BANCO NACIONAL DE DESENVOLVIMENTO
ECONÔMICO E SOCIAL – BNDES

EDITAL

PREGÃO ELETRÔNICO

Nº **007/2024** – BNDES

Classificação: Documento Controlado (conforme OS PRESI Nº 01/2015- BNDES)

Prazo da Restrição: até a data da disponibilização do Aviso de Licitação para publicação

Restrição de Acesso: Empresas do Sistema BNDES – Uso no Âmbito Interno

Unidade Gestora: AJI/JULIC/GLIC4

BNDES

PREGÃO ELETRÔNICO
Nº 007/2024

BNDES

OBJETO

Contratação de serviços continuados, sem dedicação exclusiva de mão-de-obra, especializados em segurança cibernética para o Banco Nacional de Desenvolvimento Econômico e Social – BNDES, na modalidade Pregão Eletrônico, por **menor preço global** e modo de disputa **aberto e fechado**, conforme as especificações deste Edital e de seus Anexos, observados os seguintes **ITENS:**

ITEM I – Serviço técnico operacional especializado em segurança cibernética prestado por Centro de Operações de Segurança Cibernética (Cyber Security Operation Center – CSOC); e

ITEM II – Serviço técnico de inteligência especializado em segurança cibernética.

ABERTURA DA SESSÃO PÚBLICA

DATA	HORÁRIO	LOCAL
06/06/2024	**11**h**00**min (horário de Brasília – DF)	www.gov.br/compras/pt-br

BNDES

LEGISLAÇÃO APLICÁVEL

LEI COMPLEMENTAR Nº 123
14/12/2006

LEI Nº 13.709
14/08/2018

DECRETO Nº 8.538
06/10/2015

LEI Nº 13.303
30/06/2016

DECRETO Nº 8.945
27/12/2016

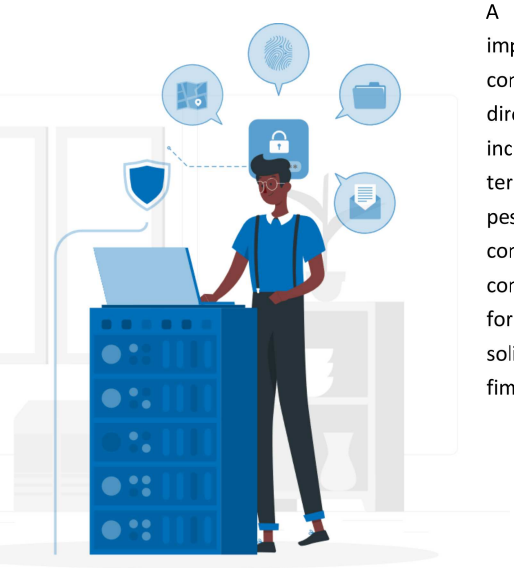
IN SEGES/ME Nº 73
30/09/2021***
***exclusivamente quanto ao rito da licitação, quando não for incompatível com o regime jurídico aplicado às empresas estatais.

LEI N° 14.133
01/04/2021**
**exclusivamente quanto ao rito da licitação, quando não for incompatível com o regime jurídico aplicado às empresas estatais.

DECRETO Nº 7.174
12/05/2010

Regulamento de Licitações e Contratos do Sistema BNDES, disponível no endereço eletrônico https://www.bndes.gov.br/wps/portal/site/home/transparencia/licitacoes-contratos

TRATAMENTO DE DADOS PESSOAIS



A participação neste procedimento licitatório importa na manifestação de inequívoco consentimento do titular, seja ele pessoa física direta ou indiretamente relacionada ao Licitante, inclusive sócios, empregados, contratados e/ou terceirizados, quando for o caso, dos dados pessoais que tenham se tornado públicos como condição para participação na licitação e para contratação, para tratamento pelo BNDES, na forma da Lei nº 13.709/2018. Poderão ser solicitados pelo BNDES dados pessoais adicionais a fim de viabilizar o cumprimento de obrigação legal.

DÚVIDAS SOBRE O EDITAL

Central de Serviços Serpro - CSS

licitacoes@bndes.gov.br

Em até 3 (três) dias úteis anteriores à data de abertura da sessão pública

ATENÇÃO!

No campo "assunto" do e-mail devem ser inseridos:

- modalidade e

- número da licitação (Pregão Eletrônico nº **007/2024 – BNDES).** As respostas serão divulgadas exclusivamente no Portal de Compras do Governo Federal (http://www.gov.br/compras/pt-br).

DÚVIDAS SOBRE O SISTEMA DE COMPRAS GOVERNAMENTAIS

Central de Serviços Serpro - CSS

css.serpro@serpro.gov.br

0800-978-9001

Manual do Portal de Compras

https://www.gov.br/compras/pt-br/acesso-a-informacao/manuais

CRÍTICAS, RECLAMAÇÕES E DENÚNCIAS

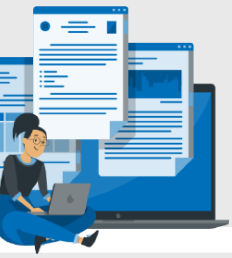
Ouvidoria do BNDES

Através de preenchimento do formulário disponível no endereço eletrônico www.bndes.gov.br/ouvidoria

Caixa Postal 15054, CEP nº 20.031-120, Rio de Janeiro – RJ

0800-7026307

ETAPAS pregão eletrônico



1 CADASTRAMENTO DA PROPOSTA

Cadastre a sua proposta no portal de compras do governo federal, preencha as informações solicitadas e inclua os documentos de habilitação.

2 ABERTURA DA SESSÃO PÚBLICA

O Pregoeiro classificará para a fase de lances as propostas em conformidade com os requisitos deste Edital e seus Anexos.

3 ORGANIZAÇÃO DAS PROPOSTAS

O sistema ordenará automaticamente as propostas classificadas pelo Pregoeiro.

4 OFERTAS DE LANCES

Se a sua proposta tiver sido classificada, você poderá ofertar o seu lance, assim como os demais Licitantes.

5 DIREITO DE PREFERÊNCIA

É garantido a:

Microempresas e empresas de pequeno porte.

Bens tecnológicos produzidos no Brasil pelo Processo Produtivo Básico (PPB).

6 NEGOCIAÇÃO DA PROPOSTA

O Pregoeiro encaminhará uma contraproposta ao Licitante que tenha apresentado o melhor preço.

7 PROPOSTA ADEQUADA AO LANCE FINAL

O Licitante de melhor lance apresentará a proposta adequada ao lance final ofertado em até 2h, a contar da solicitação do Pregoeiro.

8 ANÁLISE DOS VALORES

O Pregoeiro examinará a compatibilidade do preço ofertado em relação ao valor estimado para a contratação.

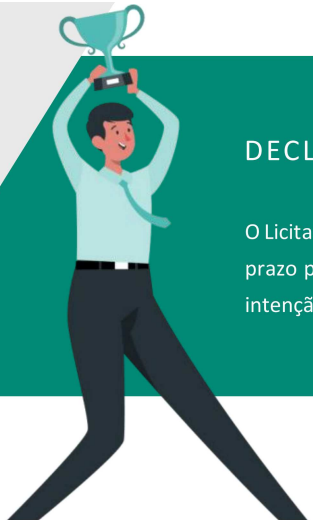
Se incompatível, será convocado o próximo colocado.

9 ANÁLISE DA HABILITAÇÃO

Aceita a proposta, o Pregoeiro analisará a habilitação.

Se incompatível, será convocado o próximo colocado.

Inversão de fases - a análise da habilitação pode ocorrer antes da proposta de valores. Confira a hipótese na cláusula 4.11.1 deste Edital.



DECLARAÇÃO DO VENCEDOR

O Licitante será declarado vencedor, abrindo-se prazo para que os outros possam manifestar a intenção de recorrer.

PREGÃO ELETRÔNICO
Nº 007/2024

BNDES

EDITAL

1 OBJETO

1.1 O presente Pregão visa à contratação de serviços continuados, sem dedicação exclusiva de mão-de-obra, especializados em segurança cibernética para o Banco Nacional de Desenvolvimento Econômico e Social – BNDES, por menor preço global e modo de disputa aberto e fechado, conforme as especificações deste Edital e de seus Anexos, observados os seguintes ITENS:

ITEM I – Serviço técnico operacional especializado em segurança cibernética prestado por Centro de Operações de Segurança Cibernética (Cyber Security Operation Center – CSOC) – valor global de até R$ 6.989.847,28 (seis milhões e novecentos e oitenta e nove mil e oitocentos e quarenta e sete reais e vinte e oito centavos) ; e

ITEM II – Serviço técnico de inteligência especializado em segurança cibernética - valor global de até R$ 1.835.303,06 (um milhão e oitocentos e trinta e cinco mil e trezentos e três reais e seis centavos).

1.1.1 Havendo divergência entre as informações constantes do registro da licitação no Compras Governamentais e as constantes deste Edital e de seus Anexos, prevalecerão as últimas.

2 PARTICIPAÇÃO NA LICITAÇÃO

2.1 Poderão participar deste Pregão os interessados cadastrados e habilitados parcialmente no Sistema de Cadastramento Unificado de Fornecedores – SICAF do Ministério do Planejamento que atenderem às exigências constantes deste Edital e de seus Anexos.

2.1.1 A inclusão dos documentos e/ou informações no Sistema de Cadastramento Unificado de Fornecedores – SICAF é de inteira responsabilidade do licitante, podendo ocasionar na sua desclassificação a ausência de qualquer documento exigido neste Edital.

2.2 Os interessados poderão participar do procedimento licitatório por intermédio de sua matriz ou filial, desde que cumpram as condições exigidas para o cadastramento e a habilitação parcial no SICAF, bem como as exigências constantes deste Edital e de seus Anexos.

2.3 Estará **impedido** de participar deste Pregão o interessado que:

I. tenha sofrido decretação de falência ou dissolução;

II. esteja cumprindo penalidade de suspensão temporária de participação em licitação e impedimento de contratar com o **BNDES**, nos termos do artigo 83, inciso III, da Lei nº 13.303/2016;

III. tenha sido declarado inidôneo para licitar ou contratar com a União Federal, nos termos do artigo 38, inciso III, da Lei nº 13.303/2016, ou esteja cumprindo penalidade de impedimento de licitar e contratar com a União Federal, nos termos do artigo 7º da Lei nº 10.520/2002 ou do artigo 156, §4º, da Lei n° 14.133/2021;

IV. esteja proibido de licitar e contratar com a Administração Pública, bem como de receber incentivos, subsídios, subvenções, doações ou empréstimos de pessoas jurídicas de direito público ou de pessoas jurídicas controladas pelo Poder Público, com fundamento em outros dispositivos legais não mencionados nos incisos II e III deste item[1];

V. se enquadre em alguma das demais vedações previstas na Lei nº 13.303/2016, notadamente em seu artigo 38;

VI. se enquadre em algumas das vedações previstas na Política para Transações com Partes Relacionadas das Empresas do Sistema BNDES (disponível no endereço eletrônico https://bndes.gov.br/wps/portal/site/home/transparencia/prestacao-de-contas/regulamentos-politicas-corporativas/politica-para-transacoes-com-partes-relacionadas) e na Política de Equidade de Gênero e Valorização da Diversidade do Sistema BNDES (disponível no endereço eletrônico https://www.bndes.gov.br/wps/portal/site/home/desenvolvimento-sustentavel/o-que-nos-orienta/outras-politicas-e-regulamentos/politica-genero-diversidade);

VII. possua em seu contrato ou estatuto social finalidade ou objetivo incompatível com o objeto deste Pregão; e

VIII. esteja organizado sob a forma de consórcio.

2.3.1 Para fins de cumprimento ao disposto no item 2.3 deste Edital, o Licitante **deverá apresentar**, juntamente com a proposta ajustada, nos termos do item 4.10 deste Edital, declaração conforme modelo A do Anexo V (Modelos de Declaração) deste Edital.

2.4 Será permitida a participação de sociedades optantes do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e das Empresas de Pequeno Porte – Simples Nacional, observadas as orientações dispostas nos subitens a seguir.

2.4.1 O Licitante optante do Simples Nacional que vier a executar atividade vedada pelo artigo 17 da Lei Complementar nº 123/2006[2] não poderá beneficiar-se da condição de optante.

2.4.1.1 Na hipótese do item 2.4.1 deste Edital, uma vez celebrado o Contrato, o Contratado deverá providenciar, perante a Receita Federal do Brasil – RFB, sua exclusão obrigatória do Simples Nacional, no prazo estipulado pelo artigo 30 da Lei Complementar nº 123/2006.

2.4.2 O Licitante optante do Simples Nacional, que não se enquadre em situação de vedação prevista no artigo

[3] BNDES Participações S/A – BNDESPAR e a Agência Especial de Financiamento Industrial – FINAME

[3] BNDES Participações S/A – BNDESPAR e a Agência Especial de Financiamento Industrial – FINAME

17 da Lei Complementar nº 123/2006, somente poderá beneficiar-se de tal condição se, com o valor ofertado em sua proposta, não vier a exceder o limite de receita bruta anual, previsto no artigo 3º da Lei Complementar nº 123/2006, ao longo da vigência do Contrato.

2.4.2.1 Se o Licitante optante do Simples Nacional extrapolar o limite de receita bruta anual previsto no artigo 3º da Lei Complementar nº 123/2006 ao longo da vigência do Contrato, uma vez sendo contratado deverá providenciar, perante a Receita Federal do Brasil – RFB, sua exclusão obrigatória do Simples Nacional, no prazo estipulado pelo artigo 30 da Lei Complementar nº 123/2006.

2.5 No âmbito do presente procedimento licitatório serão observadas as disposições constantes do artigo 4° da Lei n° 14.133/2021.

2.6 Os interessados **poderão, a seu critério,** vistoriar as dependências do BNDES, até o dia anterior à data da abertura da sessão pública, com o objetivo de obter todas as informações relativas ao local e às condições de execução do objeto, observado o disposto no Anexo I (Termo de Referência) deste Edital.

3
APRESENTAÇÃO DAS PROPOSTAS E DA DOCUMENTAÇÃO DE HABILITAÇÃO

3.1 O interessado em participar deste Pregão deverá, até a abertura da sessão pública, cadastrar sua proposta por intermédio do Portal de Compras do Governo Federal.

3.2 No âmbito do cadastramento da proposta, o Licitante deverá preencher os campos relativos:

I. à descrição do objeto ofertado para o respectivo **ITEM**;

a. a inclusão, no Portal de Compras do Governo Federal, de qualquer dado que identifique o Licitante, no campo destinado à descrição do objeto ofertado, **acarretará sua desclassificação;**

II. ao **valor global** ofertado para o respectivo **ITEM**, de acordo com as seguintes orientações:

a. **devem estar incluídas no referido valor** todas as despesas e custos, diretos e indiretos (tais como tributos, encargos sociais e trabalhistas, contribuições, transporte, viagens, seguro e insumos), necessários ao cumprimento integral do objeto a ser contratado; e

b. **o valor deverá ser expresso em Real (R$)** com 2 (duas) casas decimais;

III. à UASG – 201014 e UF – Rio de Janeiro – RJ;

IV. a quaisquer outras informações/declarações que venham a ser requeridas pelo Portal de Compras do Governo Federal.

3.3 A proposta deverá ter validade de 60 (sessenta) dias, a contar da data da abertura da sessão pública.

3.4 Não será considerada qualquer oferta de vantagem não prevista neste Edital e em seus Anexos.

3.5 O Licitante poderá retirar ou substituir a proposta inserida no Portal de Compras do Governo Federal até a abertura da sessão pública.

3.6 O cadastro da proposta no Portal de Compras do Governo Federal implica a aceitação integral e irretratável dos termos do presente Edital, não sendo admitidas alegações de desconhecimento de fatos e de condições que impossibilitem ou dificultem a execução do objeto licitado.

4
SESSÃO PÚBLICA E FASE RECURSAL

4.1 Na data e no horário definidos no preâmbulo deste Edital, a sessão pública será aberta automaticamente pelo sistema, observando-se que a verificação da conformidade da proposta será feita exclusivamente na fase de julgamento em relação à proposta mais bem classificada.

4.1.1 Sem prejuízo no disposto no item 4.1, será desclassificada a proposta que identifique o Licitante e/ou apresente valor simbólico, irrisório ou de valor zero, incompatível com os praticados no mercado e com os custos estimados para a execução do objeto.

4.2 As comunicações entre o Pregoeiro e os Licitantes serão realizadas por campo próprio do sistema, cabendo aos Licitantes acompanhar todas as operações realizadas no Portal de Compras do Governo Federal durante a sessão pública, sendo responsáveis pelo ônus decorrente da perda de transações, causada pela inobservância das mensagens e prazos registrados pelo sistema e pelo Pregoeiro, ou por sua desconexão.

4.3 Após a abertura da sessão pública, o Pregoeiro poderá suspendê-la, adiá-la ou reabri-la a qualquer momento, informando previamente os Licitantes por meio do Portal de Compras do Governo Federal, com, no mínimo, 24 (vinte e quatro) horas de antecedência.

4.4 Iniciada a etapa de lances, a qual será realizada exclusivamente por meio do Portal de Compras do Governo Federal, deverão ser observadas as seguintes regras:

I. os lances deverão ser formulados considerando o valor global do objeto ofertado para o respectivo ITEM;

II. o Licitante somente poderá oferecer lance inferior ao último por ele ofertado, ainda que superior ao menor registrado no sistema, observando-se o intervalo mínimo de R$ 1.000,00 (mil reais) entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta;

III. lances simbólicos, irrisórios ou de valor zero, incompatíveis com os praticados no mercado e com os custos estimados para a execução do objeto, poderão ser excluídos do sistema pelo Pregoeiro;

IV. não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro;

V. os lances deverão ser formulados considerando-se a necessidade de cumprimento das obrigações previstas neste Edital e em seus Anexos;

VI. durante a sessão pública os Licitantes serão informados em tempo real do valor do melhor lance registrado, vedada a identificação do Licitante;

VII. o Licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

4.5 No caso de desconexão do Pregoeiro no decorrer da etapa de lances, se o Portal de Compras do Governo Federal permanecer acessível aos Licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

4.5.1 Caso a desconexão do sistema eletrônico persistir por tempo superior a 10 (dez) minutos para o Pregoeiro, a sessão pública será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no Portal de Compras do Governo Federal.

4.6 Considerando o modo de disputa aberto e fechado, a etapa de envio de lances terá duração de 15 (quinze) minutos, após a qual o sistema encaminhará o aviso de fechamento iminente dos lances e, transcorrido o período de até 10 (dez) minutos, aleatoriamente determinado, a recepção de lances será automaticamente encerrada.

4.6.1 Após a etapa de encerramento aleatório, o sistema abrirá a oportunidade para que o autor da melhor oferta e os autores das ofertas subsequentes com valores ou percentuais até 10% (dez por cento) superiores àquela, possam ofertar um lance final e fechado em até 5 (cinco) minutos, que será sigiloso até o encerramento deste prazo.

4.6.2 Na ausência de, no mínimo, 3 (três) ofertas nas condições de que trata o item 4.6.1, os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 3 (três), poderão oferecer um lance final e fechado em até 5 (cinco) minutos, que será sigiloso até o encerramento do prazo.

4.6.3 Nos procedimentos de que tratam os itens 4.6.1 e 4.6.2, o Licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance, observando-se que, ao final, os lances serão ordenados e divulgados pelo sistema.

4.7 Encerrada a etapa de lances, o sistema estabelecerá a ordem de classificação dos Licitantes, observadas as regras de preferência a seguir elencadas:

4.7.1 Se o melhor lance não tiver sido ofertado por microempresa ou empresa de pequeno porte e houver lance apresentado por microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior àquele, proceder-se-á da seguinte forma:

I. o sistema convocará a microempresa ou a empresa de pequeno porte mais bem classificada dentre aquelas enquadradas na condição prevista no *caput* deste item 4.7.1 para, no prazo de até 5 (cinco) minutos, ofertar valor inferior ao melhor lance;

II. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos itens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta;

III. na hipótese de a microempresa ou empresa de pequeno porte mencionada no inciso I deixar de oferecer valor inferior, o sistema convocará as microempresas ou empresas de pequeno porte remanescentes que porventura se enquadrem na condição prevista no *caput* deste, na ordem classificatória, para o exercício do mesmo direito;

IV. na hipótese de todas as microempresas ou empresas de pequeno porte enquadradas na condição do *caput* deste item 4.7.1 deixarem de ofertar valor inferior, será observado o procedimento descrito no subitem 4.7.2 deste Edital.;

V. na hipótese de a microempresa ou empresa de pequeno porte ofertar valor inferior ao melhor lance, o Pregoeiro a convocará, dando prosseguimento à sessão pública.

4.7.1.1 O Pregoeiro poderá solicitar documentos que comprovem o enquadramento do Licitante na condição de microempresa ou empresa de pequeno porte.

4.7.1.2 O Licitante que se declarar microempresa ou empresa de pequeno porte para fins de obtenção dos benefícios da Lei Complementar nº 123/2006 e não possuir tal condição ficará sujeito à sanção administrativa prevista neste Edital, sem prejuízo da responsabilização em outras esferas, devendo-se observar ainda a restrição constante do artigo 4°, §2º, da Lei n° 14.133/2021.

4.7.1.3 O procedimento listado nos incisos do item 4.7 deste Edital será promovido pelo Pregoeiro, observada a ordem classificatória, sempre que o Licitante ofertante da melhor proposta for desclassificado, inabilitado ou excluído deste Pregão.

4.7.1.4 Na hipótese de o melhor lance ter sido ofertado por microempresa ou empresa de pequeno porte ou na hipótese de o melhor lance não ter sido ofertado por microempresa ou empresa de pequeno porte e não haver oferta apresentada por microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior ao melhor lance, será observado o procedimento descrito no item 4.7.2 deste Edital.

4.7.2 Ultrapassada a etapa prevista no item 4.7.1 deste Edital, serão selecionados os Licitantes cujos lances finais estiverem situados até 10% (dez por cento) acima do melhor lance, para exercício dos direitos de preferência listados nos incisos abaixo:

I. os Licitantes enquadrados na condição prevista no caput deste item 4.7.2 cujos bens possuam tecnologia desenvolvida no País e sejam produzidos de acordo com o Processo Produtivo Básico (PPB) serão convocados pelo sistema, observada a ordem classificatória, para, no prazo de até 5 (cinco) minutos, ofertar valor igual ou inferior ao melhor lance;

II. na hipótese de os Licitantes mencionados no inciso anterior deixarem de ofertar valor igual ou inferior, o sistema convocará os Licitantes cujos bens possuam tecnologia desenvolvida no país, para o exercício do mesmo direito;

III. na hipótese de os Licitantes mencionados no inciso anterior também deixarem de oferecer valor igual ou inferior, o sistema convocará os Licitantes cujos bens sejam produzidos de acordo com o Processo Produtivo Básico (PPB) para o exercício do mesmo direito;

IV. na hipótese de todos os Licitantes enquadrados nas condições acima deixarem de ofertar valor igual ou inferior, o Pregoeiro convocará o Licitante ofertante do melhor lance, dando-se prosseguimento à sessão pública;

V. na hipótese de um Licitante exercer seu direito de preferência, o Pregoeiro o convocará, dando prosseguimento à sessão pública.

