CONSELHO REGIONAL DE ENFERMAGEM DO TOCANTINS

Filiado ao Conselho Internacional de Enfermeiros – Genebra

Processo Administrativo n.º 099/2024

ESTUDOS PRELIMINARES

I - Necessidade da contratação:

1. Informações Básicas

Número do processo COFEN: 00196.004611/2024-62.

2. Descrição da necessidade

Estudo para contratação de Serviços Gerenciados e Integrados de Segurança e Serviços de Conectividade Wireless e local, compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; resposta a incidentes de segurança, transferência de conhecimento para a equipe do Coren e fornecimento de solução de conectividade para rede wireless e local.

Justificativa

Em relação às questões de segurança da informação, é de conhecimento público que diversos órgãos brasileiros são alvos de constantes ameaças, como ataques ao Ministério da Saúde, STF, STJ, TRF 3ª Região, Justiça Federal de SP e MS, etc. Além de instituições financeiras e demais entes privados. Verifica-se ainda que o sistema Cofen/Coren's lida todos os dias com elevada troca de informações, além de um grande e complexo volume de dados sensíveis de milhares de cidadãos. Além disso, em 2020 um novo cenário surgiu em decorrência da Covid-19. Processos de transformação digital das organizações públicas acabou por forçar as organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma, os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente, o que leva à conclusão da necessidade de que as instituições públicas tenham um altíssimo nível de segurança cibernética. Nestes cenário em que há o avanço das ameaças cibernéticas, cada vez mais atuante no meio governamental, as ferramentas de segurança da informação também precisam se tornar cada vez mais diversas e sofisticadas no tratamento dos riscos de ocorrência de invasões da rede, fato que torna relevante a realização de investimentos em soluções de cibersegurança, fato que motiva a realização destes estudos, que visa a identificação de solução de segurança

que possa apoiar o monitoramento da rede e controle de ações internas e identificação de situaçõessuspeitas dentro da rede de computadores do Cofen. Assim, verifica-se que a estratégia da implementação da segurança da informações em camadas, é adequada, uma vez que consiste na disposição de várias etapas de proteção à operacionalidade do Cofen, de modo a blindar seus arquivos e dados mais sensíveis contra ataques cibernéticos desde a camada física de rede até a camada de aplicações, de forma que a metodologia adotada reforça as fronteiras digitais com vários muros de sustentação de forma gradativa. Pelo exposto, resta verificada a preocupação da equipe de tecnologia da informação do Cofen em direcionar os investimentos de forma estratégica, promovendo a elevação gradativa dos níveis de segurança institucional e a maturidade das equipes técnicas de forma a alcançar vários benefícios, tais como:

* Proteção contra malwares, ransomware, wannacry, botnet entre outros;

* Proteção contra vazamentos de dados e phishing;

* Segurança ágil e dinâmica;

* Oferece proteção mais forte, multicamadas;

* Controle de ativos; e

* Gerenciamento centralizados dos recursos de rede e segurança, dentre outros citados em cada projeto.

Além disso, o COREN vivencia uma transformação em sua área de tecnologia da informação, seja atualizando os sistemas legados seja por demanda de novos serviços, com o intuito de ser tornar um órgão com 100% dos seus serviços de forma digital.

Desta forma, é essencial viabilizar a proteção adequada e atualizada do seu ambiente computacional, de modo a preservar os ativos corporativos, garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de programas maléficos que ponham em risco a segurança e a continuidade das atividades. Sendo assim, se faz necessário a contratação de solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; resposta a incidentes de segurança e transferência de conhecimento para a equipe do Coren, tendo como objetivo garantir a segurança e o controle de acesso dos usuários, a rede internet e intranet, permitindo a aplicação de filtros e a identificação de ataques externos e internos. A Solução Integrada de Serviços Gerenciados de conectividade wireless permitirá ao Coren a utilização de novas tecnologias como acesso à internet através de notebooks, tablets e celulares, bem como dar maior comodidade e mobilidade aos usuários da rede do Coren, sendo composta por itens de serviços

contínuos em tecnologia da informação e abrangendo todo o ambiente computacional. Também farão parte do escopo atividades relacionadas à transferência de conhecimento e aos serviços técnicos especializados. A ação visa proteger a rede de ameaças desconhecidas externas, além das internas que podem ocorrer com máquinas infectadas vindo de trabalho híbrido/remoto ou de visitantes.

