Estudo Técnico Preliminar 6/2024

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

Trata-se de contratação de empresa especializada em cursos para capacitação de 2 (dois) membros da equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS).

ITEM DESCRIÇÃO/ESPECIFICAÇÃO VAGAS

ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	Inscrições
1	Curso Foundations of Incident Management - FIM	02
2	Curso Advanced Topics in Incident Handling - ATIH	02

Serão contratados dois cursos para atender a necessidade de capacitação da equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS), conforme especificados abaixo:

O Curso Foundations of Incident Management tem previsão de realização nos períodos de 15 a 19 de abril de 2024 e o Curso Advanced Topics in Incident Handling no período de 23 a 27 de setembro de 2024.

O setor requisitante justifica a necessidade no Documento de Formalização da Demanda 14895634 nos seguintes termos:

com o advento do Plano Diretor de Tecnologia da Informação 2023-2025 do INSS aprovado pela **RESOLUÇÃO Nº 27 /CEGOV/INSS, DE 28 DE DEZEMBRO DE 2022** e a instituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS, conforme a RESOLUÇÃO Nº 11/CEGOV/INSS, DE 31 DE AGOSTO DE 2020 o INSS alçou um marco significativo na prevenção e combate a fraudes e incidentes cibernéticos em suas operações.

É de amplo conhecimento que o INSS tem dedicado recursos substanciais à intensificação da segurança da informação, à modernização do parque tecnológico e à implementação e fortalecimento de políticas de segurança, com vistas a garantir um ambiente de maior qualidade e seguro para todos os seus colaboradores e usuários, tanto interno quanto externos.

A Equipe de Prevenção, Tratamento e Resposta a Incidentes obteve resultados em sua atuação, conforme evidenciado a seguir:

Período	Quantidade
2019	**17**

2020	**95**
2021	**168**
2022	**421**
2023	**308**
2024	**25**

A partir do ano de 2022, constatou-se a inserção de um número considerável de dispositivos clandestinos na infraestrutura de rede do INSS, viabilizado a realização de fraudes que perfazem dezenas de milhões de reais, causando um grande prejuízo ao erário. Sendo, contabilizado aproximadamente **entre os anos de 2022 e 2023, 76 (setenta e seis) dispositivos clandestinos**.

Diante do cenário contemporâneo, notadamente caracterizado pelo acréscimo constante na complexidade e na quantidade de ameaças cibernéticas, torna-se premente o reforço das competências da Equipe de Segurança da Informação.

Esta iniciativa reveste-se de importância estratégica para o desenvolvimento de habilidades essenciais na gestão e resposta a incidentes de segurança da informação, tornando mais eficaz e eficiente no tratamento de incidentes e respostas.

O Decreto nº 10.222, de 2020, enfatiza a importância das políticas e diretrizes para a segurança da informação na administração pública federal. Destaca a necessidade de capacitação contínua dos colaboradores em práticas de segurança da informação. Além disso, ressalta a relevância da formação de uma equipe de resposta a incidentes cibernéticos bem capacitada, alinhada com os padrões internacionais e as melhores práticas recomendadas por entidades de referência como o Gartner. Vejamos:

(...)"É de amplo conhecimento que toda organização, pública ou privada, deve possuir uma equipe de tratamento e resposta aos incidentes cibernéticos - ETIR, também conhecida pela sigla - CSIRT, de Computer Security Incident Response Team. Essa equipe deve ser capacitada, e deve dispor de ferramentas computacionais adequadas às suas necessidades, e de sistemas baseados em tecnologias emergentes, condizentes com os padrões internacionais. Atualmente, o Brasil possui oito tipos de centros de tratamento e resposta aos incidentes cibernéticos, de acordo com sua atuação:

- Centros de Responsabilidade Nacional - CERT.br e CTIR Gov.

- Centros de Coordenação Internacional - CERT/Coordination Center, FedCirc e FIRST.

- CSIRTs de Infraestruturas Críticas - Energia - CSIRTCemig - Financeiro - CSIRTs do BB, da Caixa, do BASA, do BNB, do BRB e do BANESE - Telecom - CTIR/DATAPREV, GRA/SERPRO e CSIRT PRODESP.

- CSIRTs de Provedores - CSIRT Locaweb e CSIRT HP.

- CSIRTs Corporativos - CERT-RS, SEGTIC UFRJ e CSIRT Unicamp.