4.7.2.1 As microempresas e empresas de pequeno porte que atendam ao disposto nos três primeiros incisos do item 4.7.2 deste Edital terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso.

4.7.2.2 A comprovação do enquadramento nas hipóteses de preferência descritas no item 4.7.2 deste Edital dar-se-á por meio de declaração do Licitante beneficiário, inserida no momento de cadastramento de sua proposta no sistema, bem como por intermédio de consulta, realizada pelo **BNDES** à página da Internet dos sítios oficiais.

4.7.2.3 O Pregoeiro poderá, ainda, solicitar documentos adicionais que comprovem o enquadramento do Licitante na hipótese de preferência.

4.7.2.4 O procedimento listado nos incisos do item 4.7.2 deste Edital será promovido pelo Pregoeiro, observada a ordem classificatória, sempre que o Licitante ofertante da melhor proposta for desclassificado, inabilitado ou excluído deste Pregão.

4.8 Em caso de empate entre propostas serão adotados os critérios de desempate previstos no artigo 55 da Lei n° 13.303/2016.

4.9 Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro verificará a inexistência dos impedimentos previstos no item 2.3, que deverá ser confirmada em cadastros oficiais de empresas punidas ou sancionadas (tais como: CEIS, CNEP, CNIA e à certidão negativa de licitante inidôneo, emitida pelo TCU) e em sistema interno de consulta a impedimentos, e estando regular a participação do Licitante classificado em primeiro lugar, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado a melhor oferta, ressalvadas as hipóteses em que a redução possa comprometer a exequibilidade da proposta final ofertada.

4.9.1 Para oferta da contraproposta a que se refere o item acima, o Pregoeiro poderá solicitar previamente ao Licitante a apresentação da proposta adequada ao lance final ofertado, nos termos previstos no item 4.10.

4.9.2 O Pregoeiro poderá suspender a sessão para que o Licitante ofertante do melhor lance possa avaliar a possibilidade de **redução do último valor** ofertado.

4.10 O Licitante ofertante do melhor lance deverá apresentar a proposta adequada ao lance final ofertado para o respectivo ITEM, exclusivamente pelo sistema do Portal de Compras do Governo Federal, conforme modelo constante do **Anexo II (Modelo de Proposta)** deste Edital, no prazo de até 2 (duas) horas, a contar da solicitação do Pregoeiro, prorrogáveis, a critério do **BNDES**.

4.10.1 A proposta deverá identificar o Licitante, e ser redigida em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, com clareza, sem emendas, rasuras ou entrelinhas, datada e assinada por seu Representante Legal ou Procurador.

4.10.2 Os valores ofertados na proposta deverão ser expressos em Real (R$) e com 2 (duas) casas decimais.

4.10.3 Devem estar incluídas no valor global ofertado todas as despesas e custos, diretos e indiretos (tais como tributos, encargos sociais e trabalhistas, contribuições, transporte, viagens, seguro e insumos), necessários ao cumprimento integral do objeto a ser contratado.

4.10.4 O Licitante deverá informar, em sua proposta, no campo “Estabelecimentos vinculados à execução contratual (matriz/filial)” do Anexo II (Modelo de Proposta) deste Edital, o(s) estabelecimento(s) responsável(is) pela execução contratual.

4.10.5 Deverá ser anexada à Proposta a Declaração de Inexistência de Impedimentos de Participação prevista no Anexo V deste Edital.

4.10.6 Deverá ser anexada à Proposta a documentação prevista no item 12.1 do Anexo I (Termo de Referência) deste Edital.

4.11 Após o envio da documentação de proposta, o Pregoeiro examinará a compatibilidade do preço ofertado

em relação ao valor estimado para a contratação.

4.11.1 Nesta ocasião, o Pregoeiro poderá solicitar a documentação de habilitação do Licitante ofertante do melhor lance.

4.11.2 Caso sejam exigidos documentos de habilitação que não estejam contemplados no SICAF, o Pregoeiro deverá solicitar ao Licitante a apresentação das informações necessárias por intermédio do sistema, no prazo de 2 (horas), a contar da respectiva convocação, permitida a prorrogação, a critério do **BNDES**.

4.11.3 Caso adotado o procedimento previsto no item 4.11.1, a análise definitiva da proposta, em todos os seus requisitos, somente será concluída se verificado o atendimento dos requisitos de habilitação do Licitante ofertante do melhor lance.

4.12 Na análise e julgamento da proposta o Pregoeiro poderá, justificadamente, sanar erros ou falhas que não alterem sua substância da proposta (vícios sanáveis), atribuindo-lhe validade e eficácia, rejeitando aquela:

I. que possuir vícios insanáveis;

II. que não atender às exigências deste Edital e de seus Anexos;

III. cujo **valor unitário ou global forem superiores** aos limites estabelecidos no Anexo I (Termo de Referência) deste Edital; ou

IV. cujos **valores unitários ou/e global** forem inexequíveis, observado o disposto no subitem 4.12.1 deste Edital.

4.12.1 Havendo indícios de **inexequibilidade dos valores ofertados**, será instaurada diligência para que o Licitante ofertante da melhor proposta possa, no prazo fixado pelo Pregoeiro:

I. comprovar a exequibilidade, apresentando justificativas e documentos que comprovem a viabilidade e a compatibilidade **dos valores ofertados**; ou

II. ajustar **os valores ofertados**, apresentando proposta readequada (tendo como limite **máximo o valor global ofertado** na proposta) e, se for o caso, justificativas para os ajustes realizados.

4.12.2 Os documentos apresentados pelo Licitante ofertante da melhor proposta, a título de ajuste **dos valores ofertados ou** de comprovação de sua exequibilidade, serão encaminhados para análise da Equipe Técnica do **BNDES** a fim de que possa emitir o competente parecer.

4.13 Recusada a proposta, o Pregoeiro convocará o próximo colocado, observadas as disposições relativas ao direito de preferência previstas neste Edital.

4.14 Aceita a proposta ou adotada a opção prevista no subitem 4.11.1, o Pregoeiro passará à análise de habilitação, observado o procedimento disposto no item 4.11.2.

4.14.1 Para que seja habilitado, o Licitante deverá atender a todas as exigências abaixo listadas e as previstas no subitem 4.15 deste Edital:

I. Decreto de autorização de funcionamento no Brasil, quando se tratar de sociedade estrangeira em funcionamento no País;

II. Ato de registro ou autorização para funcionamento expedido por órgão competente, quando a atividade a ser desempenhada pela sociedade assim o exigir;

III. Instrumento Particular de Mandato (Procuração) com firma reconhecida em cartório ou em conjunto com a cédula de identidade ou documento equivalente do signatário, para fins de conferência da sua assinatura ou digitalmente assinada, ou Instrumento Público de Mandato, outorgando expressamente poderes para a prática de todos os atos pertinentes à licitação, nos casos em que o Licitante for representado por Procurador;

IV. no caso de:

SOCIEDADE LIMITADA UNIPESSOAL

Ato Constitutivo em vigor, devidamente registrado no registro competente, com sua(s) respectiva(s) alteração(ções), ou a sua última consolidação, acompanhado do documento comprobatório de seus administradores devidamente registrado;

SOCIEDADE SIMPLES

Ato Constitutivo em vigor, devidamente registrado no registro competente, com sua(s) respectiva(s) alteração(ões), ou a sua última consolidação, bem como documento que comprove a indicação de seus administradores;

EMPRESÁRIO INDIVIDUAL

Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

MICROEMPREENDEDOR INDIVIDUAL

Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

Certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, ou qualquer outro documento idôneo que comprove a condição de microempresa ou empresa de pequeno porte;

V. certidão negativa ou positiva com efeitos de negativa de débitos relativos aos tributos federais, à dívida ativa da União, e às contribuições previdenciárias e às de terceiros, expedida pela Secretaria da Receita Federal;

VI. certidão de Regularidade perante o Fundo de Garantia por Tempo de Serviço, expedida pela Caixa Econômica Federal;

VII. certidão negativa de pedido de falência ou recuperação judicial, expedida na sede da pessoa jurídica;

a) Na hipótese de a sede ser situada em outra localidade que não a Capital do Rio de Janeiro, poderá ser exigido do Licitante que apresente a relação dos Cartórios de Distribuição da Comarca que expede a certidão mencionada neste inciso, emitida pelo órgão competente.

VIII. Índices de Liquidez Geral (LG), de Solvência Geral (SG) e de Liquidez Corrente (LC) iguais ou maiores que 1 (= ou > 1), observadas as fórmulas a seguir:

$$LG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

$$SG = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}} \qquad LC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

a) O Licitante deverá apresentar as informações contábeis, na forma da lei, para cálculo dos referidos índices.

b) Caso o resultado de qualquer dos índices seja menor que 1 (um), o Licitante deverá apresentar as informações contábeis, na forma da lei, a fim de comprovar que possui capital social registrado ou patrimônio líquido igual ou superior a:

ITEM I - R$ 698.984,72 (seiscentos e noventa e oito mil, novecentos e oitenta e quatro reais e setenta e dois centavos)

ITEM II – R$ 183.530,30 (cento e oitenta e três mil, quinhentos e trinta reais e trinta centavos)

b.1) Caso o Licitante apresente proposta mais vantajosa para mais de um **ITEM,** deverá comprovar que possui capital social ou patrimônio líquido igual ou superior ao somatório dos valores acima previstos, relativos a cada um dos **ITENS** ofertados.

X. qualificação técnica, relativa às parcelas de maior relevância técnica e econômica do objeto, nos termos do Anexo I (Termo de Referência) deste Edital.

4.14.2 Caso o Licitante indique na proposta outro(s) estabelecimento(s) responsável(is) pela execução contratual, deverá apresentar, além dos documentos que comprovem a sua própria habilitação, aqueles relativos à habilitação do(s) estabelecimento(s) indicado(s), observando-se que alguns documentos, por sua própria natureza, são emitidos somente em nome da matriz.

4.14.2.1 Poderá(ão) ser apresentado(s) em nome de quaisquer de seu(s) estabelecimento(s) o(s) atestado(s) de capacidade técnica exigido(s).

4.15 O Pregoeiro analisará a documentação apresentada, verificando o atendimento às exigências deste Edital e de seus Anexos. Para fins de julgamento da habilitação poderão ser consultados outros sítios da Internet, notadamente sítios oficiais emissores de certidões.

4.15.1 As certidões que não possuírem prazo de validade somente serão aceitas se as respectivas datas de emissão não excederem a 90 (noventa) dias de antecedência da data de sua apresentação.

4.15.2 Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 5 (cinco) dias úteis, contado da decisão do Pregoeiro que declarar o Licitante vencedor da licitação, prorrogáveis por igual período, a critério do

BNDES, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa, sob pena de inabilitação no sistema.

4.15.3 Caso seja necessária a instauração de diligência para o julgamento da habilitação, os documentos solicitados nesta ocasião deverão ser encaminhados exclusivamente via sistema, dentro do prazo definido pelo Pregoeiro, que não poderá ser inferior a 2 (duas) horas.

4.16 Se o Licitante não atender às exigências habilitatórias, o Pregoeiro convocará o próximo colocado, observadas as disposições relativas ao direito de preferência previstas neste Edital.

4.17 Constatado o atendimento de todos os requisitos de habilitação e verificando-se aceitabilidade da proposta, o Licitante será declarado vencedor do certame, abrindo-se prazo para que os Licitantes possam, em campo próprio do sistema, manifestar sua intenção de recorrer sob pena de preclusão deste direito.

4.17.1 Admitida pelo Pregoeiro a intenção de recurso, será concedido, ao Licitante que tenha manifestado tal intenção, o prazo de até 3 (três) dias úteis, para apresentar, pelo Portal de Compras do Governo Federal, as razões recursais, ficando os demais Licitantes, desde logo, intimados para, querendo, apresentarem as contrarrazões em igual prazo, que começará a contar do término do prazo para a apresentação das razões recursais.

4.17.2 A vista dos autos do processo desta licitação referente aos documentos que não estão no sistema do Portal de Compras do Governo Federal deverá ser solicitada, à Gerência de Licitações e Contratos 4 do **BNDES**, pelo e-mail licitacoes@bndes.gov.br.

4.17.3 O Pregoeiro poderá reconsiderar sua decisão ou mantê-la. Neste último caso, o Pregoeiro deverá, no prazo de 3 (três) dias úteis, submeter o recurso, devidamente informado, à apreciação da Autoridade Superior, que deverá promover sua decisão no prazo de 10 (dez) dias úteis.

4.17.4 O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

4.18 A sessão pública será encerrada depois de declarado o vencedor e transcorrido o prazo para manifestação de intenção de recorrer. Não havendo registro de intenção de recurso, o objeto da licitação poderá ser adjudicado ao Licitante vencedor.

5 ENCERRAMENTO DA LICITAÇÃO

5.1 Definido o Licitante vencedor, o objeto licitado lhe será adjudicado, estando a licitação sujeita à homologação pela Autoridade Competente, que analisará a conveniência e oportunidade da contratação, bem como a legalidade dos atos praticados.

5.2 A qualquer tempo, a licitação poderá ser revogada ou anulada, nos limites fixados pela Lei nº 13.303/2016.

5.2.1 Caso seja verificada, após a abertura da sessão pública, a intenção de se revogar ou anular a

licitação, será concedido aos Licitantes prazo para contestar o ato e exercer o direito ao contraditório e à ampla defesa.

5.2.2 O contraditório prévio mencionado no subitem acima poderá ser dispensado caso o fato gerador da revogação ou anulação não seja imputado aos Licitantes.

6
SANÇÃO ADMINISTRATIVA

6.1 O Licitante cuja conduta esteja prevista em um dos incisos do artigo 84 da Lei nº 13.303/2016 ficará sujeito à sanção de suspensão temporária de participação em licitação e impedimento de contratar com o **BNDES**, pelo prazo de até 2 (dois) anos.

6.2 Somente será aplicada sanção mediante procedimento administrativo punitivo licitatório, na forma do Regulamento de Licitações do Sistema **BNDES**, pelo qual será assegurado prazo de até 10 (dez) dias úteis para o exercício do contraditório e a ampla defesa.

6.3 A decisão será comunicada por escrito ao Licitante, dela cabendo recurso, dirigido à Autoridade que proferiu a decisão, no prazo de até 10 (dez) dias úteis, a contar do recebimento da notificação.

6.4 No caso de atos lesivos à Administração Pública, nacional ou estrangeira, observar-se-ão os termos da Lei nº 12.846/2013.

7
CONTRATAÇÃO

7.1 Homologada a licitação, o BNDES convocará o vencedor do certame, por e-mail, para apresentar, no prazo definido pelo BNDES no momento da convocação:

I. o Contrato assinado preferencialmente de forma digital, mediante certificação digital ICP-Brasil por seu Representante Legal, observada minuta constante do Anexo III (Minuta de Contrato) deste Edital.

7.2 Será solicitado ao Licitante vencedor que atualize as certidões exigidas na fase de habilitação, se o prazo de validade expirar durante o curso da licitação.

7.3 Na hipótese de recusa ou inércia do Licitante na apresentação dos documentos listados nos itens 7.1 e 7.2 deste Edital, a sessão pública poderá ser retomada para que o Pregoeiro providencie a exclusão do Licitante da licitação, convocando, em seguida, os licitantes remanescentes, na ordem de classificação, desde que atendidos os requisitos de proposta e habilitação, nos termos do item 4.17, para assinatura do contrato, no mesmo prazo e nas mesmas condições propostas, inclusive quanto aos preços, pelo Licitante que deixou de atender a convocação.

7.3.1 Na hipótese do item acima, deverão ser observadas as disposições relativas à preferência previstas neste Edital.

8
INFORMAÇÕES ADICIONAIS

8.1 Qualquer pessoa poderá impugnar os termos do presente Edital até **3 (três)** dias úteis anteriores à data de abertura da sessão pública.

8.1.1 A impugnação deverá ser encaminhada à Gerência de Licitações e Contratos 4 do **BNDES**, pelo e-mail licitacoes@bndes.gov.br, devendo ser informado, no campo "assunto", a modalidade e o número da licitação (Pregão Eletrônico nº 007/2024 – **BNDES**).

8.1.2 Caberá ao Pregoeiro julgar a impugnação no prazo de até 3 (três) dias úteis.

8.1.3 A ata de julgamento de impugnação será divulgada no Portal de Compras do Governo Federal (www.gov.br/compras/pt-br), para ciência de todos os interessados.

8.2 O BNDES reserva-se o direito de alterar os termos deste Edital. A alteração que afetar a formulação das propostas implicará a reabertura do prazo para a apresentação das mesmas.

8.3 É facultada ao Pregoeiro, em qualquer fase da licitação, a promoção de diligência a ser registrada em ata, com a finalidade de esclarecer, corrigir ou complementar a instrução do processo, inclusive com a possibilidade de inclusão de documentos necessários para confirmação da compatibilidade da oferta com as exigências do edital, adotando-se o princípio do formalismo moderado.

8.4 A qualquer tempo o **BNDES** poderá negociar com o Licitante, com o fim de obter proposta mais vantajosa.

8.5 As normas disciplinadoras desta licitação serão interpretadas visando à ampliação da disputa entre os Licitantes, à obtenção da proposta mais vantajosa, desde que não comprometam os interesses do BNDES, bem como à finalidade e à segurança da contratação.

8.6 Caso exigida tradução de documentos apresentados em língua estrangeira, está se dará na forma livre, facultando-se ao **BNDES** a exigência de tradução juramentada, apostilamento ou consularização do(s) documento(s) como condição para a assinatura do contrato.

8.7 Na contagem dos prazos estabelecidos neste Edital e em seus Anexos observar-se-á o que segue:

I. excluir-se-á o dia do início e incluir-se-á o do vencimento;

II. os prazos somente serão iniciados e vencidos em dias de expediente no BNDES.

8.8 Na ocorrência de qualquer fato superveniente ou na hipótese de caso fortuito ou de força maior será observado o seguinte:

I. se o fato impedir a realização de sessão pública na data marcada, a referida sessão será adiada;

II. os prazos que estiverem em curso serão suspensos, voltando a correr assim que a situação estiver normalizada.

8.9 O andamento da licitação poderá ser acompanhado por qualquer interessado no Portal de Compras do Governo Federal (www.gov.br/compras/pt-br).

8.10 Fica eleito o Foro da Cidade do Rio de Janeiro para solucionar eventuais litígios, afastado qualquer outro, por privilegiado que seja.

Rio de Janeiro, 10 de maio de 2024.

Mariana Terk Campos
Gerente
AJI/JULIC/GLIC4

Pedro Ivo Peixoto da Silva
Chefe de Departamento
AJI/JULIC

PREGÃO ELETRÔNICO Nº 007/2024 – BNDES
ANEXO I – TERMO DE REFERÊNCIA

1. **OBJETO**

1.1. A presente licitação tem como objeto a contratação de serviços continuados, sem dedicação exclusiva de mão-de-obra, especializados em segurança cibernética para o Banco Nacional de Desenvolvimento Econômico e Social – BNDES, através de processo licitatório do tipo menor preço, pelo período de 60 (sessenta) meses, com opção de rescisão a partir do 30º (trigésimo) mês, compostos por:

1.1.1. **ITEM I** - serviço técnico operacional especializado em segurança cibernética prestado por Centro de Operações de Segurança Cibernética (Cyber Security Operation Center – CSOC) abrangendo as atividades de:

1.1.1.1. Monitoramento, resposta a incidentes de SI (Segurança da Informação) e gestão de ameaças cibernéticas (Computer Security Incident Response Team - CSIRT);

1.1.1.2. Levantamento e Gestão de Vulnerabilidades de Infraestrutura (Gestão de Vulnerabilidades – GVUL); e

1.1.1.3. Apoio técnico especializado para situações de crise decorrentes de incidentes de SI relevantes, com atuação presencial quando demandada pelo BNDES, para suporte e coordenação de ações de resposta, contenção, recuperação e investigação do incidente, incluindo as atividades de forense computacional conforme a ABNT NBR ISO/IEC 27037:2013 e Norma Complementar 21 da Instrução Normativa GSI Nº01 de 8 de outubro de 2014 (Incident Response Consulting - IRC).

1.1.2. **ITEM II** - serviço técnico de inteligência especializado em segurança cibernética envolvendo as atividades de:

1.1.2.1. Busca ativa por informações sobre ameaças para identificação antecipada de ameaças à infraestrutura do BNDES e suas identidades relevantes. Deve prover ações para proteção contra o uso indevido das marcas do BNDES, incluindo o monitoramento contínuo (contemplando redes sociais, surface, deep e dark web etc) e interação com empresas e/ou instituições para realizar os eventuais takedowns de sites, domínios, aplicações etc. (Cyber Threat Intelligence - CTI e Digital Risk Protection - DRP).

1.2. É vedada a subcontratação dos serviços objeto desta contratação.

1.3. Esta contratação tem natureza de serviço comum, de caráter continuado e sem fornecimento de mão-de-obra em regime de dedicação exclusiva.

1.4. Os interessados poderão participar da presente licitação ofertando proposta para um ou ambos os ITENS, desde que atendidas as exigências do Edital e de seus Anexos, bem como ao disposto no item 1.4.1 a seguir.

1.4.1. O critério de julgamento adotado será o menor preço do item, observadas as exigências contidas neste Termo de Referência quanto às especificações do objeto.

2. DEFINIÇÕES – ITENS I e II

2.1. Ambiente (environment) – Subconjunto da infraestrutura de TIC utilizado para um propósito específico. Por exemplo, ambiente de produção, de homologação e testes e de desenvolvimento.

2.2. Atividade – Conjunto de uma ou mais etapas pertencentes a uma Tarefa.

2.3. Ativos de Informação - Conjunto de pessoas, tecnologias, marcas, nomes de domínios, entre outras informações, que será monitorado pelo serviço de Inteligência de Ameaças Cibernéticas;

2.4. Ativos de TIC – Qualquer software e/ou equipamento utilizado para provimento de serviços de TIC. São exemplos de Ativos de TIC - Estações de trabalho (Desktops, Laptops etc.), Servidores, Switches, Roteadores, Dispositivos Móveis (Smartphones e Tablets), dispositivos IOT (Impressoras, Câmeras de Monitoramento, Totens etc.), Sistemas Operacionais, Imagens para contêineres hospedadas nas plataformas de gerenciamento de repositórios e Contêineres em execução nas plataformas de gerenciamento de contêineres.