4. Necessidades de Negócio

* No atual cenário do Coren-TO, em relação a Segurança, temos instalado um firewall opensource que foi implantado e configurado por um técnico que já não faz parte do quadro de funcionários; temos switch, roteadores, access point que não suportam e/ou já não atendem as necessidades do órgão; visto que vamos partir pra uma ampliação de espaço, que atualmente não possuímos equipamentos necessários para atender essa ampliação.

* A Contratação de uma solução integrada irá trazer uma gerência centralizada e única de segurança e conectividade do tipo proprietária, ou seja, ao elaborar esse estudo com a parte de serviços de locação de equipamentos com serviços também prestados pela futura contratada, sem tirar a autonomia do CORENEN em operar a solução, teria uma equipe por traz da solução e não dependeríamos de uma única pessoa, sendo a responsabilidade compartilhada com especialistas nas soluções.

II - Requisitos da contratação:

Conforme ETP COFEN em anexo : SEI_COFEN_-_00433710_-_Estudo_Técnico_Preliminar_(ETP)

III - Estimativa das quantidades, acompanhadas das memórias de cálculo e dos documentos que lhe dão suporte:

LOTE	ITEM	DESCRIÇÃO	QTD
1	3	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	2
	6	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	2
	7	Serviços Técnicos Especializado	Sob demanda
	8	Treinamento da Solução de Serviços Gerenciados de Firewall	1
	9	Serviços de Solução de proteção para Estações	45
	10	Serviços de Solução de proteção para Servidores	1
	11	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações	45

	12	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para servidores	1
	13	Instalação da solução de Segurança de Endpoints, Detecção e Respostas	45
	14	Instalação da solução de Segurança de Servidores	1
	15	Treinamento da Solução de Endpoints	1
	16	Serviços de Conectividade Wireless	4
	17	Instalação da solução de Conectividade Wireless	4
	18	Treinamento da Solução e Conectividade Wireless	1
2	19	Serviços de Conectividade Local	2
	20	Instalação da solução de Conectividade Local	2
	21	Treinamento da Solução de Conectividade Local	1

IV - Estimativas de preços ou preços referenciais:

Conforme ETP COFEN em anexo : SEI_COFEN_-_00433710_-_Estudo_Técnico_Preliminar_(ETP)

V - Descrição da solução como um todo:

SEI_COFEN_-_00433710_-_Estudo_Técnico_Preliminar_(ETP)

VI - Justificativas para o parcelamento ou não da solução quando necessária para individualização do objeto:

Conforme ETP COFEN em anexo : SEI_COFEN_-_00433710_-_Estudo_Técnico_Preliminar_(ETP)

VII - Resultados Pretendidos:

Entre os principais resultados e benefícios a serem obtidos com a implantação da solução a ser contratada, destacam-se:

- Possibilitar o atendimento aos controles e diretrizes previstas na LGPD;
- Mitigação de riscos de segurança da informação associados à exposição, perdas, violações e/ou vazamentos de dados intencionais ou não por usuários do Coren;
- Diminuição de falsos positivos e negativos;
- Diminuição do tratamento manual de incidentes;
- Aumentar a taxa de automatização de detecção e respostas Melhoria da qualidade dos serviços de TIC prestados pelo Coren à sociedade, com adoção das melhores práticas de mercado relativas à segurança da informação e comunicação;
- Prevenir a ocorrência de incidentes cibernéticos que podem causar impactos à imagem e reputação do Coren, inclusive o que dispõe a Lei de Proteção de Dados Pessoais;
- Ampliar o índice de confiabilidade dos usuários em relação aos serviços prestados pela área de TIC do Coren, tendo em vista a garantia de segurança destes serviços com a implantação da solução;
- Mitigar internamente os riscos de falhas na segurança dos dados institucionais, bem como identificar, investigar e tratar ocorrências, tendo em vista que a perda, roubo e/ou vazamento de dados do Órgão podem propiciar inúmeros inconvenientes e prejuízos financeiros tanto ao próprio Coren quanto aos usuários de seus sistemas

1. Membros da Equipe de Planejamento da Contratação:

Nome: José Emerson A da Silva
Integrante Demandante