- CSIRTs Acadêmicos - CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS/UFRN e TRI/UFRGS.

- CSIRTs do Poder Público - Executivo - CTIR Gov, Legislativo - GRIS-CD e Judiciário - GATI, CLRI e TRF-3.

- CSIRTs Militares - Marinha - CTIM, Exército - CCTIR/EB e Aeronáutica - CTIR.FAB.

Esses centros atuam em constante comunicação, e mantêm registros de incidentes nacionais, para avaliação de dados estatísticos referentes às ameaças e a esses incidentes. Os atuais esforços concentram-se em simplificar o compartilhamento de informações entre todos os CSIRTs, uma vez que o número de atores do Governo e do setor privado vem se ampliando, ao lado dos crescentes desafios no campo cibernético..."

https://www.planalto.gov.br/ccivil_03/_ato20192022/2020/decreto/d10222.htm

As diretrizes apresentadas pelo GARTNER para as esferas de segurança da informação e desenvolvimento das equipes abrangem os temas, a seguir:

Desenvolvimento de Competências Específicas: A capacitação deve abranger competências específicas, tanto técnicas quanto gerenciais, para uma cobertura ampla das necessidades organizacionais em segurança cibernética.

Aprendizado Contínuo e Adaptativo: É crucial adotar uma abordagem de aprendizado contínuo, adaptando-se às rápidas mudanças no cenário de ameaças, para manter as equipes sempre atualizadas

Simulações e Treinamentos Práticos: A realização de simulações e exercícios práticos, como testes de penetração e jogos de guerra cibernéticos, é essencial para aprimorar a capacidade de resposta das equipes a incidentes reais.

Foco em Habilidades Interdisciplinares: O desenvolvimento de habilidades interdisciplinares, combinando TI, gestão de riscos, análise de negócios e comunicação, é fundamental para uma abordagem integrada à segurança cibernética.

[...]

Objetivos Esperados:

Aprimorar e elevar o nível de eficácia e eficiência da equipe DTI;

Refinar os procedimentos, análises e respostas a diversos cenários de incidentes, proporcionando embasamento para investigações e atendendo às demandas dos diversos órgãos internos, externos e de controle;

Desenvolver o reconhecimento e a gestão de abordagens de reação diante de variados tipos de ocorrências em segurança da informação;

Identificar aprimoramentos nos procedimentos de bloqueio e desbloqueio de credenciais, uma vez que exerce grandes impactos diretamente nas filas de análise de reconhecimento inicial de direitos, conforme estabelecido no Planejamento Estratégico de TIC para 2024.

Conclui-se, que ao efetuar a seleção de um curso, torna-se relevante ponderar sobre a reputação da Instituição, a pertinência e importância do conteúdo em relação às necessidades específicas.

A capacitação solicitada, alinhada às diretrizes do GARTNER e às demandas específicas do INSS, desempenham uma função primordial em assegurar a integridade, confiabilidade das informações gerenciais. Isso contribui de maneira substancial para salvaguarda dos cidadãos brasileiros e para a resiliência das infraestruturas críticas nacionais.

As informações coletadas têm como objetivo subsidiar e impulsionar investigações realizadas pela Polícia Federal, buscando a identificação dos integrantes de quadrilhas especializadas em fraudes previdenciárias.

A Coordenação Geral de Tecnologia da Informação e Segurança - CGTIS, considera impreterível que o Instituto Nacional do Seguro Social realize os investimentos necessários para aprimorar e fortalecer a segurança dos dados e informações que estão sob sua custódia.

[...]

Os servidores da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética do Instituto Nacional do Seguro Social - ETIR-INSS passam por um abrangente processo de treinamento e educação especializados. O ciclo de capacitação técnica e operação previamente mencionado constitui apenas uma parcela desse programa integral. Este ciclo, dedicado à capacitação técnica e operacional, faz parte de uma série mais ampla de fases de treinamento necessários para as equipes responsáveis pela detecção, tratamento e resposta a incidentes de segurança cibernética.

A ação de desenvolvimento em tela visa a capacitação de 2 (dois) servidores membros da equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS), para aprimorar e elevar o nível de eficácia e eficiência da equipe DTI no INSS.