2.5. Autenticidade - propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

2.6. Backup – Ato de copiar dados com o objetivo de proteger a versão original contra falhas de integridade ou de disponibilidade.

2.7. BATIC – Base de Ativos de TIC é a lista de ativos de TIC com suas características técnicas necessárias aos processos de gestão de vulnerabilidades e tratamento de incidentes de segurança da informação.

2.8. Catálogo de Serviços – Lista das tarefas que podem ser demandadas, contendo suas descrições, detalhamentos e níveis de serviço associados.

2.9. Certificações profissionais - processo negociado pelas representações dos setores sociais, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou na experiência de trabalho, com o objetivo de promover o acesso, permanência e progressão no mundo do trabalho e o prosseguimento ou

conclusão de estudos.
2.10. Checklist – lista de atividades a serem executadas rotineiramente, utilizada no controle da execução dos serviços e/ou na verificação da saúde do ambiente de TIC.
2.11. Cluster – conjunto de dois ou mais equipamentos, cada um denominado de nó, que trabalham em conjunto para executar uma mesma função. Os principais tipos de clusters são - cluster de alto desempenho, de alta disponibilidade (redundância) e de balanceamento de carga.
2.12. Comissionamento – processo avaliação que visa a assegurar que o elemento em análise foi projetado, instalado, testado, operado e mantido de acordo com as necessidades e requisitos operacionais.
2.13. Confidencialidade - propriedade de que a informação somente seja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados a acessá-la.
2.14. Console de CTI/DRP - Interface de consulta amigável para consumo das informações disponibilizadas pela CONTRATADA para o serviço de Inteligência de Ameaças Cibernéticas.
2.15. Contingência – situação que pode ser declarada pelo BNDES em casos de indisponibilidade de grande extensão de recursos de TI, pessoas ou localidade.
2.16. Data Center – Local onde estão concentrados os equipamentos de processamento e armazenamento de dados, também conhecido como Centro de Processamento de Dados (CPD).
2.17. Disponibilidade - propriedade da informação estar acessível e utilizável por uma pessoa física ou determinado sistema, órgão ou entidade, no momento em que for necessária.
DPO - De acordo com a LGPD, o encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". O encarregado é a figura conhecida como DPO (Data Protection Officer).
2.18. ETIR-BNDES - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação em Redes do BNDES;
Evento – é qualquer mudança no estado da infraestrutura, sistemas ou serviços de Tecnologia da Informação que tem importância para a gestão de determinado ativo de tecnologia da informação.
Evento de SI - Qualquer ocorrência identificada em um sistema de TIC, serviços providos e contratados, ou na Nuvem privada do BNDES, que indique possíveis falhas na aplicação da PCSI, ou das salvaguardas das informações processadas, armazenadas ou transmitidas, ou ainda, uma situação até então desconhecida, que possa se tornar relevante em termos de segurança cibernética.
Gestão de Segurança da Informação e Comunicações - ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.
Incidente – Interrupção não planejada ou potencial interrupção de um serviço de TIC ou redução de sua qualidade. A falha de um item de configuração que ainda não tenha prejudicado um serviço de TIC também é considerada um incidente.
Incidente de SI - Qualquer evento adverso, confirmado ou sob suspeita, que ameace os objetivos da Política Corporativa de Segurança da Informação (PCSI) do BNDES, tais como a tentativa de exploração de vulnerabilidade de um Sistema de TIC do BNDES; o acesso ou tentativa de acesso não autorizado a ativos de informação; ataques de negação de serviço; distribuição de software malicioso; etc.
Infraestrutura de tecnologia da informação e comunicação – Equipamentos, softwares, redes, instalações etc., que são requeridos para prover serviços de TIC.
Integridade - propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
Item de configuração (IC) – Identifica um elemento único da infraestrutura de serviços de TIC que deve ser controlado, em acordo com as melhores práticas definidas no ITIL.
ITIL (Information Technology Infrastructure Library) - conjunto de melhores práticas para gerenciamento de serviços de TIC.
Máquina virtual – computador implementado através de software que executa programas como um computador real.
Melhores práticas – Processos que têm sido utilizados com sucesso por muitas organizações para execução de atividades similares.
Monitoração – Observação continuada de um item de configuração (IC), serviço de TIC ou processo com o objetivo de detectar e registrar eventos e incidentes, além de conhecer seu estado operacional.
Níveis de serviço (NS) – Resultados esperados para as tarefas do Catálogo de Serviços normalmente atrelados a indicadores que permitam mensurar o grau de conformidade do resultado entregue com o resultado esperado.
Operação – Gerenciamento diário de um serviço de TIC, sistema ou outro item de configuração, compreendendo atividades tais como a atualização e configuração de software, assim como qualquer outra necessária ao funcionamento do serviço de acordo com as melhores práticas e os níveis de serviço definidos.
PCSI - Política Corporativa de Segurança da Informação do BNDES. É o documento aprovado pelo Conselho de Administração do BNDES, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

Playbook - Para os fins deste edital, entende-se playbook como o conjunto de ações necessárias para realizar o tratamento e a resposta a um determinado incidente de SI. Esse conjunto de ações deve ser o mais automatizado possível. O termo playbook, nesta especificação técnica, pode ser usado de forma intercambiável com runbook, a depender do contexto.
Problema – Investigação da causa-raiz de um ou mais incidentes.
Procedimento – Documento que contém os passos necessários à execução de uma atividade.
Quebra de segurança - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
Resolução – Ação tomada para eliminar a causa raiz de um incidente ou problema.
Segurança da Informação e Comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
Sistemas de TIC - Aplicativos, Aplicações (Web ou não), Softwares e Sistemas que são executados nos Ativos de TIC. São exemplos de Sistemas de TIC - Aplicações Web, Web Services, WebSocket, Aplicações em Contêineres, Gerenciadores de Repositórios de Imagens-Base de Contêineres, Contêineres e Gerenciadores de Contêineres, Bancos de Dados (BD) e Sistemas Gerenciadores de Banco de Dados (SGBD), Aplicações de Inteligência Artificial (Machine Learning, Deep Learning etc.), Aplicações Cliente-Servidor e Aplicativos desenvolvidos pelo, ou para o, BNDES para dispositivos móveis. Obs - Esta lista de sistemas não é exaustiva.
SOAR - Security Orchestration, Automation and Response é um sistema de TIC cujo objetivo é a orquestração, automação da execução, do enriquecimento e das respostas aos eventos e incidentes de segurança cibernética.
Software de Gerenciamento de Serviços de TIC ou ITSM (Information technology service management) – Software usado para gerenciar requisições de serviço, incidentes, problemas, mudanças, liberações e itens de configuração referentes aos serviços de TIC disponibilizados.
Solução da CONTRATADA – conjunto de hardwares e softwares, licenciados ou livres de licenciamento, empregados pela CONTRATADA, de sua propriedade ou contratados como serviço, para prover os serviços demandados pelo BNDES.
Sustentação – Conjunto de tarefas executadas conforme as melhores práticas, com o objetivo de manter um ativo de TIC operacional e de acordo com o nível de serviço estabelecido. A sustentação contempla a monitoração, a operação e a manutenção preventiva e corretiva.
Tarefa – Item do Catálogo de Serviços pertencente a um ou mais dos tipos de serviço que podem ser demandados pelo BNDES e que fazem parte do escopo do Contrato.
TIC – Tecnologia da Informação e Comunicação.
Tratamento da informação - recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.
TRD - Termo de Recebimento Definitivo.
TRP - Termo de Recebimento Provisório.
TTPs - São Táticas, Técnicas e Procedimentos utilizados por hackers, para explorarem vulnerabilidades em sistemas de TIC, em ativos (de TIC, de informação ou de localidade) ou em processos, de forma a alcançarem seus objetivos.

3. CONDIÇÕES GERAIS – ITENS I e II

3.1. Os serviços deverão ser prestados de acordo com as especificações, padrões técnicos de qualidade, desempenho, arquiteturais, processos, normas e plataforma tecnológica estabelecidos pelo BNDES e conforme condições, quantidades e exigências estabelecidas neste instrumento e seus anexos.
3.2. Todos os prazos nessa Especificação Técnica são definidos e contados em dias corridos e em horas corridas.
3.3. Toda a comunicação entre o BNDES e a CONTRATADA utilizará a língua portuguesa, como falada no Brasil.
3.4. A CONTRATADA apenas receberá as parcelas mensais após o aceite definitivo do respectivo serviço pelo BNDES, emissão do TRD, conforme condições do item 15.
3.5. Todas as soluções e/ou ferramentas utilizadas para prestação do serviço devem, obrigatoriamente, ser de propriedade ou licenciadas para a CONTRATADA, instaladas em sua versão mais estável e mantidas atualizadas durante toda a vigência do contrato (minor, major e patches), não serem modificadas ou adaptadas e devem estar cobertas por contratos de suporte e de atualização de versão do fabricante, durante toda a vigência do respectivo item de serviço.
3.6. A CONTRATADA deve garantir o serviço de assistência técnica/suporte da solução e/ou ferramentas utilizadas pela CONTRATADA, o qual deve prover, durante o prazo contratado:
3.6.1. Acesso, pelo BNDES, à base de conhecimento e fóruns no site do fabricante.
3.6.2. O serviço de assistência técnica poderá ser prestado de forma remota e, quando solicitado pelo BNDES, presencialmente nas instalações do BNDES (on-site).
3.6.3. Toda e qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de patches etc.) deverão ocorrer mediante autorização do BNDES.

3.6.3.1. O BNDES poderá, previamente, definir janelas de manutenção para a CONTRATADA executar as atividades de manutenção da solução empregada para prestação dos serviços ao BNDES como forma de agilizar o referido processo.
3.7. Caso a solução ou parte dela seja descontinuada pelo fabricante ou venha a apresentar alguma incompatibilidade técnica ou legal com sua aplicação no BNDES, esta deverá ser substituída, pela CONTRATADA, por solução equivalente, sem custo para o BNDES e mediante aprovação pelo BNDES.
3.8. É de responsabilidade da CONTRATADA a instalação e a configuração das ferramentas fornecidas no âmbito dos serviços que possuem essa previsão, inclusive suas integrações.
3.9. Caso a CONTRATADA seja a desenvolvedora e mantedora de algum software da solução empregada para prestação dos serviços, ficam mantidas todas as obrigações aplicáveis a softwares de mercado, atualizações de segurança etc. Entretanto, estas serão de responsabilidade da CONTRATADA como "fabricante" do software.
3.10. A CONTRATADA deve produzir e disponibilizar para o BNDES a documentação com os procedimentos, ações e detalhes técnicos das instalações e integrações.
3.11. A CONTRATADA será responsável pela aplicação de controles de segurança adequados (criptografia, gestão de acesso etc.) para garantir a confidencialidade de qualquer dado ou informação do BNDES que receber em seu ambiente ou em terceiro contratado por esta (plataforma SaaS, serviço de nuvem etc).
3.12. A solução para prestação da atividade de CSIRT, especificamente a ferramenta de SOAR, deverá ser instalada no ambiente do BNDES, de acordo com os requisitos de infraestrutura do item 7, de modo a manter os dados no ambiente do BNDES.
3.13. A solução para prestação das atividades de GVUL, especificamente o(s) scanner(s) de vulnerabilidades ou seu gateway, no caso de solução SaaS, e a base de ativos de TIC – BATIC (item 14.1.3.4) deverão ser instalados no ambiente do BNDES, de acordo com os requisitos de infraestrutura do item 7.
3.13.1. Caso a contratada opte pelo fornecimento da solução para gestão de vulnerabilidades na forma de serviço de computação em nuvem (SaaS) ou similar, o serviço deverá ser instalado em datacenter no Brasil, devendo observar os controles presentes na INSTRUÇÃO NORMATIVA nº 05 de 30 de agosto de 2021 do GSI/PR (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684).
3.14. Para prestação das demais atividades e para soluções complementares do ITEM I, a CONTRATADA poderá optar ou não pela instalação das soluções ou componentes na infraestrutura do BNDES, obedecendo os requisitos de infraestrutura do item 7, ou em seu ambiente próprio ou contratado conforme os requisitos abaixo.
3.14.1. Os demais itens (servidores, appliances software etc) necessários à prestação dos serviços previstos deverão ser instalados nos ambientes de datacenter da CONTRATADA no Brasil (item 14.1.1.4) ou em nuvem no Brasil e deverão observar os controles presentes na INSTRUÇÃO NORMATIVA nº 05 de 30 de agosto de 2021 do GSI/PR (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684).
3.15. Para prestação das atividades do ITEM II, a CONTRATADA poderá optar ou não pela instalação das soluções ou componentes na infraestrutura do BNDES, obedecendo os requisitos de infraestrutura do item 7, ou em seu ambiente próprio ou contratado em nuvem em qualquer localidade. Pois o ITEM II trata informações capturadas no ambiente público.
3.16. A CONTRATADA para o ITEM I deverá utilizar apenas infraestrutura de Tecnologia da Informação (TI) localizada em território nacional para armazenar e processar as informações manejadas no âmbito da prestação dos serviços, incluindo eventuais réplicas e cópias de segurança. Para o ITEM II não se aplicam as mesmas restrições, pois se tratam de informações capturadas no ambiente público.
3.16.1. Salvo em caso de necessidade de troubleshooting junto ao fabricante da solução onde deverão ser enviadas de forma anonimizada.
3.17. O BNDES e seus colaboradores deverão ter acessos individualizados e simultâneos, via usuário e senha próprios, no caso de colaboradores, para, no mínimo, 15 (quinze) usuários, a todas as ferramentas e consoles dos produtos ofertados pela(s) CONTRATADA(s) e utilizados durante a prestação dos serviços, bem como os perfis de acesso devem ser suficientes para execução e validação das funcionalidades ofertadas e utilizadas para prestação dos serviços, além do acompanhamento e auditoria das ações realizadas pela CONTRATADA.
3.17.1. Um ou mais acessos simultâneos devem ser disponibilizados via API, preferencialmente API REST, para integração aos demais processos do CSOC; e
3.17.2. O BNDES poderá solicitar a alteração de login e senha do acesso conforme a sua necessidade.
3.18. A SOLUÇÃO DA CONTRATADA deverá ser prover uma API REST, utilizando o protocolo HTTPS com TLS 1.2, com autenticação via (mínimo): chave/token, usuário e senha, certificado digital (autenticação mútua) ou outra composição definida pelo BNDES.
3.19. A CONTRATADA deverá possuir mecanismos para garantir os direitos e deveres previstos na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) como, por exemplo:

3.19.1. Disponibilizar acesso ao BNDES ou meio equivalente para apagar dados pessoais na solução da CONTRATADA ofertada para atendimento aos requisitos dos ITENS I e II.
3.20. A CONTRATADA deve oferecer ao BNDES capacitação suficiente para permitir a compreensão e a utilização eficaz dos recursos (controles) disponibilizados na solução que são necessários para atender requisitos de Segurança da Informação do BNDES.
3.21. Todos os feeds de informação utilizados para prestação do serviço deverão ser acessíveis pelo BNDES e, obrigatoriamente, mantidos em sua versão mais atual de acordo com a política do fornecedor da informação e/ou disponibilidade de novas informações sobre ameaças.
3.22. Se solicitado pelo BNDES, toda a comunicação entre os componentes da solução instalados no BNDES e instalados na CONTRATADA deve ser cifrada com algoritmos públicos, padrão de mercado, usando chaves fortes.
3.23. As características técnicas descritas para todos os equipamentos, dispositivos, materiais, softwares e serviços solicitados neste documento são as características mínimas que devem ser atendidas pelas Licitantes. Assim sendo, podem ser oferecidos quaisquer outros de desempenho equivalente ou superior, desde que compatíveis com os requisitos destas especificações.
3.24. Os colaboradores ou sistemas da CONTRATADA que necessitarem de acesso à infraestrutura do BNDES, terão acesso individualizado via usuário e senha próprios, no caso de colaboradores, sendo vedado o compartilhamento conforme a PCSI do BNDES. No caso de sistemas, estes deverão respeitar os requisitos de segurança da API da respectiva infraestrutura do BNDES que necessitarem de acesso. O BNDES avaliará a pertinência da necessidade de acesso e poderá negá-lo ou cancelá-lo ao qualquer momento.
3.25. A CONTRATADA deverá prover todas as ferramentas e componentes de hardware, softwares, licenciamentos e integrações necessários à integral execução e cumprimento dos serviços contratados, sem custos adicionais para o BNDES.
3.26. É responsabilidade da CONTRATADA gerenciar os recursos alocados ao Contrato de maneira a assegurar a disponibilidade dos serviços e a sua execução nos prazos previstos.
3.27. A CONTRATADA deve, quando solicitado pelo BNDES e sem ônus para o BNDES, realizar a remoção definitiva (de forma irrecuperável) de todas ou de parte das informações manejadas durante a prestação dos serviços, a critério do BNDES, que estejam armazenadas na infraestrutura do CONTRATADA ou na infraestrutura de terceiros utilizada pela CONTRATADA, fornecendo evidências da execução do pedido.
3.28. A CONTRATADA deve, quando solicitada pelo BNDES e sem ônus para o BNDES, providenciar a exportação das informações manejadas durante a prestação dos serviços que estejam armazenadas na infraestrutura da CONTRATADA ou na infraestrutura de terceiros utilizada pela CONTRATADA, a fim de permitir a migração para outros prestadores de serviço, conforme detalhado no item 22.
3.29. Se solicitado pelo BNDES, a SOLUÇÃO DA CONTRATADA deve armazenar os dados corporativos do BNDES (em repouso) com a utilização de criptografia, sem que isso inviabilize a utilização dos serviços contratados, a fim de mitigar o risco de acesso indevido por terceiros não-autorizados.
3.29.1. As informações devem ser cifradas através da utilização de algoritmos criptográficos considerados fortes, que sejam de domínio público e que estejam especificados em um padrão FIPS (Federal Information Processing Standards) vigente ou em uma recomendação, atual e de cunho específico, do NIST (National Institute of Standards and Technology), dando preferência para a utilização de chaves criptográficas assimétricas para proteger chaves simétricas utilizadas neste processo.
3.30. A CONTRATADA deverá observar os normativos do Gabinete de Segurança Institucional da Presidência da República (GSI - https://www.gov.br/gsi/pt-br/ssic/legislacao) e do Banco Central do Brasil (Resolução CMN n° 4.893 de 26/2/2021) na prestação dos serviços.
3.31. Todos os prazos estabelecidos nestas Especificações Técnicas poderão ser prorrogados, pelo Gestor do Contrato, a critério do BNDES, se devidamente justificados pela CONTRATADA e se não causarem prejuízo ao BNDES.
3.32. A CONTRATADA é responsável por assegurar a preservação da confidencialidade, da integridade e da disponibilidade das informações do BNDES manejadas no âmbito da prestação dos serviços contratados.
3.33. A SOLUÇÃO DA CONTRATADA deve viabilizar o acesso aos serviços da plataforma por meio de HTTP sobre Tranport Layer Security (TLS) versão 1.2 ou superior (HTTPS).
3.33.1. A CONTRATADA deverá estabelecer rede dedicada e/ou VPN específica entre a infraestrutura do BNDES e a infraestrutura da CONTRATADA, conforme item 9, para troca de dados entre componentes da solução e acesso à solução instalada pela CONTRATADA para prestação dos serviços.
3.34. A SOLUÇÃO DA CONTRATADA deve dispor de certificado emitido por Autoridade Certificadora (AC) nativamente reconhecida como confiável pelos principais navegadores na Internet.
3.35. A SOLUÇÃO DA CONTRATADA deve dispor de controle para mitigar a realização de ataques automatizados de força-bruta ou adivinhação de senhas, como por exemplo utilizar CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart).
3.36. A SOLUÇÃO DA CONTRATADA deve permitir a utilização de múltiplos fatores de autenticação (multi-factor authentication), doravante chamado de “MFA”, para acesso à solução.
3.37. O BNDES poderá demandar que a SOLUÇÃO DA CONTRATADA utilize a autenticação de usuários

