cumpra com os objetivos esperados.

QUESTÃO 9: Entendemos que a CONTRATADA realizará entrevista com o time PRODEMGE, e a CONTRATANTE ficará responsável por mostrar quais são os protocolos, configurações, para que a CONTRATADA possa avaliar a maturidade de tal sistema. Esse entendimento está correto?

Resposta Técnica: Sim. O entendimento está correto. A equipe técnica da PRODEMGE será responsável por fornecer a CONTRATADA todas as informações necessárias para montagem do diagnóstico e demais entregáveis.

QUESTÃO 10: Entendemos que a CONTRATADA não irá realizar configurações, implementação ou ajustes nas configurações atuais do ambiente PRODEMGE. Correto?

Resposta Técnica: Sim. O entendimento está correto. Mas, conforme o item 4.1 do Termo de Referência anexo ao Edital, a CONTRATADA deve realizar o diagnóstico de estratégia de cibersegurança considerando a execução de diversas atividades de mapeamento e análise de processos de segurança realizados pela PRODEMGE. Ao final do trabalho, a CONTRATADA deve entregar esse Diagnóstico, bem como planos de ação de curto e médio prazo, a proposição de métricas e indicadores corporativos e um relatório de avaliação de riscos cibernéticos identificados.