Assim, busca-se preparar servidores da ETIR-INSS de forma gradual, considerando as experiências profissionais e cargos ocupados, para atuarem na identificação de incidentes cibernéticos darem soluções concretas, ante ao atual cenário de ameaças e vulnerabilidades relacionados ao vazamento de credenciais com causas desconhecidas e comprovadamente complexas.

As necessidades das contratações justificam-se, portanto, em virtude da pertinência temática das capacitações com as atribuições exigidas e esperadas dos servidores, membros da ETIR-INSS. Em consonância com Plano de Desenvolvimento de Pessoas - PDP -2024 do Instituto Nacional do Seguro Social.

3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Infraestrutura e Operações	Israel Eduardo Zebulon Martins de Souza

4. Descrição dos Requisitos da Contratação

Trata-se de solicitação de contratação de empresa especializada para a prestação de serviços de capacitação para servidores membros da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS), com o objetivo de fortalecer, por meio da especialização de seus membros, a capacidade de detecção, tratamento e resposta a incidentes cibernéticos no INSS.

O objetivo principal desta contratação esta pautada nas necessidades e a correta e imediata identificação das ameaças de incidentes cibernéticos, na busca de minimizar a vulnerabilidade ainda existente, face ainda limitada gestão de tecnológica, de limitado quantitativo de times especializados de segurança da informação e comunicações e de urgência na continuidade de otimização de segurança e inteligência enfrentados pelo INSS, o que impacta, dentre outros processos, a imagem e a consecução da Missão do Instituto.

A execução dos serviços desta contratação, visa o uso dos conhecimentos das boas práticas internacionais de gerenciamento de incidentes cibernéticos esperados por equipes de SOC (*Security Operations Center*), de CSIRT (*Computer Security Incident Response Team*) e de CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança), com a capacitação de amplo alcance no Instituto, visando abarcar todos os servidores que lidam com o tema.

Ante o exposto, é de substancial necessidade de que os servidores que atuam na ETIR-INSS, estejam abastecidos de amplo conhecimento, no sentido de maximizar suas ações em prevenção e respostas as ameaças de incidentes, que possam acorrer aos sistema de informações e comunicação do Instituto.

A contratação desses cursos oportunizará aos servidores (a) lotados nas áreas de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS) uma relevante melhoria no tocante as competências operacionais necessárias ao desenvolvimentos de suas atividades.

A importância dessas ações de desenvolvimento foi reconhecida internamente e na própria Política Nacional de Desenvolvimento de Pessoal – PNDP.
O PNDP, instituído pelo Decreto 9.991/2019, nos artigos 1º e 3º, bem como Instrução Normativa SGP-ENAP/SEDGG/ME Nº 21 de 1º de fevereiro de 2021, prevê que:

> Art. 1º Este Decreto dispõe sobre a Política Nacional de Desenvolvimento de Pessoas - PNDP, com o objetivo de promover o desenvolvimento dos servidores públicos nas competências necessárias à consecução da excelência na atuação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.'
>
> Art. 3º Cada órgão e entidade integrante do SIPEC elaborará anualmente o respectivo PDP, que vigorará no exercício seguinte, a partir do levantamento das necessidades de desenvolvimento relacionadas à consecução dos objetivos institucionais.
>
> INSTRUÇÃO NORMATIVA SGP-ENAP/SEDGG/ME Nº 21, DE 1º DE FEVEREIRO DE 2021
>
> Estabelece orientações aos órgãos do Sistema de Pessoal Civil da Administração Pública Federal - SIPEC, quanto aos prazos, condições, critérios e procedimentos para a implementação da Política Nacional de Desenvolvimento de Pessoas - PNDP de que trata o Decreto nº 9.991, de 28 de agosto de 2019.
>
> Art. 2º Para os fins desta Instrução Normativa, considera-se:

> II - ação de desenvolvimento, capacitação ou treinamento regularmente instituído: atividade de aprendizagem estruturada para impulsionar o desempenho competente da atribuição pública em resposta a lacunas de performance ou a oportunidades de melhoria descritas na forma de necessidades de desenvolvimento, realizada em alinhamento aos objetivos organizacionais, por meio do desenvolvimento assertivo de competências;

A contratação atende à necessidade do Plano de Desenvolvimento de Pessoas - PDP/2024, código 239784, que tem como descrição: Entender e aplicar conhecimentos em segurança da informação e dentre os objetivos estratégicos previstos no Mapa Estratégico 2024-2027, nas bases de conhecimento verifica-se o objetivo de promover a segurança da informação.