e autorização federadas, integradas com o repositório corporativo de credenciais de acesso do BNDES (Azure Active Directory) por meio de protocolos abertos como SAML ou OAuth2 com OpenID.
3.37.1. Deve possuir controle de acesso baseado no modelo RBAC (Role Based Access Control) para os acessos aos consoles web da solução.
3.37.2. Deve ser capaz de realizar a autorização de acessos de usuários utilizando de vinculação de usuários a papéis, obtidos do diretório corporativo (grupos) ou de uma base de autorização local à solução.
3.38. A SOLUÇÃO DA CONTRATADA deve identificar automaticamente, por meio de heurísticas e de análise comportamental, indícios do comprometimento e do uso indevido de credenciais de acesso à solução.
3.39. A SOLUÇÃO DA CONTRATADA deve assegurar que a indicação da data e da hora seja realizada por padrão no fuso Universal Time Coordinated (UTC) e esteja sincronizada com fontes confiáveis de tempo.
3.40. Quanto os registros de auditoria, a SOLUÇÃO DA CONTRATADA também deve observar os seguintes aspectos:
3.40.1. Manter registros de endereços IP e usuários que acessaram ou tentaram acesso;
3.40.2. Possuir uma API para permitir o acesso aos registros de auditoria ou a capacidade de exportar os registros de auditoria de forma periódica.
3.41. A SOLUÇÃO DA CONTRATADA deve realizar a retenção dos dados referentes aos serviços prestados ao BNDES, de forma online para uso pelo BNDES, por, no mínimo, 12 meses. A sobrescrita dos dados deverá ocorrer de forma circular a partir do 13º mês. Caso demandado pelo BNDES, a CONTRATADA deverá exportar os dados antes do início da rotação dos dados retidos.
3.42. A SOLUÇÃO DA CONTRATADA, instalada no ambiente do BNDES, deverá ser configurada para permitir a coleta de dados de desempenho e disponibilidade pelo software de monitoramento Zabbix, versão 5.4.9 e superioras, adotado e implantado na infraestrutura do BNDES, além do envio de notificações e alarmes (traps SNMP).
3.43. A CONTRATADA deverá monitorar, analisar e controlar o desempenho de cada software especializado fornecido, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes das soluções.
3.44. A CONTRATADA deve facultar ao Banco Central do Brasil (BACEN) o acesso aos contratos e aos acordos firmados com o BNDES para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre o seu processamento, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.
3.45. Em caso da decretação de regime de resolução do BNDES pelo Banco Central do Brasil (BACEN), a CONTRATADA deve conceder acesso pleno e irrestrito do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da SOLUÇÃO CONTRATADA; além de observar os demais requisitos aplicáveis e dispostos na regulamentação do Banco Central do Brasil que trata da contratação de serviços de processamento e armazenamento de dados e de computação em nuvem em vigor (atualmente a Resolução nº 4.893, de 26 de fevereiro de 2021).
3.46. A CONTRATADA deve dispor de processo(s) de gestão de mudança, sobretudo no tocante à implantação, atualização e manutenção dos recursos utilizados na prestação dos serviços para o BNDES, a fim de evitar impacto à disponibilidade dos serviços contratados.
3.47. A CONTRATADA deverá interagir com todas as ferramentas do BNDES e processos de trabalho necessárias a completa execução dos fluxos de trabalho estabelecidos, bem como a operacionalização dos processos inerentes aos serviços contratados, sem custos adicionais para o BNDES. O ambiente está descrito no item 8.2.
3.47.1. O tipo de interação dependerá da ferramenta e da atividade. Exemplo: operar o SIEM vai exigir que um profissional interaja com sua console gráfica, enquanto o registro de um ticket no Remedy e/ou RT vai exigir interação via API etc. Os tipos de interações estão descritos ao longo do documento.
3.48. Caso haja a possibilidade de integração ou automação de algum processo a partir das soluções da CONTRATADA e/ou entre as soluções da CONTRATADA e do BNDES, esse não deverá gerar custos adicionais para o BNDES, bem como deverá ser implementada se demandada e autorizada pelo BNDES.
3.49. Todos os serviços e soluções ofertados deverão estar protegidos contra intrusão e acesso indevido;
3.50. Todos os serviços e soluções deverão ser configurados de forma que a falha de um dos equipamentos ou rede isoladamente NÃO interrompa a prestação dos serviços;
3.51. A CONTRATADA deve ter em seu datacenter ou provedor de serviço, componentes de segurança necessários à integral recuperação dos dados do BNDES em caso de ocorrência de incidentes cibernéticos de qualquer natureza;
3.52. A CONTRATADA deve ter em seu datacenter ou provedor de serviço, componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e a execução de plano de recuperação de catástrofes;
3.53. A CONTRATADA deverá possuir processos implementados que garantam a segurança das informações do BNDES, em conformidade com a norma ABNT NBR ISO/IEC 27001.
3.54. A CONTRATADA será responsável pela aplicação de controles de segurança adequados, como

criptografia e rotinas de backup, para garantir a confidencialidade, integridade e disponibilidade de qualquer dado ou informação do BNDES que receber em seu ambiente ou em terceiro contratado.
3.55. A CONTRATADA deverá comunicar formalmente o BNDES sempre que identificar algum serviço com falhas de implementação, erro, degradação de performance, perda ou corrupção de dados da CONTRATADA ou qualquer outro cenário que afete os pilares de confidencialidade, integridade e disponibilidade.
3.56. Quando solicitado pelo BNDES, a CONTRATADA deverá demonstrar anualmente a segurança da infraestrutura de TIC que suporta a prestação dos serviços, através de ao menos uma das opções abaixo:
3.56.1. Evidência de execução de teste de invasão, por empresa especializada, em seus elementos de infraestrutura ou documento que comprove a ocorrência dessa contratação.
3.56.2. Evidência de execução de varreduras de vulnerabilidades de segurança e de aplicação de patches de segurança em seus elementos de infraestrutura ou documento que comprove a ocorrência dessa contratação.
3.56.3. Relatório de auditoria de firma especializada e reconhecida, que não faça parte do grupo econômico da CONTRATADA, atestando os processos de segurança necessários para os elementos de infraestrutura de TIC que suportam a prestação dos serviços em relatórios de auditoria compatíveis com SAS70 tipo II, SSAE 18 SOC2, ISAE3402 ou similares, aceitos pelo BNDES.
3.57. Quando solicitado pelo BNDES, a CONTRATADA deverá demonstrar que realiza testes de segurança em novas versões dos softwares que são parte integrante da SOLUÇÃO DA CONTRATADA.
3.58. A CONTRATADA deve garantir que existem registros de auditoria (logs, imagens etc) para todos os acessos realizados à infraestrutura de TIC física, definida no item 14.1.1.8, e lógica que suporta a prestação dos serviços, com vistas a suportar o processo de tratamento de incidentes de segurança da informação. Esses registros deverão ser fornecidos ao BNDES quando solicitado e em formato que permita o BNDES analisá-los.
3.58.1. A CONTRATADA deve garantir que os componentes que suportam a prestação dos serviços executam em ambiente abrangido por:
3.58.1.1. Políticas e procedimentos destinados ao efetivo e eficaz tratamento de incidentes de segurança da informação.
3.58.1.2. Políticas e procedimentos destinados à efetiva execução de processos de realização e restauração de cópias de segurança dos dados.
3.58.1.3. Política de continuidade de negócio para a infraestrutura de TIC.
3.58.1.4. Boas práticas de segurança da informação, evidenciadas através de uma política corporativa de segurança da informação aprovada e implantada, com a publicação de seus termos de uso aceitáveis (Acceptable Use Policy) ou por meio de certificações de entidades reconhecidas pelo mercado para esta finalidade.
3.59. A SOLUÇÃO DA CONTRATADA deverá prover consoles web de administração e uso compatíveis com HTML 5.
3.59.1. Todos os consoles web da aplicação devem ser acessados através do protocolo seguro HTTPS.
3.59.2. Os consoles web de administração e uso da solução devem prover acesso a todas as funcionalidades do produto.
3.59.3. Os consoles web de administração e uso da solução não poderão depender de tecnologias ou componentes que tenham sido descontinuados por seus fabricantes, como, por exemplo, o Adobe Flash Player, para executar suas funcionalidades, em parte ou em todo.
3.59.4. Os consoles web de administração e uso da solução devem ser compatíveis com os navegadores de Internet, de 64 bits, Google Chrome, versão 122 e superiores e Microsoft Edge, versão 122 e superiores, quando executados em uma estação de trabalho Windows 10 Pro e superior.
3.60. As equipes da CONTRATADA e ferramentas/processos devem interagir com as equipes de suporte de TI e com ETIR do BNDES pelos meios definidos pelo BNDES, conforme item 16.1.2.
3.61. Todos os relatórios e/ou entregáveis previstos nesta Especificação Técnica poderão ter seu conteúdo ajustado por demanda do BNDES, para melhor aproveitamento dos serviços e informações disponibilizadas pela solução disponibilizada pela CONTRATADA.
3.62. Todos os frameworks e padrões de segurança citados nesta Especificação Técnica devem ser seguidos considerando sua última versão e só podem ser trocados por outros similares e/ou por outra versão se aprovado pelo BNDES. Portanto, por exemplo, frameworks/padrões como MITRE ATT&CK e CIS-Control só podem ser substituídos com anuência da BNDES, o mesmo para versões como do NIST CSF 1.1 para o CSF 2.0.
3.63. O BNDES poderá promover, a qualquer tempo, diligência nas instalações da CONTRATADA para checar a veracidade das informações e para confrontação com os requisitos desta Especificação Técnica.
3.64. Todas as atividades que envolverem autorização ou alguma outra definição do BNDES poderão ser previamente definidas, pelo BNDES, para agilidade do processo, podendo ser dispensada a autorização ou definição a cada interação.
3.65. Qualquer alteração na SOLUÇÃO DA CONTRATADA, instalada ou não no ambiente do BNDES, após a emissão do TRD, deverá ser comunicada previamente ao BNDES e só poderá ocorrer mediante aprovação pela BNDES.

4. REQUISITOS PARA A EQUIPE PRESTADORA DOS SERVIÇOS – ITENS I e II

4.1. As equipes deverão ser dimensionadas pela empresa CONTRATADA de forma a atender as demandas de acordo com os níveis mínimos de serviço exigidos no item 18 (24x7). Para tanto, salienta-se que a responsabilidade de formação da equipe de profissionais é exclusiva da empresa CONTRATADA.

4.2. A CONTRATADA deverá comprovar a qualificação da equipe correspondente ao ITEM de serviço apresentando:

4.2.1. Para as certificações técnicas, cópia do certificado de treinamento ou comprovação da certificação em questão pelos meios disponibilizados pela instituição certificadora. A certificação, se possuir data de expiração, não poderá estar expirada;

4.2.2. Para o vínculo com a CONTRATADA, serão aceitos como documentos: Carteira de Trabalho e Previdência Social, Contrato Social em que conste como Sócio ou Diretor, ou contrato de prestação de serviços.

4.3. No mínimo, a equipe técnica da CONTRATADA envolvida com a prestação dos serviços previstos no ITEM I deverá possuir, em conjunto, as seguintes certificações válidas:

4.3.1. Duas das certificações a seguir: Certificação CompTIA Security+ ou equivalente de Segurança de Redes; Certificação CEH (Certified Ethical Hacker) ou equivalente de Segurança no Desenvolvimento de Software; Certificação GCIH - GIAC (Certified Incident Handler) ou equivalente para Tratamento de Incidentes de Segurança Computacional; Certificação CHFI (Certified Hacking Forensic Investigator) ou equivalente de Forense Computacional; Certificação CISM (Certified Information Security Manager) ou equivalente de Gestão da Segurança da Informação, todas conforme definido na Norma Complementar 17 da Instrução Normativa GSI Nº01 de 13 de junho de 2008;

4.3.2. Certificação AZ-500: Microsoft Azure Security Technologies (Microsoft) ou equivalente para operação das consoles de segurança do Microsoft 365;

4.3.3. Certificação IBM Certified SOC Analyst - QRadar SIEM V7.5 Plus CompTIA Cybersecurity Analyst ou equivalente para operação da plataforma de SIEM do BNDES; e

4.3.4. Certificação no nível de especialista (expert) nos produtos adotados para prestação dos serviços (GVUL, SOAR etc). Exemplos de certificações: Tenable Vulnerability Management Specialist, InsightVM Certified Administrator, Splunk SOAR Certified Automation Developer, Nexpose Advanced Certified Administrator etc.

4.3.4.1. A lista de certificações acima é meramente exemplificativa e não vincula a CONTRATADA a utilizar nenhum dos produtos citados.

4.3.4.2. Caso um ou mais produtos sejam desenvolvidos integralmente pela CONTRATADA, sendo tal fato devidamente comprovado pela CONTRATADA, fica dispensada essa exigência para o respectivo produto.

4.4. No mínimo, a equipe da CONTRATADA envolvida com a prestação dos serviços previstos no ITEM II deverá possuir uma das seguintes certificações:

4.4.1. Certificação CISM (Certified Information Security Manager) ou equivalente de Gestão da Segurança da Informação conforme definido na Norma Complementar 17 da Instrução Normativa GSI Nº01 de 13 de junho de 2008; ou

4.4.2. Certificação CEH (Certified Ethical Hacker) ou equivalente de Segurança no Desenvolvimento de Software conforme definido na Norma Complementar 17 da Instrução Normativa GSI Nº01 de 13 de junho de 2008.

4.5. Para ambos os ITENS, além do preposto administrativo, deverá ser constituído um preposto técnico que deverá possuir, no mínimo, as certificações abaixo:

4.5.1. Certificação CISM (Certified Information Security Manager) ou equivalente de Gestão da Segurança da Informação conforme definido na Norma Complementar 17 da Instrução Normativa GSI Nº01 de 13 de junho de 2008.

4.5.2. ITIL - Suporte e Análise Operacional (OSA) ou equivalente.

4.6. A função de preposto técnico e administrativo não poderá ser exercida pela mesma pessoa.

4.7. Caso a mesma empresa seja a prestadora de ambos os ITENS, será necessário apenas um preposto técnico e um preposto administrativo.

4.8. Caso o GSI/PR (Gabinete de Segurança Institucional da Presidência da República - https://www.gov.br/gsi/pt-br/ssic/legislacao) venha a atualizar as certificações recomendadas, caberá a CONTRATADA atualizar a formação dos técnicos envolvidos na prestação dos serviços.

4.9. A equipe qualificada deverá estar disponível durante todo o período de prestação dos serviços, conforme previsto no item 16.

4.10. A CONTRATADA deverá promover, no prazo máximo de 90 (noventa) dias, a atualização das certificações de seus profissionais caso haja expiração, atualização de versão ou migração para uma nova solução de TIC devido à modernização do ambiente tecnológico do BNDES e/ou da CONTRATADA. No caso de nova solução de TIC, este prazo se iniciará a partir da comunicação pelo BNDES à CONTRATADA.

4.10.1. Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior; e

4.11. A CONTRATADA deverá manter a sua equipe devidamente certificada durante toda a vigência do contrato.

4.12. Não existe restrição ou limite para acúmulo de certificações em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos para cada serviço.
4.13. Durante a vigência contratual e a qualquer tempo, os profissionais da CONTRATADA serão avaliados pelo BNDES, a qual poderá solicitar a substituição destes, caso não estejam correspondendo às necessidades e requisitos para cada perfil. Esta substituição deverá ocorrer em até 15 (quinze) dias, contados a partir da notificação por parte do BNDES.
4.13.1. Todos os profissionais que compõem a equipe devem prestar os seus serviços em instalações privadas da CONTRATADA sediadas no país. Em situações excepcionais e de interesse do BNDES, o BNDES poderá permitir a prestação do serviço por profissional em localidade diversa das privadas da CONTRATADA.
4.14. A CONTRATADA deverá promover o repasse de conhecimento aos seus novos profissionais, em caso de substituição dos responsáveis pela execução de serviços em andamento, sem prejuízo à continuidade e à qualidade dos serviços.
4.15. A CONTRATADA deverá disponibilizar a todos os seus profissionais que prestarão os serviços contratados:
4.15.1. A Política Corporativa de Segurança da Informação (PCSI) do BNDES;
4.15.2. As cláusulas e as especificações do Contrato de prestação de serviços; e
4.15.3. Demais procedimentos e roteiros operacionais disponibilizados pelo BNDES para execução dos serviços.
4.16. A CONTRATADA deverá enviar ao Gestor do Contrato, em até 30 (trinta) dias após o início da prestação dos serviços pelo profissional, uma declaração de que ele tomou ciência e sanou eventuais dúvidas sobre os tópicos descritos no item 4.15.

5. UNIDADES FUNCIONAIS DO BNDES – ITENS I e II

5.1. Os escritórios do BNDES listados na tabela abaixo serão denominados, doravante, para simplificar, como Unidades do BNDES (individualmente ou em conjunto).

Unidades BNDES
A. Rio de Janeiro (*datacenter* principal e prédio administrativo) **DC1 –** Datacenter principal do BNDES **EDSERJ** - Edifício de Serviços do BNDES Avenida República do Chile 100 Centro - CEP: 20031-917 - Rio de Janeiro – RJ
B. Rio de Janeiro (*datacenter* alternativo e sala de crise) **DC2 –** Datacenter alternativo do BNDES Rio de Janeiro - RJ Estr. dos Bandeirantes, 10.916 Vargem Pequena – CEP 22783-111 - Rio de Janeiro - RJ
C. São Paulo (escritório regional) Av. Presidente Juscelino Kubitsheck 510, 5º andar Vila Nova Conceição - CEP: 04543-906 - São Paulo – SP
D. Brasília (escritório regional) Centro Empresarial Parque Cidade SCS B, Quadra 09, Lote C, Torre C, 12° andar Setor Comercial Sul - CEP: 70308-200 - Brasília – DF
E. Recife (escritório regional) Centro Empresarial Queiroz Galvão Rua Padre Carapuceiro 858, Torre Cícero Dias, 18º e 19º andar Boa Viagem - CEP: 51020-280 - Recife – PE

5.2. Durante a vigência do contrato, o BNDES poderá mover os componentes objeto do serviço entre as suas unidades sem prejuízo ao serviço prestado por cada CONTRATADA.
5.3. Em relação às localidades listadas, poderá haver alteração de endereço dentro do mesmo município durante a vigência do contrato, devendo ser mantidas as obrigações da CONTRATADA listadas nestas especificações técnicas, sem custos adicionais para o BNDES.

6. CASOS DE USO SIEM – ITEM I

6.1. A lista de casos de uso já definidos para início do serviço da CONTRATADA são:
6.1.1. Viagens impossíveis / account takeover.
6.1.2. Tentativa de uso de conta bloqueada ou desabilitada.
6.1.3. Tentativas de quebra de credenciais por força-bruta.
6.1.4. Campanhas de phishing (tentativas e bem-sucedidas).
6.1.5. Ataques de ransomware.
6.1.6. Usos atípicos de DNS (como detectar o uso de domain generation algorithms – DGAs – para comunicação com redes de C&C de botnets).
6.1.7. Acessos a sites de Internet considerados maliciosos.
6.1.8. Conexões e tentativas de conexão suspeitas para a infraestrutura do BNDES, como varreduras de rede e acessos cujos endereços de origem estejam contidos em feeds (de inteligência ou de ameaças) ou watchlists, por exemplo.
6.1.9. Conexões suspeitas saindo da infraestrutura do BNDES.
6.1.10. Movimentação lateral de ameaças.
6.1.11. Padrões de comunicação (de rede e de processos) associados a malwares.
6.1.12. Problemas com o sistema de proteção das estações de trabalho (antivírus), como proteção desativada ou vacinas desatualizadas.
6.1.13. Vazamento de informações.
6.1.14. Abuso de acesso privilegiado no acesso a locais contendo dados sensíveis.
6.1.15. Acesso a dados privilegiados a partir de origens não usuais.
6.1.16. Negação de serviço, distribuída ou não.

7. REQUISITOS PARA INFRAESTRUTURA DA CONTRATADA – ITENS I e II

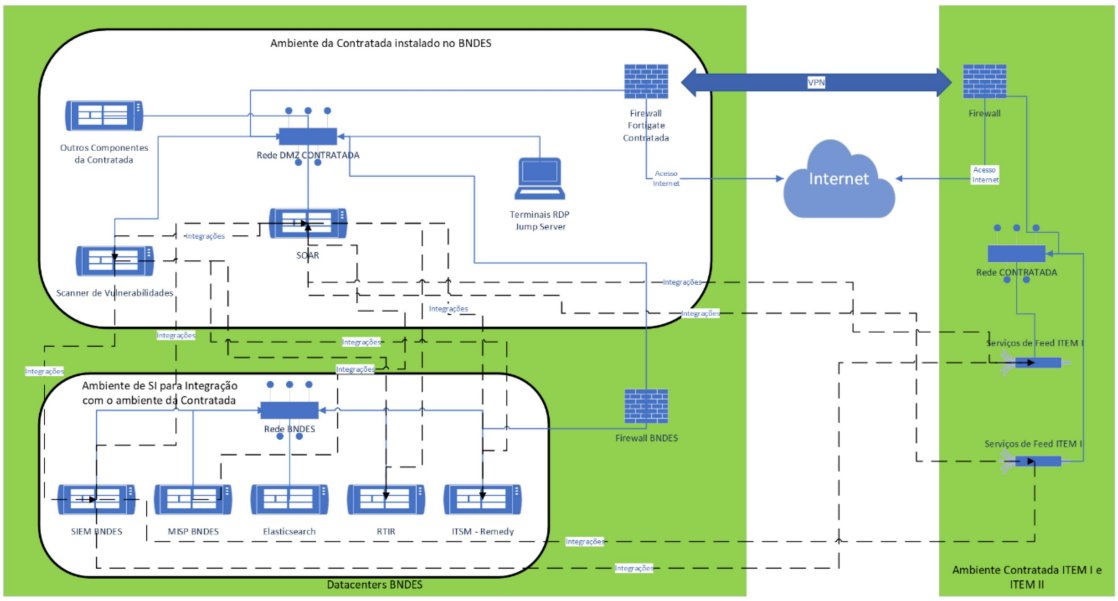
7.1. O BNDES fornecerá o ambiente datacenter com racks, energia elétrica, refrigeração e rede LAN, para hospedagem da infraestrutura da CONTRATADA instalada on premises, conforme requisito dos itens 3.12, 3.13, 3.14 e 3.15. Entretanto, os ativos da CONTRATADA deverão cumprir os seguintes requisitos:
7.1.1. Alimentação redundante utilizando duas linhas de fornecimento de energia elétrica de forma que a solução continue em operação em caso de falha do fornecimento de energia em uma das linhas. Cada linha de alimentação do datacenter irá fornecer no máximo 2 kW, com configuração de circuitos bifásicos (2 fases + neutro + terra), com frequência de 60Hz, diferença de tensão de 220V entre fases e utilizando tomadas do tipo C14, com capacidade de suportar, no mínimo, 10A.
7.1.2. O consumo por rack não poderá ultrapassar 2 (dois) kW.
7.1.3. O peso máximo deverá ser de, no máximo, 300 kg.
7.1.4. Possuir estrutura para instalação em rack de 19'' aberto e fechado (padrão EIA-310-D), sendo que deverão ser fornecidos os respectivos kits de fixação para rack ou deverão possuir abas de fixação já integradas ao próprio corpo do equipamento. Os bastidores (racks) e cabeados serão fornecidos pelo BNDES e seguem o padrão de 19 polegadas (norma EIA-310-D).
7.1.5. A refrigeração a ar deve possuir exaustão do ar quente pela parte traseira e admissão pela parte frontal (refrigeração front to back). Se a exaustão for feita pelo topo ou lateral, deverão ser fornecidos e instalados, pela CONTRATADA, os rebatedores e os acessórios necessários para preservar a segregação de corredores quentes e frios do CPD do BNDES.
7.1.6. Deve operar entre 18°C e 32°C.
7.1.7. No caso de servidores, deverão possuir placa de gerência remota no hardware (Integrated Lights-Out (iLO), Integrated Dell Remote Access Controller (iDRAC) etc).
7.1.8. Rede de dados utilizando duas conexões físicas de forma que a solução continue em operação em caso de falha em uma das conexões físicas. Deverá apresentar, no mínimo, 2 (duas) interfaces de conexão de rede local (LAN) metálica (RJ45 de 1 Gbps) ou óptica (LC Duplex de 1 ou 10 Gbps).
7.1.9. Todos os demais endereços IP/NATs a serem utilizados pela CONTRATADA deverão ser previamente aprovados pelo BNDES, a fim de evitar possíveis conflitos com endereços IP já utilizados em suas redes locais.
7.1.10. Deverão ser fornecidos todos os dados de acesso e configuração para monitoração dos ativos da CONTRATADA instalados no BNDES como, por exemplo, comunidade SNMP com as MIBs etc.