Além da previsão no PDP/2024, a capacitação encontra-se planejada no Plano de Contratações Anuais - PCA 2024, conforme dados abaixo:

I- ID PCA no PNCP: 29979036000140-0-000006/2024

II- IData de publicação no PNCP: 20/5/2023

III- Id do item no PCA: 8

IV- Classe/Grupo: 929 - OUTROS SERVIÇOS DE EDUCAÇÃO E TREINAMENTO

V- Identificador da Futura Contratação: 512006-90044/2023

5. Levantamento de Mercado

Frente ao levantamento da demanda, existem no mercado algumas soluções em matéria de capacitação para os agentes públicos:

a) cursos abertos - são cursos oferecidos ao público em geral, realizados sempre com datas, conteúdo e material previamente determinados pela empresa.

b) cursos in company - são cursos fechados, cujas datas, conteúdo e material são determinados pelo contratante, realizados dentro da sua própria estrutura, com professores em contato direto com os participantes.

c) cursos online - são cursos que podem ser contratados de modo fechado ou aberto ao público em geral, com conteúdo e material previamente determinados pela empresa.

A solução indicada para esta capacitação é a participação dos servidores em curso aberto, tendo em vista tratar-se de tema bastante específico e técnico e cujo número de participantes não configura-se suficiente para justificar a formação de uma turma fechada.

A escolha destes cursos está relacionada a necessidade de:

a) garantir a adequada detecção de eventos e seu adequado tratamento, desde a categorização destes como incidentes de segurança da informação ou não;

b) garantir que incidentes de segurança da informação sejam identificados, avaliados e respondidos adequadamente;

c) mitigar, aceitar, transferir ou eliminar tempestivamente riscos negativos (ameaças contra o INSS) relacionados a incidentes de segurança da informação, além de melhorar, aceitar, compartilhar e explorar os riscos positivos (oportunidades de geração e compartilhamento de inteligência);

d) reportar as vulnerabilidades de segurança da informação, após seu adequado tratamento e;

e) promover a adequada prevenção de futuras ocorrências, através da manutenção de uma base de lições aprendidas.

Primeiramente, fez-se um estudo em sites da internet por instituições que ofertam esse curso e não localizamos outra instituição que atenda a necessidade em tela.

A escolha pela capacitação pleiteada deve-se pelo fato do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br) ser o único *Software Engineering Institute Partner* (conforme chancela do *Software Engineering Insitute* da *Carnegie Mellon University*) brasileiro e estar licenciado para ministrar oficialmente no Brasil os seguintes cursos do CERT® Division, a saber: *Fundamentals of Incident Handling* (FIH) e *Advanced Topics in Incident Handling* (ATIH).

O *CERT Coordination Center*® (CERT®/CC) foi criado em 1988, sendo o primeiro CSIRT a ser estabelecido no mundo. Com a expansão da Internet e com a sofisticação dos atacantes surgiram novas demandas, que levaram o CERT®/CC a ser apenas um dos componentes do *CERT® Division* e cursos ofertados são destinado ao pessoal técnico de Grupos de Segurança e Resposta a Incidentes (CSIRTs), SOCS e outras áreas relacionadas com atividades de Gestão de Incidentes de Segurança Cibernética.

Os instrutores dos cursos do CERT.br possuem sólida formação em administração e segurança de redes, além de uma ampla experiência na área de tratamento de incidentes de segurança em computadores e foram aprovados e treinados pelo CERT® Division, da Carnegie Mellon® University, para ministrar estes cursos, e detém a credencial *SEI-Authorized CERT Instructor*. Apresentamos o currículo dos instrutores:

Cristine Hoepers, Gerente Geral do CERT.br, é formada em Ciências da Computação pela Universidade Federal de Santa Catarina (UFSC) e Doutora em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE). Possui a credencial *SEI-Authorized CERT Instructor*, que a habilita a ministrar os cursos do CERT® Division licenciados pelo CERT.br. Possui também a certificação *Certified SIM3 Auditor*, que a habilita a auditar o nível de maturidade de CSIRTs de acordo com o Modelo de Maturidade SIM3 (*Security Incident Management Maturity Model*).