8. INFRAESTRUTURA DO BNDES – ITENS I e II

8.1. A infraestrutura relevante para o início dos serviços.
8.1.1. Infraestrutura de estações de trabalho (notebooks e desktops) é composta por, aproximadamente, 4.000 (quatro mil) estações de trabalho (notebooks e desktops), executando o sistema operacional Windows 10 64 bits e versões superiores e Microsoft Defender for Endpoint Plan 2.
8.1.2. Infraestrutura de servidores Windows, composta por, aproximadamente, 300 (trezentos) servidores Windows Server físicos e/ou virtuais, executando o sistema operacional Windows Server 2003 (3), 2008 (21), 2012 (21), 2016 (169), 2019 (98) 64 bits e versões superiores e Symantec Endpoint Protection (SEP), versão 14 ou superior.

8.1.3. Infraestrutura de servidores Linux composta por, aproximadamente 650 (seiscentos e cinquenta) servidores Linux físicos e/ou virtuais, executado o sistema operacional Red Hat Linux 5 (12), 6 (12), 7 (488), 8 (146) de 64 bits e versões superiores.
8.1.4. Infraestrutura de virtualização composta por, aproximadamente, 150 (cento e cinquenta) servidores VMware ESXi executando a versão 7 ou superiores. Devem ser considerados 2 servidores VMware vCenter.
8.1.5. Infraestrutura de containers Docker com, aproximadamente, 650 imagens e 8000 tags/versões diferentes no registry; e, aproximadamente, 2000 containers ativos em nosso ambiente de infraestrutura de containers (swarm/standalone/okd).
8.1.6. Servidores Apache HTTPD, IBM IHS, IBM WebSphere, SAP ERP etc.
8.1.7. Servidores de Banco de Dados SQL Server, Oracle, MySQL etc.
8.1.8. A infraestrutura de telefonia e videoconferência do BNDES é o Microsoft Teams em nuvem com terminais VoIP Yealink T29G.
8.1.9. Licenças de nuvem da Microsoft em uso no BNDES:
8.1.9.1. Microsoft 365 E5 ("Microsoft M365E5 Full USL Unified Shared ALNG Monthlysub PerUsr"), licenciado para 3.500 (três mil e quinhentos) usuários.
8.1.9.2. Microsoft Common Area Phone ("Microsoft CommonAreaPhone ShrdSvr AllLng MontrlhySubscriptions-VolumeLicense MVL 1License PerDvc"), licenciado para 600 (seiscentos) dispositivos.
8.1.10. Infraestrutura de proxies web do BNDES é composta de servidores executando a solução Secure Web Gateway da SkyHigh.
8.1.11. Infraestrutura de CFTV IP Hikvision com 6 (seis) gravadores e 166 (cento e sessenta e seis) câmeras;
8.1.12. Infraestrutura de controle de acesso IP Avigilon com 3 (três) servidores de gerência e, aproximadamente, 80 controladoras de porta modelo Mercury EP1501;
8.1.13. Infraestrutura de armazenamento com 2 (dois) Huawei/OceanStor Dorado 6000 V6, 4 (quatro) comutadores SAN DCX8510-4, 3 (três) Storwize v3700, 2 (dois) VNX5600, 2 (dois) Hitachi/VSP5x00, 2 (dois) IBM/FS5035, 1 (um) VTS TS7760 e 1 (uma) fitoteca TS3500;
8.1.14. Infraestrutura de mainframe composta por 2 (dois) IBM Mainframe z14;
8.1.15. Infraestrutura da infraestrutura de telecomunicações:
8.1.15.1.265 (duzentos e sessenta e cinco) switches de borda dos fabricantes Aruba, TP-Link e Juniper com solução de autenticação e gerência;
8.1.15.2.10 (dez) switches de chassi Huawei série CE12800S com solução de gerência;
8.1.15.3.23 (vinte e três) roteadores dos fabricantes Cisco e Juniper;
8.1.15.4.4 (quatro) acessos à Internet de 4 Gbps;
8.1.15.5.1 (um) cluster de firewalls virtuais Fortinet FortiGate-VM e 3 (três) firewalls virtuais Fortinet FortiGate-VM;
8.1.15.6.2 (dois) appliances analisadores de log Fortinet FortiAnalyzer-VM64;
8.1.15.7.2 (dois) appliances de gerenciamento Fortinet FortiManager-VM64;
8.1.15.8.4 (quatro) firewalls Open Source pfSense;
8.1.15.9.3 (três) appliances F5 BIG-IP Best Bundle;
8.1.15.10. 260 (duzentos e sessenta) Access-Points modelo Aruba AP-555 com solução de autenticação e gerência;
8.1.15.11. 40 (quarenta) appliances virtuais.
8.1.16. Infraestrutura da infraestrutura de alimentação elétrica composta por 450 PDUs modelos Emerson Network Power MPI Intelligent PDU System e MP-EHCNHA08N00X e 250 LTS modelos Emerson Network Power UF-LTS16-1P e Liebert LTS 16A;
8.1.17. Durante a vigência do contrato, o BNDES poderá alterar os quantitativos e modelos dos componentes acima descritos sem prejuízo ao serviço prestado por cada CONTRATADA, devendo ser mantidas as obrigações da CONTRATADA listadas nestas especificações técnicas, sem custos adicionais para o BNDES.
8.2. A infraestrutura do BNDES relevante para a execução dos serviços de SI pela CONTRATADA (monitoramento de eventos e incidentes de segurança da informação, logs, ITSM etc), todos on-premises, é composta por:
8.2.1. Que deverão ser operados e integrados à solução da(s) CONTRATADA(S) de acordo com o ITEM de prestação de serviços:
8.2.1.1. SIEM (Security Information and Event Management - IBM Q-Radar 7.5 UpdatePackage 6) com volume máximo de 4.200 (quatro mil e duzentos) eventos (EPS) e 85.000 (oitenta e cinco mil) fluxos (FPM) com a opções Offenses e Network Activity e os plug-ins Platform Configuration, QRadar Log Source Management, Pulse – Dashboard, QRadar Assistant, QRadar Use Case Manager, Reference Data Management, Deployment Intelligence, User Analytics e Machine Learning Analytics.
8.2.1.2. MISP (Malware Information Sharing Platform - www.misp-project.org/) para compartilhamento de informações de ameaças (IoCs - Indicators of Compromise); e
8.2.1.3. Consoles de segurança da plataforma Microsoft 365 (Defender Portal, atualmente, security.microsoft.com).

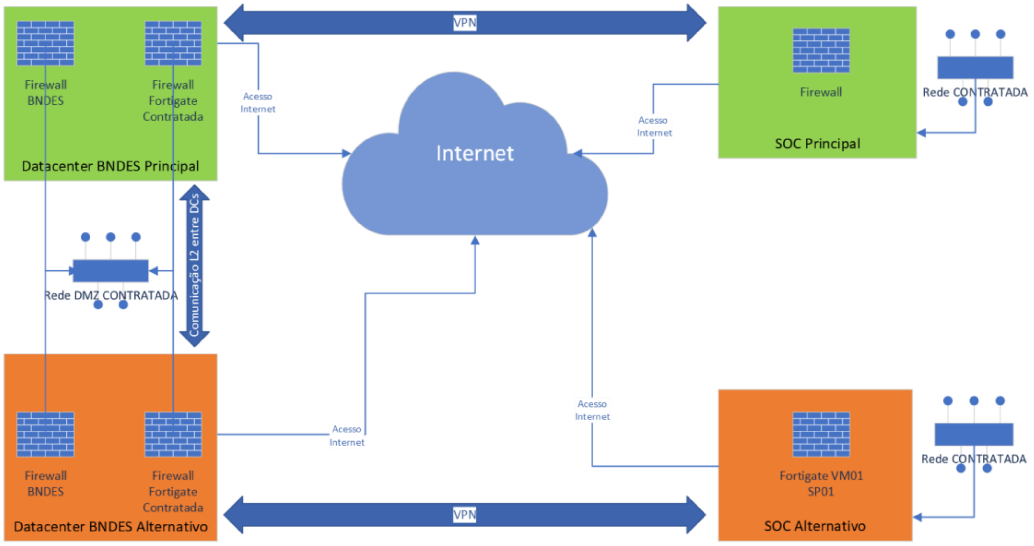
8.2.2. Que deverão ser consultados e integrados à solução da CONTRATADA de acordo com o ITEM de prestação de serviços:
8.2.2.1. Stack ELK (ElasticSearch, Linux e Kibana), com ElasticSearch v7.17 ou superior, com picos de 200 (duzentos e cinquenta) Gigabytes de logs por dia;
8.2.2.2. RTIR (Request Tracker for Incident Response - bestpractical.com/rtir) para controle de tickets de eventos de segurança;
8.2.2.3. ITSM (IT Service Management - BMC Remedy) para controle de tickets direcionados para as equipes de sustentação de TIC; e
8.2.2.4. SAP Identity Manager (IdM); e
8.2.2.5. Microsoft Active Directory (AD).
8.2.3. Exemplo de esquema de comunicação para consulta e integração.
8.2.3.1. Todos os fluxos de comunicação entre o ambiente do BNDES e a solução da CONTRATADA, inclusive o acesso de seus colaboradores, deverão ocorrer pela rede dedicada e/ou pelos túneis VPN, conforme item 9.
8.2.3.2. O acesso pelos colaboradores da CONTRATADA ao tenant do BNDES na plataforma Microsoft 365 será realizado diretamente a partir das instalações da CONTRATADA que terá um conjunto de endereços IP autorizados.
8.2.3.3. No caso do uso de gateway para uma solução SaaS de gestão de vulnerabilidades, por exemplo, o BNDES poderá autorizar a comunicação do gateway diretamente com a nuvem da solução SaaS, sem utilizar a rede dedicada e/ou túneis VPN, especificados no item 9, desde que possam ser definidos o endereço IP ou um pequeno conjunto de endereços IP (/24) e porta(s) autorizados a se comunicar com o gateway.



9. REQUISITOS DE CONECTIVIDADE – ITENS I e II

9.1. A infraestrutura remota da CONTRATADA deverá se comunicar com a infraestrutura do BNDES utilizando canais de comunicação redundantes e, opcionalmente, balanceados.
9.2. Todos os serviços devem estar disponíveis por quaisquer um dos canais de comunicação de forma automática do caso de indisponibilidade de um deles.
9.2.1. Todos os fluxos de comunicação entre o ambiente do BNDES e a solução da CONTRATADA, inclusive o acesso de seus colaboradores, deverão ocorrer pela rede estabelecida entre CONTRATADA e o BNDES aqui detalhada.
9.3. Abaixo, estão listadas as características mínimas para a infraestrutura de telecomunicações.
9.3.1. Atender aos requisitos de infraestrutura listados no item 7;
9.3.2. A CONTRATADA deverá fornecer e implantar uma das opções abaixo de conectividade (incluído os canais de comunicação, roteadores, firewalls etc), sempre contemplando os dois datacenters do BNDES definidos no item 5:
9.3.2.1. Uma conexão dedicada entre seu ambiente principal e o datacenter principal do BNDES e uma conexão dedicada entre o seu ambiente secundário e o datacenter alternativo do BNDES;
9.3.2.2. Uma conexão via VPN entre seu ambiente principal e a conexão Internet instalada pela CONTRATADA no datacenter principal do BNDES e uma conexão via VPN entre seu ambiente secundário e a conexão Internet instalada pela CONTRATADA no datacenter alternativo do BNDES; ou
9.3.2.3. Uma combinação das opções anteriores.

9.3.3. A CONTRATADA deverá fornecer toda a infra de conectividade: canais de comunicação com a Internet e/ou dedicados, roteadores, firewall etc. Apenas o detalhado no item 7 será disponibilizado pelo BNDES.
9.3.4. Cada conexão VPN deverá terminar ou passar, no caso de conexão dedicada, por um appliance físico de firewall/UTM FortiGate da Fortinet fornecido e instalado pela CONTRATADA em cada um dos datacenters do BNDES que deverão operar em alta disponibilidade (HA). A definição da marcar de firewall/UTM se deve à experiência do BNDES com o referido fabricante para auditar e acompanhar as configurações que serão realizadas pela CONTRATADA.
9.3.4.1. Caso a CONTRATADA opte por conexões dedicadas e isoladas do ambiente público da Internet e de outros clientes, não serão necessários os appliances de firewall, pois os roteadores deverão ser conectados diretamente na infraestrutura do BNDES, conforme requisitos do item 7, e terão seu tráfego filtrado pelos firewalls do BNDES.
9.3.5. Caso a mesma empresa seja a prestadora de ambos os ITENS, será necessário apenas um conjunto de conexões.
9.3.6. Os circuitos virtuais (VPNs) deverão utilizar, no mínimo, criptografia AES com chave de 256 bits e autenticação SHA2.
9.3.7. A CONTRATADA deverá dimensionar e monitorar as conexões para que a utilização de cada conexão não ultrapasse 90% (noventa por cento) de sua capacidade por mais de 10 (dez) minutos), conforme nível de serviço (GER15) definido no catálogo de serviço do item 17.
9.4. Exemplo do esquema de conectividade.



10. VISTORIA – ITENS I e II

10.1. As empresas licitantes deverão optar pela realização ou não de vistoria nas instalações do BNDES, com o objetivo de avaliar as condições dos serviços a serem realizados, em dias e horários previamente acordados.
10.2. A licitante que não realizar a vistoria não poderá alegar qualquer desconhecimento das condições para a perfeita compreensão do objeto e integral execução contratual nos termos previstos nas Especificações Técnicas.
10.3. Durante a vistoria, as Licitantes serão acompanhadas por um membro da equipe técnica do BNDES, devendo marcar previamente a visita pelo e-mail gseg@bndes.gov.br.
10.4. Todas as vistorias deverão ocorrer em até 2 (dois) dias úteis antes da data de abertura das propostas.
10.5. Durante a vistoria, nas instalações das Unidades Funcionais do BNDES no Rio de Janeiro, listadas no item 5, não será permitido o porte de imãs, de aparelhos que gerem campos eletromagnéticos, de aparelhos de comunicação de voz e de dados de qualquer tipo, de alimentos, de bebidas e de materiais para fumantes. Fotos serão permitidas caso não venham a comprometer a segurança do ambiente;
10.6. O porte e a utilização de qualquer equipamento eventualmente necessário para as análises dos quesitos técnicos durante a vistoria devem ser previamente autorizados pelo BNDES ou por profissional por ele designado.
10.7. A vistoria deverá ser utilizada pelas Licitantes para aferir as condições gerais dos serviços a serem executados, tais como: locais de trabalho presencial, quando demandado pelo BNDES, características e condições dos datacenters para instalação da SOLUÇÃO DA CONTRATA e recursos de telecomunicações etc.

11. PROPOSTAS DE PREÇO – ITENS I e II

11.1. Os Licitantes deverão cotar, na forma das planilhas contidas nesta Especificação Técnica, os valores unitários, totais e global de acordo com as exigências do edital e seus anexos.

11.2. Os preços deverão ser preenchidos conforme o respectivo modelo de planilha constante no Anexo II ao Edital, cabendo à equipe do BNDES, responsável pela análise técnica das propostas, a validação dos resultados dos cálculos apresentados pela licitante.

11.3. As descrições constantes na Planilhas de Formação de Preços, estão apresentadas sob forma resumida, sendo obrigatória, portanto, a consulta às respectivas especificações neste documento, para a correta definição dos serviços a serem fornecidos.

11.4. Nos preços cotados deverão estar incluídas todas as despesas com salários, softwares, encargos sociais, fiscais e comerciais, impostos, taxas e quaisquer outros tributos, quando aplicáveis, necessárias ao integral cumprimento do objeto pela CONTRATADA. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais designados para a prestação dos serviços, tais como deslocamentos, hospedagens, treinamentos etc.

11.5. A Licitante deverá apresentar, de imediato, memória de cálculo para comprovação de quaisquer um dos valores apresentados em sua proposta quando requisitado pelo BNDES.

11.6. A Proposta de Preço deverá ser redigida em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, com clareza, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo firme e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em Reais (R$).

11.7. A Proposta deverá ter prazo de validade não inferior a 60 dias corridos, a partir da data de abertura das propostas.

11.8. As Licitantes não poderão alterar a estrutura da Planilha de Formação de Preços.

12. REQUISITOS PARA ACEITAÇÃO DA PROPOSTA – ITENS I e II

12.1. Serão exigidos, para aceitação da proposta, os seguintes requisitos:

12.1.1. Planilha de preços, conforme modelo de planilha constante no Anexo II ao Edital;

12.1.2. Documento contendo, obrigatoriamente: a descrição detalhada dos componentes da solução (software e hardware) que serão utilizados para prestação dos serviços e quais elementos serão instalados na infraestrutura do BNDES (ITENS I e II); e a topologia da conexão entre a infraestrutura da CONTRATADA e o BNDES (ITEM I e II);

12.1.3. Memória de cálculo dos custos envolvidos na prestação do serviço contendo, no mínimo, o detalhamento dos custos com hardware, software, telecomunicações e pessoal. Tais custos poderão ser utilizados pelo BNDES para análise de exequibilidade da proposta.

12.1.4. Declaração de que a proposta comercial atende a todos os prazos, requisitos e especificações técnicas, conforme modelo definido no Anexo VII ao Edital; e

12.1.5. Relação de todos os números de CNPJ que emitirão faturas de cobrança dos serviços contratados.

12.2. Como condição para aceitação da proposta, a equipe técnica que dará suporte à licitação poderá, sempre que julgar necessário, realizar diligência com vistas à comprovação da exequibilidade da proposta e das características técnicas exigidas para os serviços.

13. HABILITAÇÃO TÉCNICA/ECONÔMICA – ITENS I e II

13.1. Para fins de habilitação técnica, a LICITANTE deverá apresentar:

13.1.1. Atestados de Capacidade Técnica ou outro documento idôneo, fornecido por pessoa jurídica de direito público ou privado, que comprove que a LICITANTE executou ou executa serviços pertinentes e compatíveis em características técnicas com o objeto destas Especificações Técnicas para Instituição Financeira que atue no Brasil.

13.1.1.1. A definição de Instituição Financeira considerada neste Termo de Referência é a constante no Art. 17 da Lei nº 4.595, de 31 de dezembro de 1964, além do próprio Banco Central do Brasil. As referidas instituições devem ser autorizadas, reguladas ou supervisionadas pelo Banco Central, sendo que a relação delas está disponível para consulta nos seguintes endereços eletrônicos: https://www.bcb.gov.br/estabilidadefinanceira/relacao_instituicoes_funcionamento ou https://www.bcb.gov.br/estabilidadefinanceira/encontreinstituicao.

13.1.2. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução e sem ressalvas quanto a qualidade do serviço.

13.1.3. Para fins de comprovação da experiência em cada serviço de cada item não será aceito o somatório de atestados do mesmo serviço em períodos subsequentes, mas será aceito o somatório de atestados de períodos concomitantes. Por exemplo, serão aceitos dois atestados de operação da solução de SIEM (Security Information and Event Management) QRADAR do fabricante IBM, utilizada no BNDES, em entidades com 500 (quinhentos) usuários, desde que tenham ocorrido no mesmo período de 1 (um) ano, para atender ao requisito do item 13.1.9.1;

13.1.4. O conceito de usuário empregado para fins de aferição dos atestados será a quantidade de contas de usuário que estejam ativas no diretório de usuários da entidade. Estas são contas de usuários que interagem com sistemas de informação da entidade e que, em fazendo isto, geram eventos de interesse

para uma SOLUÇÃO de SIEM, por exemplo. Este conjunto de usuários ativos são atrelados a colaboradores, diretos (primeiros) ou indiretos (terceiros), e a contas de serviço (contas utilizadas por sistemas da entidade para interagirem com outros sistemas, da entidade ou de terceiros). As contas que representam computadores (desktops, notebooks, servidores etc.) não devem ser consideradas nesse quantitativo.
13.1.4.1. Caso o atestado não faça referência expressa ao número de usuários, tal quantidade será considerada como o quantitativo de microcomputadores mencionado no atestado.
13.1.5. As informações mínimas que não estejam expressamente indicadas nos documentos de atestação apresentados pela LICITANTE deverão ser comprovadas por meio de documentação complementar.
13.1.6. Não restará comprovada a qualificação técnica da LICITANTE se o objeto ou parcela dele tiver sido executada por sociedade(s) subcontratada(s) pela LICITANTE.
13.1.7. Será permitido atestado de empresas de um mesmo grupo econômico ou de subsidiária do mesmo conglomerado, desde que a criação da subsidiária (a licitante do presente certame licitatório) consistiu na transferência parcial de patrimônio e de recursos humanos da controladora inerentes à execução dos serviços descritos no atestado para a subsidiária, conforme preconizado no Acórdão n. 4.936/2016 - 2ª Câmara/TCU.
13.1.8. A Licitante deverá enviar, em conjunto com o Atestado, informações mínimas que permitam identificar o atestante, tais como:
13.1.8.1. CNPJ, nome comercial, endereço e telefone da(s) sociedade(s) atestante(s);
13.1.8.2. Nome, cargo/função, endereço, telefone e e-mail do(s) representante(s) da(s) sociedade(s) atestante(s) que vier(em) a assinar o(s) atestado(s), a fim de que o BNDES possa com ele(s) manter contato;
13.1.8.3. O período de execução do serviço; e
13.1.8.4. Descrição do objeto atestado, contendo dados que permitam a aferição de sua similaridade com o objeto licitado, por exemplo, cópia do contrato.
13.1.9. Para o ITEM I, a Licitante deverá apresentar os seguintes atestados de prestação de serviço para Instituição Financeira:
13.1.9.1. Operação da solução de SIEM (Security Information and Event Management) QRADAR do fabricante IBM, utilizada no BNDES, em entidades com, no mínimo, 1.000 (mil) usuários, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES;
13.1.9.2. Implantação e Operação de uma solução de SOAR (Security Orchestration, Automation and Response), em entidades com, no mínimo, 1.000 (mil) usuários, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES;
13.1.9.3. Serviços de monitoramento e resposta de incidentes de Segurança da Informação em empresas com, no mínimo, 1.000 (mil) usuários, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES;
13.1.9.4. Administração, configuração e/ou operação das consoles de segurança ou correlatas da solução Microsoft 365, em entidades com, no mínimo, 1.000 (mil) usuários, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES;
13.1.9.5. Serviços de detecção e gestão de vulnerabilidades de infraestrutura em empresas com, no mínimo, 2.000 (dois mil) ativos de TIC, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES; e
13.1.9.6. Serviços de apoio técnico especializado para situações de crise decorrentes de incidentes de segurança da informação relevantes com coleta de evidências/forense computacional em empresas com, no mínimo, 1.000 (mil) usuários, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES ou que tenha envolvido a coleta de evidências em ambiente de servidores virtualizados e/ou de estações com o sistema operacional Windows.
13.1.10. Para o ITEM II, a Licitante deverá apresentar os seguintes atestados de prestação de serviço para Instituição Financeira:
13.1.10.1. Serviço técnico especializado de Inteligência de Ameaças Cibernéticas em empresas com, no mínimo, 1.000 (mil) usuários, o que corresponde a aproximadamente 25% (vinte e cinco por cento) da quantidade existente no ambiente do BNDES.
13.1.11. As quantidades mínimas exigidas nos atestados têm por objetivo avaliar a capacidade da Licitante em prestar os serviços de segurança da informação de complexidade e por período similar ao requerido pelo BNDES na presente especificação técnica. Os quantitativos e período exigidos são inferiores a 50% das quantidades da contratação em questão, metodologia aceita pelo TCU para qualificar as empresas licitantes.
13.2. Considerando a relevância dos serviços para o BNDES, para fins de habilitação econômica, a LICITANTE deverá apresentar:
13.2.1. certidão negativa de falência expedida pelo distribuidor da sede do licitante;
13.2.2. balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;
13.2.2.1. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;
13.2.2.2. é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

13.2.3. índices econômico-financeiros usualmente adotados no âmbito das contratações públicas, quais sejam: Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG), observando-se que, caso os índices apresentem resultado inferior a 1, o Licitante deverá comprovar que possui patrimônio líquido ou capital social de, no mínimo, 10% (dez por cento) do valor do respectivo ITEM da contratação.
13.2.3.1. Os índices deverão ser calculados pela licitante e confirmados pelo responsável por sua contabilidade, mediante sua assinatura e a indicação do seu nome e do número de registro no Conselho Regional de Contabilidade (CRC).

14. REQUISITOS TÉCNICOS DOS SERVIÇOS – ITENS I e II

14.1. ITEM I - CENTRO DE OPERAÇÕES DE SEGURANÇA CIBERNÉTICA (CSOC)
14.1.1. CONSIDERAÇÕES GERAIS
14.1.1.1. Os registros de problemas, requisições de serviços e incidentes que serão encaminhados para as equipes do BNDES deverão ser registrados na ferramenta ITSM (Remedy) de propriedade do BNDES, conforme item 16. Sugere-se que a CONTRATADA desenvolva integrações com o Remedy por API.
14.1.1.2. Caso a BNDES venha adquirir e implantar uma nova ferramenta de ITSM a integração com a plataforma da CONTRATADA deverá ser avaliada e implementada no limite das possiblidades técnicas existentes e não deve gerar custos adicionais a CONTRATADA.
14.1.1.3. A CONTRATADA deve possuir solução de monitoramento de disponibilidade e desempenho das soluções ofertadas para prestação dos serviços.
14.1.1.4. O serviço deverá ser prestado por meio de estruturas de CSOC's – Cyber Security Operation Center redundantes, obrigatoriamente no Brasil. Um dos centros deverá ser provido em ambiente físico próprio da CONTRATADA e um segundo poderá ser provido em ambiente físico terceirizado, desde que os serviços sejam comprovadamente prestados por funcionários da CONTRATADA.
14.1.1.4.1. A equipe técnica envolvida na prestação do serviço especificado no ITEM apenas deverá ter acesso ao ambiente do BNDES a partir da rede do CSOC da CONTRATADA. Eventuais acessos remotos ao CSOC da CONTRATADA com acesso ao ambiente do BNDES deverão ser justificados pela CONTRATADA e previamente submetido à aprovação pelo BNDES.
14.1.1.5. Para fins da presente licitação, entende-se como ambiente físico privado da CONTRATADA o ambiente onde são executadas as atividades relacionadas à prestação dos serviços, exclusivamente por profissionais com vínculo jurídico com a CONTRATADA.
14.1.1.6. O CSOC funcionará de forma ininterrupta 24 horas por dia e 7 dias por semana.
14.1.1.7. Deve possuir plataforma de Sandbox para análise de ameaças avançadas.
14.1.1.8. Os CSOCs devem estar ativos simultaneamente e deverão atender aos seguintes requisitos mínimos:
14.1.1.8.1. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
14.1.1.8.2. Filmar toda a área, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias;
14.1.1.8.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 (noventa) dias;
14.1.1.8.4. Estarem localizados em instalações independentes e distantes em, pelo menos, 10 KM;
14.1.1.8.5. O perímetro deve ser protegido contra intrusão e acesso indevido;
14.1.1.8.6. Ser vigiado de forma ininterrupta por segurança especializada em regime de 24x7x365;
14.1.1.8.7. Ter controle de acesso físico com pelo menos 2 (dois) fatores de autenticação;
14.1.1.8.8. Ser configurado de forma que a falha de um dos equipamentos isoladamente não interrompa a prestação dos serviços;
14.1.1.8.9. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;
14.1.1.8.10. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
14.1.1.8.11. Deverá possuir processos implementados que garantam a segurança das informações do BNDES, em conformidade com a norma ABNT NBR ISO/IEC 27001; e
14.1.1.8.12. Adotar controles que garantam a segregação dos dados de diferentes clientes, de forma a preservar a confidencialidade, a integridade e disponibilidade dos dados referentes ao serviço prestado ao BNDES.
14.1.2. ATIVIDADE DE CSIRT
14.1.2.1. As atividades de monitoramento, resposta a incidentes de SI (Segurança da Informação) e gestão de ameaças cibernéticas (Computer Security Incident Response Team - CSIRT), têm por objetivo, de forma continuada, detectar, triar, categorizar, analisar e documentar os eventos de segurança da informação que sejam transformados em um incidente de segurança da informação, obedecendo os principais frameworks de gestão de incidentes de segurança da informação e boas práticas de mercado (MITRE ATT&CK, NIST CSF, SIM3 etc).
14.1.2.2. A CONTRATADA deverá operar o sistema de correlação de eventos de segurança da informação (SIEM) do BNDES, descrito no item 8.2, realizando as atividades de monitoramento, triagem, investigação,

classificação, resposta e documentação das ações de resposta (playbooks) aos eventos registrados no SIEM do BNDES a partir de fontes internas e externas, por exemplo, o Active Directory, a plataforma Microsoft 365, o proxy web, a ferramenta de Levantamento e Gestão de Vulnerabilidades, o serviço de threat intelligence/brand intelligence especificados no item 14.2 etc.

14.1.2.2.1. A CONTRATADA deverá prover e alimentar o SIEM do BNDES com fontes (feeds) de inteligência de ameaça cibernética (Threat Intelligence), informações sobre artefatos maliciosos, IPs suspeitos ou com veredito malicioso, bem como, incluir informações de indicadores de comprometimento que possam auxiliar a resposta de um incidente, aumentando a eficiência e a eficácia dos processos envolvidos.

14.1.2.2.1.1. Essas fontes de Threat Intelligence não se confundem com o serviço de Threat Intelligence do ITEM II. Aqui, as fontes de Threat Intelligence deverão ser disponibilizadas pela CONTRATADA para o ITEM I e devem trazer informações genéricas e gerais para enriquecimento dos eventos do SIEM (IPs suspeitos, CVEs sendo explorados ativamente na Internet, artefatos maliciosos conhecidos, etc) e apoio no tratamento dos mesmos. As fontes de Threat Intelligence do ITEM II também serão conectadas ao SIEM do BNDES mas trarão dados filtrados para os ativos indicados pelo BNDES para monitoração no ambiente externo (IP do BNDES, nomes de servidores, nomes de sistemas, campanhas envolvendo o setor financeiro, BATIC etc).

14.1.2.2.2. A CONTRATADA deve comunicar ao BNDES toda vez que ocorrer alteração da linha de base relacionada à quantidade de tráfego enviado ao SIEM, que não tenha sido previamente acordada com o BNDES.

14.1.2.2.3. Espera-se que a linha de base dos eventos de segurança monitorados seja revista de forma mensal, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados, e se espera que a CONTRATADA tome ciência destes ataques e, por sua vez, atualize a linha de base para que em um cenário onde estes novos ataques sejam direcionados ao BNDES, sejam detectados através dos serviços em questão.

14.1.2.2.4. O BNDES pode, a qualquer momento, solicitar a inclusão ou a exclusão de fontes de dados, de campos personalizados em eventos, de regras de correlação de eventos, de geração de alertas e de incidentes de SI.

14.1.2.2.5. A CONTRATADA será responsável pela gestão e documentação dos casos de uso configurados no SIEM do BNDES e pelo aperfeiçoamento das regras, limiares e alertas do SIEM do BNDES, visando reduzir o número de falsos positivos e falsos negativos, além da criação de novas regras.

14.1.2.2.6. A atividade de monitoramento deve realizar o acompanhamento contínuo e ininterrupto de ataques cibernéticos direcionados ao BNDES, utilizando, por exemplo, o SIEM do BNDES para correlação de logs, pacotes/fluxos de redes, bem como, analisar e identificar comportamentos maliciosos de usuários, aplicações, serviços e infraestrutura do BNDES.

14.1.2.2.7. Faz parte da atividade de operação do SIEM do BNDES a implantação de novos casos de uso, configurando regras, limiares e alertas de acordo com:

14.1.2.2.7.1. As especificações fornecidas pelo BNDES.

14.1.2.2.7.2. As especificações desenvolvidas por equipe especializada da CONTRATADA com base em ameaças identificadas em outros clientes ou nos incidentes e eventos observados no BNDES.

14.1.2.2.7.3. A implementação dos casos de uso deverá ocorrer inicialmente em ambiente de SIEM de teste/homologação do BNDES para prévia validação pelo BNDES. Após validação, testes e aprovação, o caso de uso poderá ser implantado no SIEM de produção.

14.1.2.2.7.4. Deve ser priorizada a implementação dos casos de uso definidos no item 6.

14.1.2.2.7.5. A evolução da implementação de casos de uso no SIEM do BNDES frente à lista de casos de uso prioritários definidos no item 6 será objeto de acompanhamento e deve ser regularmente reportada ao BNDES.

14.1.2.2.8. A atividade de resposta a incidentes engloba:

14.1.2.2.8.1. Os eventos de segurança da informação devem ser analisados, podendo ocasionar em incidentes de segurança da informação, obedecendo a um processo cíclico e rigoroso de gestão de eventos, com registro dos incidentes e a evolução detalhada do tratamento, integrado, mandatoriamente, com a ferramenta de gestão de demandas indicada pelo BNDES, conforme item 16.1.2.3.

14.1.2.2.8.2. A CONTRATADA deve prover o diagnóstico e recomendar o tratamento e a resposta aos incidentes de segurança detectados; com o encaminhamento dos incidentes e os seus respectivos planos de ação, por meio da ferramenta de gestão de demandas adotada pelo BNDES.

14.1.2.2.8.3. A CONTRATADA deve prover a proposta de contenção, erradicação e recuperação associadas aos incidentes de segurança da informação, além de realizar a articulação com as equipes do BNDES, acompanhando e orientando as ações, notificações, avaliando e realizando o escalonamento dos incidentes, quando pertinente.

14.1.2.2.8.4. Em caso de ataque, devem ser elaborados alertas e estratégias de prevenção para o BNDES.

14.1.2.2.8.5. A CONTRATADA deve criar, revisar e manter os playbooks com objetivo de simplificar e dar agilidade ao processo de resposta a incidentes.

14.1.2.2.8.6. Os referidos playbooks devem ser transferidos para o BNDES.

14.1.2.2.9. A atividade de triagem engloba:
14.1.2.2.9.1. A CONTRATADA deve realizar uma avaliação das informações relevantes associadas ao incidente, com a finalidade de determinar classificação, conforme Tabela de Classificação de Severidade de Incidentes de SI, criticidade e prioridade, a ser disponibilizada pelo BNDES.
14.1.2.2.9.2. Deve investigar os eventos recebidos para determinar se eles geraram incidentes de segurança da informação. Portanto, deve realizar a atividade de Threat Hunting e classificar toda a cadeia do ataque (Tática, Técnica e Procedimento - TTP) de acordo com o framework MITRE ATT&CK.
14.1.2.2.9.3. O processo de investigação deve buscar identificar os IoCs associados, a causa raiz, a extensão e o impacto do incidente de segurança da informação, além de formas de conter e de erradicar os artefatos maliciosos encontrados.
14.1.2.2.9.4. Deve classificar os eventos considerados como verdadeiros-positivos ou falsos-positivos, de acordo com escala de criticidade e demais critérios de categorização definidos pelo BNDES.
14.1.2.2.9.5. Com o intuito de diminuir o tempo de resposta ao incidente, alguns aspectos importantes devem ser observados, pela CONTRATADA, para sua correta classificação/categorização:
14.1.2.2.9.5.1. Qualidade das informações disponibilizadas e registradas.
14.1.2.2.9.5.2. Identificação dos ativos e serviços afetados.
14.1.2.2.9.5.3. Mensuração dos impactos relacionados.
14.1.2.2.10. A atividade de analisar engloba:
14.1.2.2.10.1. A CONTRATADA deve analisar o incidente como um todo, observando quais ações são necessárias ao seu tratamento, além de identificar a severidade e a urgência associadas ao incidente de segurança da informação.
14.1.2.2.10.2. Uma vez confirmado um incidente, a CONTRATADA deve:
14.1.2.2.10.2.1. Gerar alerta ao BNDES imediatamente por meio de chamado na ferramenta de gestão de demandas definida pelo BNDES; e
14.1.2.2.10.2.2. Preparar o processo de tratamento, documentando-o em um playbook.
14.1.2.2.10.3. A CONTRATADA deve elaborar junto com as equipes internas do BNDES os planos de contenção, erradicação e/ou recuperação total do ambiente afetado, onde:
14.1.2.2.10.3.1. Contenção: ações temporárias, também conhecidas como mitigação, que limitem o dano causado pelo incidente ao ambiente.
14.1.2.2.10.3.2. Erradicação: identificar a causa raiz do incidente e promover ações de solução removendo as ameaças e restaurando o ativo afetado, para que retorne ao estado anterior ao incidente.
14.1.2.2.10.3.3. Recuperação: ações de retorno à situação anterior ao incidente, após realização de testes e validações que venham a garantir que os itens de configuração afetados foram devidamente tratados e estão livres de ameaças.
14.1.2.2.11. A atividade de tratamento do incidente engloba:
14.1.2.2.11.1. Uma vez registrados pela CONTRATADA, conforme item 16.1.2.3, de acordo com o playbook definido, deve aplicar as ações de tratamento do incidente contidas nos planos de contenção, erradicação e/ou recuperação.
14.1.2.2.11.2. Por exemplo: A CONTRATADA deverá solicitar bloqueios e criação de regras de segurança à equipe de operação do BNDES, e acompanhar a conclusão das solicitações, via ferramentas de ITSM do BNDES (BMC Remedy).
14.1.2.2.11.3. Avaliar o tratamento do incidente
14.1.2.2.11.3.1. A CONTRATADA deve avaliar, em conjunto com o BNDES, se as soluções aplicadas foram adequadas, se o ambiente se encontra livre de ameaças e se a causa raiz do incidente foi erradicada.
14.1.2.2.11.3.2. Caso haja inconsistência relacionada ao incidente, a CONTRATADA deve iniciar um novo ciclo de tratamento, onde novas possibilidades de contenção, erradicação e/ou recuperação devem ser providas.
14.1.2.2.11.4. Encerrar o incidente
14.1.2.2.11.4.1. A CONTRATADA deve finalizar o incidente documentando todas as ações realizadas na fase de tratamento, detalhando cada etapa com as respectivas evidências e análise complementar e recomendações para redução de risco de novo incidente similar.
14.1.2.2.11.4.2. Importante ressaltar que todo processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado pela CONTRATADA.
14.1.2.3.A CONTRATADA deverá operar as consoles de segurança do Microsoft 365, conforme consta no item 8.2, realizando as atividades de monitoramento, investigação, classificação, resposta e documentação das ações de reposta (playbooks) aos eventos de segurança da informação.
14.1.2.3.1. A CONTRATADA deverá prover YubiKey suficientes para todos os seus colaboradores envolvidos na operação das consoles Microsoft, considerando o regime de operação 24x7 do serviço. Não será aceito o compartilhamento de credenciais.
14.1.2.3.2. O acesso à instância do Microsoft 365 será restrito aos endereços IP dos CSOCs da CONTRATADA ou por outro meio definido pelo BNDES.
14.1.2.3.3. As ações abaixo deverão ser desempenhadas nas consoles Microsoft, além das atividades descritas no item 14.1.2.2 e subitens.
14.1.2.3.3.1. Tratar Incidentes/Alertas;

14.1.2.3.3.2. No Action Center aprovar ações de remediação;
14.1.2.3.3.3. Pesquisar informações e executar ações (iniciar uma varredura, isolar dispositivo etc) em dispositivos. Exemplo: No caso da regra de detecção no SIEM de malware via defender ser ativada, realizar o seguinte procedimento - receber o ticket de acordo com o processo definido pelo BNDES; identificar o usuário e a máquina afetada; identificar o potencial malware; analisar o potencial malware; conter o malware; e executar uma varredura completa na estação de trabalho, Notificar os envolvidos e Fechar o ticket.
14.1.2.3.3.4. Pesquisar informações e executar ações (analisar e liberar mensagens da quarentena de correio eletrônico, apagar, enviar para lixo eletrônico, submeter para Microsoft etc.) na caixa de correio eletrônico. Exemplo: No caso da regra de detecção no SIEM de phishing ser ativada realizar o seguinte procedimento - Analisar a mensagem de e-mail e verificar se é um falso-positivo ou um verdadeiro-positivo; analisar se outros(as) colaboradores(as) foram alvejados(as); procurar por campanhas similares; coletar os IoCs do golpe; analisar os IoCs do golpe; bloquear os IoCs do golpe; remover os e-mails maliciosos das caixas postais; submeter os e-mails maliciosos para análise do fabricante do antispam; analisar se houve comprometimento de estações de trabalho; se necessário, acionar o caso de uso de contenção de malware; se necessário, forçar a troca de senha do(s) usuário(s); compartilhar os IoCs pertinentes; e notificar os envolvidos.
14.1.2.4. A CONTRATADA deverá implantar e utilizar ferramenta de SOAR para automatizar o tratamento de todo o ciclo dos eventos de segurança: detecção da ameaça, triagem, definição das ações e contenção.
14.1.2.4.1. A ferramenta de SOAR deve estar integrada às ferramentas de SIEM, MISP, RTIR, etc do BNDES, listadas no item 8.2, para coleta de dados e geração de tickets;
14.1.2.4.2. A ferramenta de SOAR deve estar integrada à ferramenta de Levantamento e Gestão de vulnerabilidades para compartilhamento de inventário de ICs e suas respectivas vulnerabilidades detectadas.
14.1.2.4.3. Deverá efetuar o tratamento dos eventos em near real-time;
14.1.2.4.4. Deverá ser utilizada para automatizar total ou parcialmente as etapas do processo de gestão de incidentes de SI. Não sendo possível a automatização total, caberá à CONTRATADA a realização manual das demais etapas definidas para o processo de gestão de incidentes de SI, itens 14.1.2.2.
14.1.2.4.4.1. A CONTRATADA deve automatizar os processos de segurança para reduzir o desperdício de recursos e tempo de resposta a ameaças;
14.1.2.4.4.2. A CONTRATADA, após aprovação do BNDES, poderá automatizar a respostas aos eventos, alertas ou incidentes criados na solução de SIEM por meio da correlação de eventos.
14.1.2.4.5. Os incidentes automaticamente tratados deverão ser registrados e acompanhados na solução de RTIR ou ITSM do BNDES seguindo o fluxo definido para o processo de gestão de incidentes.
14.1.2.4.6. Preferivelmente, a ferramenta de SOAR e a integração entre SOAR e SIEM deve contemplar:
14.1.2.4.6.1. Ofensa detectadas pelo SIEM podem ser automaticamente escalada para o SOAR com critérios configuráveis;
14.1.2.4.6.2. Integração bidirecional permitindo que o incidente encerrado no módulo de SOAR encerre automaticamente a ofensa correspondente no SIEM.
14.1.2.4.6.3. Anotações realizadas numa ofensa no SIEM são sincronizadas para o SOAR.
14.1.2.4.6.4. Permite pesquisas nos eventos do SIEM a partir de playbooks do SOAR, colocando o resultado como evidências (logs) e tabelas do incidente.
14.1.2.4.6.5. Cria artefatos, ao mesmo tempo em que o mapeamento de incidentes é definido.
14.1.2.4.6.6. Criação e customização de playbooks dinâmicos, envolvendo regras, condições, lógica de negócio e tarefas, para responder a um incidente através de inteligência, automação e orquestração.
14.1.2.4.6.7. Novos processos podem ser definidos na plataforma em playbooks dinâmicos, que representa um Plano de Resposta a Incidente, que muda e se adapta de acordo com as regras de negócio definida pelo usuário.
14.1.2.4.6.8. Lógicas mais complexas podem ser criadas como scripts Python, permitindo maior flexibilidade.
14.1.2.4.6.9. O construtor de playbooks permite unir em um único fluxo, tarefas do analista, ações e ferramentas externas e processamento interno.
14.1.2.4.6.10. Sub playbooks permitem que lógicas comuns a vários playbooks seja escrita uma vez e usada em diferentes playbooks, mantendo a consistência e reduzindo o esforço de gestão.
14.1.2.4.6.11. Os playbooks podem ser exportados e importados.
14.1.2.5. A CONTRATADA deverá executar ainda, as seguintes atividades:
14.1.2.5.1. Realizar estudos e a criação de processos e rotinas operacionais, que permitam desenhar e automatizar os fluxos de trabalho;
14.1.2.5.2. Consolidar dados e extrair informações úteis de fontes diversas de inteligência e das tecnologias de segurança existentes e se integrando e interagindo com todas as fontes de informações relevantes para a atividade;
14.1.2.5.3. Parametrizar, gerenciar e se integrar eficazmente aos fluxos e ferramentas referentes a requisições, incidentes de segurança da informação e privacidade, permitindo a definição de um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção;