Trabalha com Gestão de Incidentes de Segurança no CERT.br desde 1999, onde atualmente se dedica mais à área de Transferência do Conhecimento, em especial Treinamentos e Aconselhamento Técnico e de Políticas. Participou do Conselho Diretor do FIRST e da Coordenação dos Fóruns de Boas Práticas sobre Spam e CSIRTs do Internet Governance Forum (IGF), das Nações Unidas. Em 2020 recebeu do M^3AAWG, maior organização mundial de combate a abusos online, o prêmio anual Mary Litynski, por seu trabalho para aumentar a resiliência da Internet. Foi moderadora e palestrante em eventos nacionais e internacionais, incluindo fóruns da OEA, ONU, ITU, LACNIC, FIRST, APWG e M^3AAWG, abordando os temas de Gestão de Incidentes, Privacidade, Implantação de CSIRTs, Fraudes na Internet, *Spam* e *Honeypots*.

Klaus Steding-Jessen, Gerente Técnico do CERT.br, é formado em Engenharia da Computação pela Universidade Estadual de Campinas (Unicamp) e Doutor em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE). Possui a credencial *SEI-Authorized CERT Instructor*, que o habilita a ministrar os cursos do CERT® Division licenciados pelo CERT.br. Possui também a certificação *Certified SIM3 Auditor*, que o habilita a auditar o nível de maturidade de CSIRTs de acordo com o Modelo de Maturidade SIM3 (*Security Incident Management Maturity Model*).

Atua com tratamento de incidentes no CERT.br desde 1999, e atualmente se dedica às áreas de Consciência Situacional e de Transferência de Conhecimento, em especial Treinamentos. Na área de Consciência Situacional trabalha com o desenvolvimento de ferramentas que permitam, através de honeypots, entender melhor os ataques atuais e correlacionar estes dados com aqueles dos incidentes de segurança reportados ao CERT.br. Tem trabalhado no apoio à implantação de novos CSIRTs no Brasil e tem sido palestrante em diversos eventos, no Brasil e no exterior, sobre os temas de seguranca da informação, boas práticas de operação de redes e prevenção de *spam* e *phishing*.

Assim, considerando a singularidade dos serviços a serrem contratados e a notória especialização da empresa NUCLEO DE INFORMACAO E COORDENACAO DO PONTO BR - NIC .BR, por sua experiência de mercado na contratação dos cursos promovidos por essa empresa com outros órgãos, são caracterizadas pela inviabilidade de competição prevista no art. 74, inciso III, alínea "f" da Lei nº 14.133 de 1º de abril de 2021, e, por isso, deve ser realizada pela forma direta, por inexigibilidade de licitação.

Durante o curso serão incorporadas atividades interativas com discussões em grupo e exercícios práticos para compreensão necessária no tratamento de incidentes; políticas e procedimentos técnicos relacionados aos tipos de ataques comumente reportados; desenvolvimento de habilidades de pensamento crítico na resposta de incidentes, identificando, dessa forma, os potencias problemas a serem evitados durante o trabalho de gestão de incidentes.

Os serviços a serem contratados possuem natureza de “não-continuado” e enquadram-se nos pressupostos do Decreto n° 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades, previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

Destarte, à luz do que atualmente o mercado oferece, é possível identificar as metodologias, tecnologias e qualificações que satisfazem melhor as necessidades do INSS, com foco no atendimento das especificidades que envolvem a capacitação dos profissionais da Instituição, quais sejam: o reconhecimento, notoriedade e qualificação da empresa.

A contratação deve ocorrer com fundamento em inexigibilidade de licitação, com base no art. 74, inciso III, alínea "f" da Lei nº 14.133 de 1º de abril de 2021. Não seria viável cogitar da realização de uma licitação para a contratação de curso aberto com esta especificidade, porque não é possível estabelecer critérios objetivos de escolha, o que torna impossível a realização da licitação e determina a inexigibilidade como fundamento adequado para a contratação.

De forma objetiva, essa entidade atende os requisitos exigidos pela Lei e que devem ser reunidos para a contratação por inexigibilidade com fundamento no dispositivo acima mencionado, quais sejam:

1) O serviço deve ser técnico e especializado

Nesse aspecto, podemos dizer que, conforme expressamente previsto no art. 74, inciso III, alínea "f" da Lei nº 14.133 de 1º de abril de 2021, serviços técnicos especializados de natureza predominantemente intelectual com profissionais ou empresas de notória especialização são assim definidos:

> Art. 74. É inexigível a licitação quando inviável a competição, em especial nos casos de:
>
> [...]
>
> III - contratação dos seguintes serviços técnicos especializados de natureza predominantemente intelectual com profissionais ou empresas de notória especialização, vedada a inexigibilidade para serviços de publicidade e divulgação:
>
> [...]
>
> f) treinamento e aperfeiçoamento de pessoal;

6. Descrição da solução como um todo

Contratação de empresa especializada para a prestação de serviços de capacitação para servidores quanto a capacidade de Detecção, Tratamento e Resposta a Incidentes Cibernéticos no INSS.

Os cursos serão realizados na modalidade presencial na sede NIC.br, São Paulo- SP, conforme folder da empresa especificado nos anexos: 14995108 e 14999598.

O curso destina-se a capacitação de 02 (dois) servidores.

ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	Inscrições
1	Curso Foundations of Incident Management - FIM	02
2	Curso Advanced Topics in Incident Handling - ATIH	02

7. Estimativa das Quantidades a serem Contratadas

A estimativa de contratação será de 2 (dois) cursos, para 2 (dois) servidores com previsão de realização nos meses de abril e setembro de 2024, sendo que o curso Foundations of Incident Management - FIM será realizado no período de 15 a 19 de abril de

2024, com carga horária de 40h e o Curso Advanced Topics in Incident Handling no período de 23 a 27 de setembro de 2024, com carga horária de 40h, ambos na modalidade presencial.

8. Estimativa do Valor da Contratação

Valor (R$): 13.200,00

O preço do serviço decorre da proposta comercial de capacitação apresentada pela CONTRATADA, com investimento previsto de R$ 13.200,00 (treze mil e duzentos reais), conforme propostas em anexo 6690917 e 6690924;

Em pesquisa no portal da transparência localizou-se dados de cursos realizadas, pela CONTRATADA, com outras entidades públicas:

O valor da contratação será de R$ 13.200,00 (treze mil e duzentos reais) e, conforme observado na Pesquisa de preço realizadas pelo Portal da Transparência **(15163343),** o valor do curso está de acordo com o praticado, pelo Núcleo de Informação e Coordenação do Ponto BR, no mercado e em outras contratações com a Administração Pública nos últimos 6 meses, consoante propostas da empresa anexadas nos autos (14995108 e 14999598, observa-se que os valores praticados frente a outros órgãos públicos é o mesmo proposto para o INSS, conforme Pesquisa de preço realizadas, listadas abaixo:

Entidade/Órgão Público	Participantes	Valor (R$)	Ano
MINISTÉRIO DO TRABALHO E EMPREGO – UNIDADES COM VÍNCULO DIRETO	2	3.3OO,OO	2O23
AGENCIA NACIONAL DE AVIAÇÃO CIVIL	2	6.600,00	2O23
MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS	2	6.600,00	2O23

9. Justificativa para o Parcelamento ou não da Solução

A pretensa contratação será realizada com base em critérios de qualificação e notoriedade nos cursos *Fundamentals of Incident Handling* (FIH) e *Advanced Topics in Incident Handling* (ATIH) demonstrado nos autos, critérios esses que inviabiliza a seleção de fornecedores distintos com a mesma qualificação da contratação.

A prestação do serviço será realizada conforme folder apresentado pela empresa e o pagamento poderá ser realizado em parcela única conforme proposta apresentada pela empresa.

10. Contratações Correlatas e/ou Interdependentes

Não há contratação dessa natureza no órgão, não havendo, portanto, sobreposições contratuais.

A contratação em questão não demanda a realização de contratação anterior que viabilize a sua execução.

11. Alinhamento entre a Contratação e o Planejamento

A importância dessas capacitações foi reconhecida internamente e na própria Política Nacional de Desenvolvimento de Pessoal – PNDP.

O PNDP, instituído pelo Decreto 9.991/2019, nos artigos 1º e 3º, bem como Instrução Normativa SGP-ENAP/SEDGG/ME Nº 21 de 1º de fevereiro de 2021, prevê que:

Art. 1º Este Decreto dispõe sobre a Política Nacional de Desenvolvimento de Pessoas - PNDP, com o objetivo de promover o desenvolvimento dos servidores públicos nas competências necessárias à consecução da excelência na atuação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.'