14.1.2.5.4. Criar dashboards nas ferramentas fornecidas para atendimento do serviço de acordo com as especificações fornecidas pelo BNDES
14.1.2.5.4.1. A solicitação dos serviços de criação e customização de regras e dashboards específicos para o BNDES será realizada por meio de chamado.
14.1.2.5.5. Enriquecer os dados dos eventos e incidentes cibernéticos a partir das fontes contratadas pela CONTRATADA (bancos de reputação de endereços IP, URLs, padrões de Phishing, assinatura de feeds de inteligência de terceiros etc), fontes de OSINT (Open Source Intelligence) e dados oriundos do serviço de CTI (ITEM II).
14.1.2.5.6. Tratar os incidentes identificados e aqueles reportados pela ETIR-BNDES de acordo com os playbooks da base de conhecimento do BNDES.
14.1.2.5.7. Analisar as causas e os impactos dos incidentes tratados e propor controles para evitar novos incidentes similares.
14.1.2.5.8. Deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado.
14.1.2.5.9. Escalar incidentes cibernéticos que não sejam da sua alçada de acordo com os playbooks da base de conhecimento do BNDES.
14.1.2.5.10. Deve identificar novos IoC´s e automatizar o envio para ferramentas de inteligência para enriquecimento do alerta, quando autorizado pelo BNDES.
14.1.2.5.11. Construir novos ou aprimorar os playbooks para tratamento de incidentes similares para formar uma base de conhecimento do BNDES. Os playbooks, de acordo com a avalição do BNDES, poderão ser automáticos (sem interação humana) ou semiautomáticos (com alguma interação humana) para tratamento de incidentes e alertas.
14.1.2.5.12. Caso a CONTRATADA identifique a ausência de insumo interno (logs, pacotes de rede etc) a ser gerado por um item de configuração do BNDES, necessário à prestação do serviço, será de reponsabilidade da CONTRATADA solicitar ao BNDES a correção e/ou habilitação de tal insumo. Caso o insumo seja externo, feed de informação para identificação de ameaças, por exemplo, o fornecimento será obrigação da CONTRATADA.
14.1.2.5.13. Propor e empregar métodos e ferramentas para apoiar nas atividades de gestão de ameaças cibernéticas, garantindo a adoção de padrões – propostos pela CONTRATADA ou definidos pelo BNDES – para o devido registro, análise e tratamento de incidentes, e que permitam a realização de buscas, acompanhamento do seu ciclo de vida e a eventual identificação de relacionamento com outros incidentes, ativos ou vulnerabilidades já registradas.
14.1.2.5.14. Planejar e apoiar a implementação de mecanismos para automatizar e acelerar o tratamento e a resposta aos eventos e incidentes cibernéticos, quer pela implementação de solução SOAR, quer por soluções de automatização implementadas manualmente, desde que garanta a automação e a prontidão das respostas aos eventos e incidentes cibernéticos e não acarretem custos adicionais para o BNDES.
14.1.3. ATIVIDADE DE LEVANTAMENTO E GESTÃO DE VULNERABILIDADES
14.1.3.1. A atividade de levantamento e gestão de vulnerabilidades de infraestrutura tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação no ambiente de TIC do BNDES (Vulnerability Assessment - VA), a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.
14.1.3.2. A gestão de vulnerabilidades está dividida em duas frentes:
14.1.3.2.1. A frente contínua/proativa de monitoramento das vulnerabilidades, onde a CONTRATADA deverá alertar o BNDES sobre as vulnerabilidades publicadas nos sites dos fabricantes e em outras fontes (assinatura de feeds de terceiros) para os produtos de infraestrutura existentes do BNDES; e
14.1.3.2.2. A frente de monitoramento recorrente, onde a CONTRATADA deverá, sob demanda do BNDES, executar o serviço de levantamento de vulnerabilidades de acordo com o escopo ajustado com o BNDES, que será formalizado por meio de chamado aberto pelo BNDES.
14.1.3.3. O serviço contempla as fases de varreduras por vulnerabilidades, alertas de vulnerabilidades e controle das vulnerabilidades, com identificação dos achados, soluções e identificação das vulnerabilidades corrigidas/remediadas.
14.1.3.4. Caberá a CONTRATADA criar e manter uma base de ativos de TIC - BATIC, em ferramenta adequada e aprovada pelo BNDES, para utilização pela solução de varredura e demais sistemas da infraestrutura de segurança. Os dados iniciais poderão ser obtidos a partir dos sistemas do BNDES de CMDB/Remedy, monitoramento/Zabbix, cadastro de IPs, DNS, AD etc. Caso essas fontes não contenham todas as informações necessárias, a CONTRATADA deverá realizar uma varredura de IPs e seus serviços nas redes indicadas pelo BNDES. Essa base de ativos de TIC deverá ser a fonte para as varreduras e relatórios de vulnerabilidades, e deverá ser compartilhado com outras ferramentas, por exemplo, de SOAR para que esta tenha ciência da infraestrutura vulnerável.
14.1.3.4.1. A base de ativos de TIC, no mínimo, deverá conter as seguintes informações: nome DNS, IP, SO, versão do SO, descrição do ativo, equipe responsável, serviços de rede, versão dos módulos de serviço, criticidade para a TIC (0 a 4), criticidade para o negócio (0 a 4) e grupo de serviço de negócio. O BNDES poderá analisar e talvez aceitar uma composição diferente desta base, desde que seja possível atribuir, pelo menos, diferentes criticidades para influenciar a percepção de risco das vulnerabilidades

encontradas nos ativos, e que seja possível relacionar os ativos a diferentes grupos de tratamento de vulnerabilidades.
14.1.3.4.2. O BNDES apoiará a CONTRATADA na criação e manutenção da referida base fornecendo informações que não puderem ser obtidas de forma automática.
14.1.3.4.3. A BATIC deverá ter suas informações revisadas e atualizadas continuamente.
14.1.3.5. O serviço de varredura e gestão de vulnerabilidades de infraestrutura também deverá contemplar as seguintes atividades:
14.1.3.5.1. Instalar, configurar e elaborar documentação das ferramentas fornecidas, inclusive suas integrações.
14.1.3.5.2. Realizar a manutenção preventiva, corretiva e atualizações das ferramentas fornecidas.
14.1.3.5.3. Apoiar a equipe do BNDES no uso das ferramentas para execução de varreduras ad-hoc, por exemplo, quando o BNDES estiver fazendo uso destas.
14.1.3.5.4. Preparar e realizar varreduras sob demanda/agendadas para levantamento de vulnerabilidades de ativos de infraestrutura de TIC incluindo a elaboração do relatório com o resultado da análise (informações da base de ativos de TIC, CVE do NVD e do fabricante, CVSS score e vetor CVSS, informações dos alertas do CTIR gov , informações do KEV da CISA , informações do EPSS da FIRST, informações do exploit.db e de outras bases de exploit, e correção aplicável e/ou solução de contorno). A CONTRATADA deverá calcular o CVSS score quando um CVSS score 3.1 e o vetor CVSS 3.1 quando estes não estiverem disponíveis. A CONTRATADA deverá ponderar o CVSS score atribuído à vulnerabilidade com base em fatores indicados pelo BNDES para cada ativo e recalcular o CVSS score (versão 3.1 e superior) de acordo com a exposição/criticidade do ativo, do fato de detalhes da vulnerabilidade terem ou não sido se tornado públicos e de haver ou não um exploit público para a vulnerabilidade [base de ativos de TIC - criticidade para a TIC (0 a 4)] definido em conjunto com o BNDES.
14.1.3.5.5. Interagir com as equipes de suporte de TI e com CSIRT do BNDES para tratar de aspectos relacionados à execução das varreduras e das vulnerabilidades identificadas (explicações técnicas sobre as vulnerabilidades, orientações para sanar as vulnerabilidades e varreduras pontuais para verificar sua correção), bem como para garantir o alinhamento necessário para o adequado encaminhamento das vulnerabilidades identificadas para correção pelas equipes técnicas.
14.1.3.5.6. A fim de mitigar e prever possíveis impactos durante as rotinas de validação de vulnerabilidade, antes do início da execução do serviço, as ferramentas e técnicas adotadas para execução deverão ser apresentadas à equipe do BNDES, que poderá ou NÃO aprovar a utilização delas.
14.1.3.5.7. Registrar demandas de correção, pelas equipes de suporte de TI do BNDES, das vulnerabilidades identificadas de acordo com procedimentos e critérios estabelecidos pelo BNDES na ferramenta de ITSM. O registro deverá conter, no mínimo, as informações listadas no item 14.1.3.5.4.
14.1.3.5.8. Elaborar as ações de correção para corrigir as vulnerabilidades comunicadas de forma definitiva ou as ações de mitigação com as ações temporárias que limitam a exploração da vulnerabilidade identificada caso não haja soluções conhecidas e/ou definitivas.
14.1.3.5.9. Elaborar Baselines de segurança para ativos de tecnologia da informação, utilizando-se de boas práticas de mercado, tais como o CIS-Control ou outro framework compatível.
14.1.3.6. Para a prestação do serviço de varredura e gestão de vulnerabilidades deverá ser utilizada uma solução especializada com as seguintes características:
14.1.3.6.1. A solução deve ser capaz de apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para a correção.
14.1.3.6.2. A solução deve possuir recurso para acompanhamento da evolução das remediações de vulnerabilidades encontradas.
14.1.3.6.3. Quanto à varredura:
14.1.3.6.3.1. Ser capaz de identificar e analisar os sistemas operacionais Windows Server, Windows Desktop e Red Hat Enterprise Linux, ESXi, dentre outros listados no item 8.1, além dos módulos/serviços/aplicações/bibliotecas instalados. Não faz parte do escopo, mesmo que listados no referido item, as estações de trabalho e sistemas desenvolvidos.
14.1.3.6.3.2. Permitir a varredura de vulnerabilidades utilizando scanners de rede com ou sem credenciais de autenticação (autenticada ou não autenticada) e abrangente ou limitada.
14.1.3.6.3.3. Possuir ao menos três gradações de varredura: (i) descoberta de ativos, (ii) varredura branda, sem impactos negativos esperados (iii) varredura agressiva, onde impactos negativos não são esperados, mas podem ocorrer.
14.1.3.6.3.4. Por padrão, deverá ser realizada sem agente instalado, mas será permitido o uso de agentes temporários (dissolvable) para endpoints Red Hat Enterprise Linux, Windows Server e outros que sejam compatíveis, de acordo com a avaliação e autorização do BNDES.
14.1.3.6.3.5. Executar a descoberta, classificação e varredura de vulnerabilidades em containers e imagens Docker e Kubernetes (OKD como usada no OpenShift).
14.1.3.6.3.6. Possuir recursos para executar uma varredura completa de, no mínimo, 200 alvos em até 1 hora.
14.1.3.6.3.7. Estar licenciada para, no mínimo, para os quantitativos e tipos de dispositivos listados no item 8.1.

14.1.3.6.3.8. Realizar escaneamento de descoberta utilizando os seguintes critérios como alvo: IP, CIDR e range de rede.
14.1.3.6.3.9. Durante a descoberta, deve alimentar a base de ativos de TIC com novos ativos e serviços que forem descobertos de forma online ou offline via processo desenvolvido pela CONTRATADA. Para os serviços deve cadastrar a versão dos módulos e respectivas portas de rede ativas.
14.1.3.6.4. Quanto à análise de conformidade:
14.1.3.6.4.1. Permitir a auditoria de sistemas Red Hat Enterprise Linux e Windows Server utilizando perfis de segurança SCAP.
14.1.3.6.4.2. Possuir padrões de varredura em conformidade com a regulamentação Payment Card Industry Data Security Standard (PCI DSS).
14.1.3.6.4.3. Permitir a auditoria das configurações de ativos de rede Aruba, Fortinet, F5, Huawei, Cisco, Juniper e os listados no item 8.1.
14.1.3.6.5. Quanto às bases de vulnerabilidades:
14.1.3.6.5.1. Possuir assinatura de base de vulnerabilidades com atualizações permanentes, no mínimo, diárias.
14.1.3.6.5.2. Utilizar como fonte umas das bases de vulnerabilidades NVD, MITRE, o PCISRT do produto ou outra fonte que seja autorizada pelo BNDES.
14.1.3.6.5.3. A base de vulnerabilidades deve tratar, no mínimo, todas as plataformas listadas no no item 8.1, menos desktops e sistemas desenvolvidos para/pelo BNDES.
14.1.3.6.5.4. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades, utilizando no mínimo os seguintes critérios: CVSS Score (versão 3.1 ou 4); existência de códigos de exploração da vulnerabilidade encontrada (exploit); existência de módulos de exploração da vulnerabilidade em frameworks automatizados, tais como: Metasploit, Core Impact, CANVAS; frequência de uso da vulnerabilidade em ataques e campanhas atuais e popularidade da vulnerabilidade em fóruns e comunicações na Darkweb.
14.1.3.6.6. Quanto às integrações nativas ou desenvolvidas pela CONTRATADA:
14.1.3.6.6.1. Possuir integração com o BMC Remedy, permitindo o registro automático de problemas na ferramenta.
14.1.3.6.6.2. Enviar ou disponibilizar insumos para soluções de correlação de eventos externa (SIEM) de forma automática.
14.1.3.6.6.3. Possuir integração com a ferramenta de monitoramento de eventos de segurança/SOAR para cadastramento dos alertas em ativos com vulnerabilidades identificadas.
14.1.3.6.6.4. Possuir integração com infraestrutura de virtualização VMware vSphere 7 e superior para descoberta de hosts.
14.1.3.6.7. Quanto à apresentação das informações:
14.1.3.6.7.1. Apresentar relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque de TIC do BNDES em relação aos riscos de segurança em TI, contendo: hosts encontrados, serviços, vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade;
14.1.3.6.7.2. Capacidade de exportação de relatório de vulnerabilidades em formato PDF e CSV;
14.1.3.6.7.3. Possibilitar a configuração de dashboards customizados conforme agrupamentos e definições a serem definidas pelo BNDES.
14.1.3.6.7.4. Agrupamento de ativos por quaisquer uma das informações da base de ativos de TIC.
14.1.3.7. Para o monitoramento contínuo/proativo (24x7x365) das vulnerabilidades publicadas para os produtos da infraestrutura do BNDES, de acordo com a base de ativos de TIC construída e mantida pela CONTRATADA, a solução implantada pela CONTRATADA, não necessariamente instalada no BNDES, deverá comunicar a equipe do BNDES via e-mail e ticket no sistema de ITSM, se assim definido pelo BNDES, sempre que uma vulnerabilidade for identificada, de acordo com os tempos e prioridades definidas no catálogo de serviços.
14.1.3.7.1. O comunicado deve conter, no mínimo, as informações listadas no item 14.1.3.5.4.
14.1.3.8. Para a frente de levantamento de vulnerabilidades sob demanda, a CONTRATADA deverá produzir os seguintes relatórios após solicitação da atividade pelo BNDES:
14.1.3.8.1. Relatório de Detecção e Gestão de Vulnerabilidades com as informações especificadas no item 14.1.3.5.4.
14.1.3.9. Em caso de comunicado incorreto/falso positivo de vulnerabilidade descoberta e/ou falta de comunicação de vulnerabilidade conhecida, a CONTRATADA sofrerá ajuste de qualidade.
14.1.4. ATIVIDADE DE IRC (INCIDENT RESPONSE CONSULTING)
14.1.4.1. Atuação sob demanda para suporte ao BNDES e coordenação de ações de resposta, contenção, recuperação e investigação de incidentes graves de segurança da informação em andamento, com as seguintes características:
14.1.4.1.1. Atendimento remoto e/ou presencial, sob demanda, a partir do acionamento pelo BNDES, por meio de equipe especializada para atuar em casos de incidentes de segurança de maiores proporções (de acordo com critérios e avaliação do BNDES) – potencialmente envolvendo indisponibilidade de processos críticos, vazamento de dados e/ou danos à imagem, reputação ou integridade do BNDES.

14.1.4.1.1.1. A decisão de acionamento da CONTRATADA para tratar os Incidentes Cibernéticos de impacto extremo, bem como sua liberação cabem, única e exclusivamente ao BNDES.
14.1.4.1.1.2. A equipe especializada deve se deslocar e estar presente nas dependências da sede do BNDES no Rio de Janeiro-RJ (ou outra localização no Rio de Janeiro indicada pelo BNDES) a partir da solicitação do BNDES de atendimento presencial.
14.1.4.1.1.3. Durante o período de deslocamento (a partir do acionamento até a presença nas dependências do BNDES), a empresa já deve iniciar o atendimento prévio de forma remota, por meio de equipe especializada.
14.1.4.2. Um exemplo de acionamento do serviço de IRC seria um incidente com ransomware, em que o BNDES demandaria o apoio da CONTRATADA para determinar que sistemas foram afetados e isolá-los, realizar as atividades de contenção, erradicação, recuperação etc (referência: https://www.cisa.gov/stopransomware/ive-been-hit-ransomware).
14.1.4.3. O pagamento referente à execução do serviço será devido somente no caso de acionamento pelo BNDES e aprovação do laudo produzidos ao final.
14.1.4.3.1. Este serviço está dividido em dois tipos de pacotes com duração de 40 (quarenta) horas. Sendo um com atendimento presencial e o outro com atendimento totalmente remoto. A contagem de horas para os níveis de serviço inicia, é suspensa e encerra de acordo com a demanda do BNDES. Já a contagem horas para fiz de consumo do pacote se inicia com o primeiro contato remoto ou presencial, pode ser suspensa pelo BNDES, e se encerra com a demanda do laudo pelo BNDES
14.1.4.3.2. O atendimento remoto poderá ser convertido em presencial caso o BNDES entenda necessário o atendimento presencial durante o desenrolar do atendimento remoto.
14.1.4.3.3. Dois ou mais pacotes podem ser concatenados para atender períodos maiores que 40 (quarenta) horas.
14.1.4.3.4. Durante o atendimento à crise, a CONTRATADA deverá envolver quantos especialistas forem necessários para tratar as diversas matérias envolvidas na crise, mas a contagem de horas não é por profissional, mas sim por horas de prestação do serviço pela CONTRATADA. Entretanto, o preposto técnico será o responsável pela interlocução com o BNDES.
14.1.4.4. O serviço deve contemplar minimamente as seguintes atividades e aspectos:
14.1.4.4.1. Tratamento inicial para cessar o incidente: atuação e apoio técnico para interromper o ataque ou a ameaça de segurança, minimizando o impacto do incidente, bem como implementação de medidas para evitar que o incidente se espalhe para outros ativos de TIC.
14.1.4.4.2. Investigação para identificar as causas, responsabilidades e extensão dos danos: condução de investigação detalhada para determinar como o incidente ocorreu, quais os responsáveis por ele e qual é a extensão dos danos causados.
14.1.4.4.3. Apoio para definição da estratégia de recuperação e restauração de dados: recuperação de dados perdidos ou danificados como resultado do incidente e restauração de sistemas ou rede para seu estado original.
14.1.4.4.4. Serviços forenses/Coleta e Preservação Forense de Dados, apoiando na verificação e na análise dos incidentes, gravando-os em formato adequado para posterior uso em processos administrativos, cíveis e criminais.
14.1.4.4.4.1. Deve atender às normas ABNT ISO/IEC 27037:2013 e. complementar 21 da Instrução Normativa GSI Nº01 de 8 de outubro de 2014;
14.1.4.4.4.2. Os serviços forenses iniciam-se a partir da demanda do BNDES para execução do processo de restauração dos serviços e soluções afetadas. Todo este processo será realizado em conjunto entre a CONTRATADA e as demais equipes de TIC do BNDES.
14.1.4.4.4.3. Devem ser reunidos os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense dos mesmos. Essa atividade será realizada pelo BNDES, com o apoio técnico e ferramental da CONTRATADA.
14.1.4.4.4.4. A CONTRATADA deverá possuir ferramental adequado para a coleta e preservação de evidências considerando as plataformas Windows, Linux e VMware instaladas em servidores e/ou estações do tipo desktop e/ou notebooks;
14.1.4.4.4.5. Tal análise deve ser realizada com o objetivo de identificar a cronologia de eventos (datas, horas, ações, pessoas, locais, ativos, informações etc.), correlacionando todas as informações reunidas, e gerando como produto um laudo sobre o incidente de segurança em questão.
14.1.4.4.4.6. Caso seja necessário a reconstrução do ataque, este deve ser realizado pela CONTRATADA em ambiente controlado, usando-se, por exemplo, uma sandbox. Tal ambiente deve ser de propriedade e controle da CONTRATADA.

14.2. ITEM II - SERVIÇO TÉCNICO DE INTELIGÊNCIA ESPECIALIZADO EM SEGURANÇA CIBERNÉTICA
14.2.1. CONSIDERAÇÕES GERIAS
14.2.1.1. O BNDES e seus colaboradores deverão ter acesso via usuário e senha próprios a todas as ferramentas e consoles dos produtos ofertados pela CONTRATADA e utilizados durante a prestação dos serviços, conforme item 3.17.