Art. 3º Cada órgão e entidade integrante do SIPEC elaborará anualmente o respectivo PDP, que vigorará no exercício seguinte, a partir do levantamento das necessidades de desenvolvimento relacionadas à consecução dos objetivos institucionais.

INSTRUÇÃO NORMATIVA SGP-ENAP/SEDGG/ME Nº 21, DE 1º DE FEVEREIRO DE 2021

Estabelece orientações aos órgãos do Sistema de Pessoal Civil da Administração Pública Federal - SIPEC, quanto aos prazos, condições, critérios e procedimentos para a implementação da Política Nacional de Desenvolvimento de Pessoas - PNDP de que trata o Decreto nº 9.991, de 28 de agosto de 2019.

Art. 2º Para os fins desta Instrução Normativa, considera-se:

II - ação de desenvolvimento, capacitação ou treinamento regularmente instituído: atividade de aprendizagem estruturada para impulsionar o desempenho competente da atribuição pública em resposta a lacunas de performance ou a oportunidades de melhoria descritas na forma de necessidades de desenvolvimento, realizada em alinhamento aos objetivos organizacionais, por meio do desenvolvimento assertivo de competências;

A contratação atende à necessidade do Plano de Desenvolvimento de Pessoas - PDP/2024, código 239784, que tem como descrição: Entender e aplicar conhecimentos em segurança da informação e dentre os objetivos estratégicos previstos no Mapa Estratégico 2024-2027, nas bases de conhecimento verifica-se o objetivo de promover a segurança da informação.

Além da previsão no PDP/2024, a capacitação encontra-se planejada no Plano de Contratações Anuais - PCA 2024, conforme dados abaixo:

ID PCA no PNCP: 29979036000140-0-000006/2024

Data de publicação no PNCP: 20/5/2023

Id do item no PCA: 8

Classe/Grupo: 929 - OUTROS SERVIÇOS DE EDUCAÇÃO E TREINAMENTO

Identificador da Futura Contratação: 512006-90044/2023

Além disso esta em consonância com o previsto no Decreto nº 10.222, de 2020, enfatiza a importância das políticas e diretrizes para a segurança da informação na administração pública federal. Destaca a necessidade de capacitação contínua dos colaboradores em práticas de segurança da informação. Além disso, ressalta a relevância da formação de uma equipe de resposta a incidentes cibernéticos bem capacitada, alinhada com os padrões internacionais e as melhores práticas recomendadas por entidades de referência como o Gartner.

12. Benefícios a serem alcançados com a contratação

Espera-se que a capacitação possibilite aos participantes:

- formação de profissionais qualificados e aptos para atuar estratégica, tática, operacional e tecnicamente com maior capacidade, competência, habilidade e eficiência nos expedientes institucionais e administrativos que exigem ações efetivas e eficazes ante à realidade de segurança cibernética que impacta, dentre outros processos, a imagem e a consecução da missão do INSS e, consequentemente, o erário da Administração Pública Federal.

- Articular o conhecimento prático adquirido no cotidiano profissional com os conhecimentos adquiridos.
- Multiplicar os conhecimentos com outros servidores da área que não tenham participado dos estudos.

13. Providências a serem Adotadas

Não se aplica, tendo em vista que o curso vai ser realizado na sede da contratada

14. Possíveis Impactos Ambientais

A contratação deverá observar, no que couber, critérios de sustentabilidade ambiental.

15. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

15.1. Justificativa da Viabilidade

Assim, considerando a singularidade dos serviços a serem contratados e a notória especialização da NUCLEO DE INFORMACAO E COORDENACAO DO PONTO BR - NIC .BR, por sua renomada competência, experiência de mercado e certificações e, a contratação dos Cursos objetos desta contratação, promovidos por essa empresa, são caracterizadas pela inviabilidade de competição prevista no art. 74, inciso III, alínea "f" da Lei nº 14.133 de 1º de abril de 2021e, por isso, deve ser realizada pela forma direta, por inexigibilidade de licitação.

16. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

HUGO RAFAEL TORMA DE LIMA

Técnico do Seguro Social

JANAINA CLARA DOS SANTOS RAMOS

Chefe de Serviço

ROBERTO CARNEIRO DA SILVA

Diretor de Gestão de Pessoas