14.2.1.1.1. Os perfis de acesso devem ser suficientes para validação das funcionalidades ofertadas, acompanhamento e auditoria das ações realizadas pela CONTRATADA.
14.2.2. ATIVIDADE DE THREAT INTELLIGENCE
14.2.2.1. A CONTRATADA deverá prover, por meio de solução própria ou feeds integrados ao SIEM do BNDES descrito no item 8.2, serviços de inteligência contra ameaças cibernéticas envolvendo pesquisa e desenvolvimento de inteligência e proteção contra ataques cibernéticos.
14.2.2.2. No caso de integração com o SIEM do BNDES, esta integração deverá ser realizada por meio fontes de alimentação – feeds – utilizando os métodos de conexão existentes e suportados pelo SIEM do BNDES.
14.2.2.3. No caso de uso de solução de Threat Intelligence não integrável diretamente no SIEM do BNDES, a solução adotada deverá ser capaz de encaminhar logs e eventos à solução de SIEM do BNDES por algum método suportado pelo SIEM do BNDES.
14.2.2.4. Caso os logs ou eventos enviados pela solução de Threat Intelligence não sejam nativamente reconhecidos pelo SIEM do BNDES, caberá à CONTRATADA construir, no SIEM do BNDES, os logs sources necessários, incluindo propriedades personalizadas, para permitir a correta interpretação dos logs enviados.
14.2.2.5. Independentemente da solução adotada pela CONTRATADA, esta deverá, às suas expensas, integrar pelo menos com 10 (dez) fontes de alimentação – feeds – de threat intelligence.
14.2.2.5.1. Os feeds de threat intelligence a serem utilizados pela CONTRATADA deverão ser submetidos à aprovação do BNDES e atender aos seguintes requisitos:
14.2.2.5.2. Serem providos por fornecedores globais e nacionais na proporção de 50% ou outra autorizada pelo BNDES;
14.2.2.5.3. Realizar monitoramento em categorias de ameaças incluindo: Domínios fraudulentos; Phishings afetando o Brasil; Códigos Maliciosos; Malwares Zero Day; Botnets; Deep e Dark Web; SPAM; Fraudes; Dispositivos Móveis; Advanced Persistent Threats; DNS, URLs e IPs; Mídias Sociais; Infraestrutura Física;
14.2.2.5.4. Realizar priorização de vulnerabilidades;
14.2.2.5.5. Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente do BNDES, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança.
14.2.2.5.6. Essas fontes de Threat Intelligence não se confundem com o serviço de Threat Intelligence do ITEM I. Aqui, as fontes trarão dados filtrados para os ativos indicados pelo BNDES para monitoração no ambiente externo (IP do BNDES, nome de servidores, nome de sistemas, campanhas envolvendo o setor financeiros, itens da BATIC etc) enquanto que as fontes de Threat Intelligence do ITEM I, que deverão ser disponibilizadas pela CONTRATADA para o ITEM I, deverão trazer informações genéricas e gerais para enriquecimento dos eventos do SIEM (IPs suspeitos, CVEs conhecidos, artefatos maliciosos conhecidos etc) e apoio no tratamento dos mesmos.
14.2.2.5.7. O BNDES poderá ainda solicitar a adição de até 5 (cinco) novos feeds ao monitoramento de Threat Intelligence de sua preferência e que deverão ser adquiridos e configurados sem custos adicionais para o BNDES;
14.2.2.5.7.1. Essas feeds podem ser, por exemplo, de provedores renomados pelo mercado ou áreas temáticas: Proofpoint ET Intelligence (reputação de IPs/domínios e exploit kits), abuse.ch URLhaus (URL maliciosas), FBI InfraGard (segurança de infraestrutura), AlienVault Open Threat Exchange etc
14.2.2.5.8. A CONTRATADA será responsável por estabelecer, manter, monitorar integralmente e melhorar criticamente as ferramentas e processos necessários à execução integral de threat Intelligence para o BNDES.
14.2.2.5.9. A CONTRATADA deverá realizar por meio de processos contínuos, estruturados e proativo as atividades de Caça às Ameaças (Threat Hunting). Tais atividades deverão considerar os baselines definidos e deverão ser feitas baseadas em:
14.2.2.5.9.1. Hipóteses definidas pela CONTRATADA em conjunto com o BNDES;
14.2.2.5.9.2. Indicadores de Comprometimento (Indicators of Compromise - IOCs) de casos relevantes, conforme proposta da própria CONTRATADA ou do BNDES;
14.2.2.5.9.3. As informações obtidas (match) pela CONTRATADA por meio do serviço de Threat Intelligence e Threat Hunting deverão acionar o BNDES para avaliação e eventual mitigação da ameaça identificada.
14.2.2.6. A CONTRATADA deverá integrar seu sistema de busca de ameaças à BATIC para que o BNDES seja comunicado sempre que for identificada alguma informação/achado relativo ao mesmo e a sua infraestrutura, conforme os dados existentes na BATIC. O comunicado deve conter, no mínimo, a descrição do achado, data e hora do achado, origem/fonte e conteúdo, se aplicável.
14.2.3. ATIVIDADE DE DRP (BRAND INTELLIGENCE – DIGITAL RISK PROTECTION)
14.2.3.1. O serviço deve monitorar a reputação do BNDES, levantando e filtrando menções, dados e outros termos sobre a instituição na Internet, permitindo que o time de segurança possa proativamente detectar e agir em tempo real, antes que o BNDES seja prejudicado.
14.2.3.2. O serviço deverá possuir a capacidade de monitorar até 500 (quinhentos) ativos. Exemplos de ativos: nome de pessoas, CPF, CNPJ, endereços IP/blocos CIDR, nome e sigla da instituição e seus produtos, e-mails, siglas internas do BNDES etc.

14.2.3.3. Deverá identificar, reconhecer, coletar, analisar, validar a veracidade, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet da deep e dark web, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis.

14.2.3.3.1. A solução de monitoramento deverá, também, além de realizar as coletas dos eventos, realizar o devido processamento, como: extração de textos encontrados em imagens (OCR), transcrições de áudios e vídeos e indexação dos eventos coletados

14.2.3.4. A solução da CONTRATADA deverá possuir e estar integrada a uma honeynet para coleta da tentativa de exploração de vulnerabilidade e, por demanda do BNDES, deverá instalar um ou mais coletores na infraestrutura do BNDES, limitado a 10 (dez) coletores nas redes internas e externas.

14.2.3.5. A solução deverá monitorar, no mínimo, 5000 (cinco mil) fontes de informações públicas e privadas e, no mínimo, coletar diariamente informações de pelo menos 50 (cinquenta) fontes privadas e relevantes de inteligência sobre ameaças disponíveis pelo mundo, de categorias como phishing, código, propriedade intelectual, chaves/senhas, botnets, internet profunda (deep web), spam, aplicativos falsos e documentos confidenciais.

14.2.3.5.1. As fontes devem ser providas por fornecedores globais e nacionais na proporção de 50% ou outra autorizada pelo BNDES.

14.2.3.6. Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: X (antigo Twitter), Facebook, YouTube, Instagram, TikTok, LinkedIn, Discord, grupos de WhatsApp, grupos de Telegram, canais de IRC, Pastebin e similares, Scribd, ReclameAQUI, 4Shared e Github e similares. É desejável, para atendimento aos níveis de serviço exigidos, que a ferramenta monitore, pelo menos, 60 (sessenta) mil grupos.

14.2.3.7. A monitoração deve contar com as informações obtidas nos principais sites relacionados à Segurança da Informação como: RiskIQ; Recorded Future; abuse.ch; Critical Stack; Dshield; Malc0de; Malwaredomains.com; Proofpoint (Emerging Threats Intelligence); SANS; Shadowserver; PastesSites; Darknet; Rede Tor; Darknet; I2P; Decentralized TLDs; Whois; Usenet; Private Leaks; Leaks COMB; Bot Logs; WikiLeaks; Public Leaks; Dumpster; Sci-Hub, Have I Been Pwned, salientando que esta lista é meramente exemplificativa.

14.2.3.8. Deverá possuir métodos de coleta de redes sociais, páginas, portais e fóruns na internet superficial, profunda e oculta (“clear web”, “deep web” e “dark web”).

14.2.3.9. Deverá monitorar informações sensíveis e vazamento de credenciais relacionados ao BNDES, considerando as palavras chaves indicadas pelo BNDES.

14.2.3.10. Deve monitorar domínios que contenham variações da marca do BNDES, a exemplo de typosquatting, variações de Top Level Domain e Homoglifos.

14.2.3.11. Informar anomalias nos registros de nomes dos domínios monitorados ("whois", registros DNS, etc).

14.2.3.12. A solução deve ser capaz de identificar práticas maliciosas de spamdexing considerando os ativos indicados para busca pelo BNDES.

14.2.3.13. Deve monitorar informações/movimentos de exploração de vulnerabilidades conhecidas (CVEs) e grupos APTs atuantes de acordo com os ativos indicados pelo BNDES.

14.2.3.13.1. É desejável, para atendimento aos níveis de serviço exigidos, que a solução a ser ofertada monitore os principais grupos de ransomware conhecidos e disponibilizar alertas específicos para este tipo de ameaça, ao que concerne aos ativos de interesse do BNDES. A exemplo dos principais grupos, destacamos: Arvin, Atomsilo, Against the West, Babuk, BianLian, Black Basta, Black Byte, Blackbyte Auction, BLACKCAT (ALPHVM), Blackshadow, Bl@ckt0r, 54BB47H Blog, Cheers, Clop, Continews, CRYP70N1C0D3, Cuba, Daixin, Dark Leak, DataLeak, Donut, Entropy, Everest, Free Civilian, Grief, Hive, Industrial Spy, Karakurt, Kelvin Security, Lapsus$, LockBit, Lock Data, Lorenz, LV Blog, Mallox, Marketo, Medusa, Midas, Mindware, Moses, Night Sky, 0mega, Onyx, Pandora, Pay2Key, Payload.bin, Project Relic, Pysa, Qilin, Quantum, Ragnar Locker, Ransomexx, Ransom House, Red Alert, Revil, Rook, RoyalLanding, Snatch, Suncrypt, Vendetta, Vice Society, Xing Locker e Yanluowang.

14.2.3.14. Monitorar as lojas de aplicativos Apple Store e Google Play com o objetivo de detectar aplicativos maliciosos que estejam relacionados com o BNDES. É de responsabilidade da CONTRATADA providenciar a remoção de aplicações falsas e maliciosas (takedown) através de parcerias com as lojas de aplicativos, quando solicitadas pelo BNDES;

14.2.3.15. Realizar o serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes do BNDES.

14.2.3.16. Realizar o serviço de TAKEDOWN para retirada do ar de perfis falsos de executivos e do próprio BNDES e suas marcas em redes sociais.

14.2.3.17. Realizar o serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso do BNDES ou que permitam burlar os meios de proteção desses direitos.

14.2.3.18. Realizar o serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque a reputação da instituição ou ainda a tentativa de captura de credenciais do BNDES.
14.2.3.19. Realizar o serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, X – o antigo Twittter, Linkedin, Instagram, YouTube, TikTok etc.) que tenham relação com o BNDES e não seja autorizado por essa instituição.
14.2.3.20. Realizar o serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas do BNDES, divulgações relacionadas a clientes e empregados do BNDES, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial.
14.2.3.21. A ação de TAKEDOWN deve ter abrangência nacional e internacional e deverá ocorrer a pedido do BNDES ou mediante sua autorização
14.2.3.22. Caso não seja possível a realização da ação de TAKEDOWN, a CONTRATADA deverá apresentar o embasamento técnico e jurídico para análise pelo BNDES que não necessariamente acatará o pedido.
14.2.3.23. Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar e deduplicar informações, gerando listas acionáveis de inteligência contra ameaças;
14.2.3.24. A solução empregada pela CONTRATADA deve possuir uma console gráfica via browser que:
14.2.3.24.1. Não limite quantidade de recursos pesquisados;
14.2.3.24.2. Permita pesquisa direcionada através da monitoração de palavras pré-selecionadas fornecidas;
14.2.3.24.3. Possua modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas.
14.2.3.24.4. Possibilite salvar os resultados das pesquisas já realizadas e apresentar os dados filtrados em painéis com as principais fontes identificadas na busca.
14.2.3.24.5. Possua um campo de descrição em que os analistas de segurança cibernética do BNDES, ou da CONTRATADA, possam contextualizar as informações associadas aos eventos. Este recurso deve facilitar o consumo das informações pelas equipes de segurança cibernética, a exemplo das equipes do serviço de CSOC;
14.2.3.24.6. Permita a pesquisa de informações nos seguintes contextos: Ameaças cibernéticas; Resposta a incidentes; Prevenção de perdas de dados; Proteção de Marca; Risco de Terceiros; Fraude; Quaisquer outras fontes disponíveis, ou que venham a se tornar disponíveis.
14.2.3.24.7. Apresente a descoberta de páginas web de “phishing”, utilizando o nome dos recursos pesquisados, a marca, identidade visual, domínios e ativos de informação que serão protegidas;
14.2.3.24.8. Apresente a verificação de sites suspeitos de phishing para domínios solicitados pelo BNDES, ou que tenham sido levantados pela CONTRATADA. Para essa verificação deve-se utilizar, entre outras, as seguintes entidades reguladoras: ICANN (Internet Corporation for Assigned Names and Numbers) e Registro.Br (Registro de Domínios para a Internet do Brasil);
14.2.3.24.9. Apresente a detecção de domínios recentemente registrados que possam oferecer riscos e serem utilizados de forma maliciosa contra o BNDES como, por exemplo: Variações comuns de nomes; Permutações de caracteres; e desvio de URL (typosquatting).
14.2.3.25. Os resultados das pesquisas na console gráfica da solução devem, no mínimo:
14.2.3.25.1. Retornar os seguintes campos: contexto pesquisado, data e hora, idioma, endereço web/deep web/dark web, conteúdo original completo;
14.2.3.25.2. Permitir que as pesquisas sejam salvas para posterior verificação.
14.2.3.25.3. Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo ordenáveis por data e hora da ocorrência mais recente para a mais antiga, e por tema, ameaça, entre outros;
14.2.3.25.4. Permitir a atualização automática do resultado de pesquisas anteriormente realizadas com alertas visuais dessas atualizações ou disponibilizar portal customizável pelo usuário com suas próprias consultas;
14.2.3.25.5. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;
14.2.3.25.6. Possuir interface de fácil visualização para demonstrar os resultados das buscas por cada categoria de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web);
14.2.3.25.7. Disponibilizar uma tela com informações consolidadas para visualização das pesquisas realizadas e alertas cadastrados;
14.2.3.25.8. Permitir exportar qualquer pesquisa realizada de forma manual ou automática para um dos seguintes formatos: JSON, HTML, PDF, CSV, XLSX, DOCX, ou em outros formatos aderentes ao E-Ping.
14.2.3.26. A CONTRATADA deve ser comunicar, pelo meio definido pelo BNDES, sempre que for identificada alguma informação/achado relativo ao BNDES. O comunicado deve conter a descrição do

achado, data e hora (incluindo a timezone) do achado, origem/fonte e conteúdo, se aplicável, além de classificado conforme as TTPs do framework do Mitre Att&ack. Exemplo: No caso de vazamento de senha, a data do vazamento, senha vazada (quando disponível), forma do vazamento (como as credenciais foram obtidas, quando disponível) e se as credenciais foram obtidas por divulgação pública, quando disponível.
14.2.3.27. Para efeito de reporte o serviço deverá gerar eventos em, pelo menos, 3 categorias:
14.2.3.27.1. Eventos de Informação: Estes eventos não requerem qualquer ação. Este grupo de eventos deve ser utilizado quando não há risco cibernético aos ativos de TIC e de informação monitorados, por exemplo, uma menção simples em uma rede social contendo o nome dos ativos de TIC e de informação do BNDES;
14.2.3.27.2. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento que represente risco cibernético em relação aos ativos de TIC e de informação monitorados, por exemplo, uma menção na internet, deep ou dark web, ou qualquer outro meio monitorado, com contexto de ameaças e/ou ataques cibernéticos direcionados contra o BNDES;
14.2.3.27.3. Eventos de Exceção: Estes eventos são aqueles que sugerem que os princípios da confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade, privilégio mínimo, necessidade de conhecer, proteção de dados pessoais e proteção da privacidade foram impactados negativamente. São exemplos desses eventos: detecção de vazamento de dados de interesse do BNDES e venda de informações atreladas aos ativos de informação monitorados em canais de fraude.

15. IMPLANTAÇÃO E INÍCIO DOS SERVIÇOS – ITENS I e II

15.1. Após a assinatura do Contrato, o BNDES poderá solicitar reuniões com a CONTRATADA, a fim de esclarecer obrigações contratuais, questões relacionadas com o início da prestação do serviço, além de verificar as providências que estão sendo tomadas pela CONTRATADA no sentido de iniciar a prestação do serviço de acordo com os comandos desta Especificação Técnica.
15.2. Após a assinatura do Contrato, cada CONTRATADA deverá apresentar, em até 15 (quinze) dias:
15.2.1. Relação dos profissionais designados que formarão a equipe de prepostos da CONTRATADA, técnico e administrativo, assim como a comprovação do vínculo jurídico destes profissionais com a CONTRATADA e certificações, conforme item 4;
15.2.2. Termos de Confidencialidade assinados pelos representantes legais da CONTRATADA e pelos prepostos envolvidos diretamente na prestação de serviços;
15.2.3. Declaração de Informações para Fornecimento - DIF, adequadamente preenchida, sob pena de instauração de procedimento punitivo para aplicação de penalidade, e de retenção tributária, pelo BNDES, nos casos previstos em lei, da alíquota que entender adequada. As informações inseridas na Declaração de Informações para Fornecimento – DIF não deverão divergir das constantes do documento fiscal ou equivalente legal;
15.2.4. Garantia Contratual, conforme item 25;
15.2.5. Dados de contato e escalation list para acionamento do serviço até, no mínimo, o nível de direção da CONTRATADA;
15.2.6. Nome completo, CPF, telefone e e-mail do preposto técnico e administrativo e do DPO da CONTRATADA;
15.2.7. Cronograma previsto para a fase de implantação do respectivo ITEM;
15.2.8. Operadoras que serão CONTRATADAS para provimento do serviço de conexão (dedicado, Internet etc);
15.2.9. Diagrama de integrações e funcionamento da solução proposta; e
15.2.10. Planilha eletrônica contendo a lista dos softwares/hardwares especializados que serão utilizados na prestação dos serviços com a descrição da integração com os softwares adotados pelo BNDES. No caso das soluções que serão instaladas no BNDES, deverá ser acrescentado os requisitos de alimentação elétrica e de rede, além do plano de face do rack (quantidade de rack units/U).
15.3. O BNDES irá avaliar a documentação, fornecendo uma resposta em até 15 (quinze) dias quanto a aprovação ou não da documentação apresentada.
15.3.1. Durante o prazo acima, o BNDES poderá pedir substituições ou documentação complementar para a CONTRATADA com objetivo de que todos os requisitos desta Especificação Técnica e seus anexos sejam atendidos. A nova documentação deverá ser entregue pela CONTRATADA em até 5 (cinco) dias corridos quando será reiniciado o período de avaliação prevista no caput até que a documentação esteja completa e aprovada pelo BNDES.
15.4. Após a conclusão da fase de entrega da documentação, conforme item 15.3, será emitido o “Termo de Recebimento Provisório (TRP)” para o respectivo ITEM, em até 5 (cinco) dias, pela Comissão de Recebimento de Materiais e Serviços.
15.5. Após a aprovação da documentação requerida no item 15.2 deste Termo de Referência, o BNDES poderá autorizar a CONTRATADA a iniciar a implantação do serviço do respectivo ITEM, em até 20 (vinte) dias, conforme descrito abaixo.
15.6. A implantação deverá respeitar o horário de expediente do BNDES, das 9h às 20h, e de acordo com a disponibilidade de empregados do BNDES ou outros colaboradores designados para acompanhamento das atividades de implantação.

15.6.1. ITEM I
15.6.1.1. Após a autorização do BNDES, a CONTRATADA deverá, em até 90 (noventa) dias, entregar/concluir:
15.6.1.1.1. Relação dos profissionais designados que farão parte da equipe da CONTRATADA que prestará os serviços, em regime 24x7, assim como a comprovação do vínculo jurídico dos profissionais com a CONTRATADA e certificações, conforme item 4;
15.6.1.1.2. Termos de Confidencialidade assinados pelos profissionais a envolvidos diretamente na prestação de serviços;
15.6.1.1.3. Declaração assinada pelos profissionais envolvidos diretamente na prestação de serviços de que tomaram ciência e sanaram eventuais dúvidas sobre os tópicos descritos no item 4.15;
15.6.1.1.4. A implantação da conexão entre os datacenters do BNDES e os CSOCs e/ou datacenters da CONTRATADA, conforme item 9;
15.6.1.1.5. A implantação das soluções em softwares, feeds e integrações com o ambiente do BNDES de acordo com os requisitos previstos nestas Especificações Técnicas, conforme item 8.2.2;
15.6.1.1.6. A Base de Ativos de TIC – BATIC, conforme item 14.1.3.4;
15.6.1.1.7. Uma lista de, no mínimo, 20 (vinte) casos de uso da biblioteca de caso de uso da CONTRATADA para escolha pelo BNDES de quais deverão ser implantados em seu SIEM e no SOAR;
15.6.1.1.8. A revisão e automação no SOAR, no mínimo, de três casos de uso listados no item 6 que serão informados pelo BNDES (DLP, PHISHING, DDOS). Deverão ser produzidos os roteiros (playbooks) para tratamento dos incidentes gerados a partir dos eventos e alertas configurados no SIEM;
15.6.1.1.9. O cadastramento das credenciais de acesso do BNDES e respectivos acessos para verificação do funcionamento da solução, conforme item 3.17, e fornecer a respectiva capacitação de uso, conforme item 3.20; e
15.6.1.1.10. A documentação da solução da CONTRATADA (as-built), formas de acesso e uso etc.
15.6.1.2. Durante a implantação dos softwares a CONTRATADA poderá, a seu critério, alocar profissionais especializados adicionais com formação distinta dos profissionais que atuarão no serviço de forma continuada, desde que não implique em custos adicionais para o BNDES.
15.6.2. ITEM II
15.6.2.1. Após a autorização do BNDES, a CONTRATADA deverá, em até 90 (noventa) dias, entregar/concluir:
15.6.2.1.1. Relação dos profissionais designados que farão parte da equipe da CONTRATADA que prestará os serviços, em regime 24x7, assim como a comprovação do vínculo jurídico dos profissionais com a CONTRATADA e certificações, conforme item 4;
15.6.2.1.2. Termos de Confidencialidade assinados pelos profissionais a envolvidos diretamente na prestação de serviços;
15.6.2.1.3. Declaração assinada pelos profissionais envolvidos diretamente na prestação de serviços de que tomaram ciência e sanaram eventuais dúvidas sobre os tópicos descritos no item 4.15;
15.6.2.1.4. A implantação da conexão entre os datacenters do BNDES e os datacenters da CONTRATADA, conforme item 9;
15.6.2.1.5. A implantação da solução de feeds e integrações com o ambiente do BNDES de acordo com os requisitos previstos nestas Especificações Técnicas, conforme item 14.2;
15.6.2.1.6. Montar, em conjunto com o BNDES, a lista de ativos monitorados, conforme item 14.2.3.2;
15.6.2.1.7. Cadastrar as credenciais de acesso do BNDES e respectivos acessos para verificação do funcionamento da solução, conforme item 3.17, e fornecer a respectiva capacitação de uso, conforme item 3.20; e
15.6.2.1.8. A documentação da solução da CONTRATADA (as-built), formas de acesso e uso etc.
15.6.2.2. Durante a implantação dos softwares a CONTRATADA poderá, a seu critério, alocar profissionais especializados adicionais com formação distinta dos profissionais que atuarão no serviço de forma continuada, desde que não implique em custos adicionais para o BNDES.
15.7. O BNDES irá avaliar a implantação, testar a efetividade das soluções, fornecendo uma resposta em até 30 (trinta) dias quanto a aprovação ou não desta.
15.7.1. Durante o prazo acima, o BNDES poderá pedir ajustes na implantação para a CONTRATADA com objetivo de que todos os requisitos desta Especificação Técnica e seus anexos sejam atendidos. O ajuste deverá ser entregue pela CONTRATADA em até 5 (cinco) dias quando será reiniciado o período de avaliação prevista no caput até que a implantação esteja completa e aprovada pelo BNDES.
15.8. Após a conclusão da fase de avaliação da implantação, conforme item 15.7, será emitido o “Termo de Recebimento Definito (TRD)” para o respectivo ITEM, em até 5 (cinco) dias, pela Comissão de Recebimento de Materiais e Serviços.
15.8.1. Excepcionalmente, a Comissão de Recebimento de Materiais e Serviços poderá emitir um “Termo de Recebimento Definito (TRD)” com ressalvas, portanto, com o recebimento parcial do serviço. Nesse caso, a CONTRATADA, para o item recebido parcialmente, fará jus ao pagamento parcial, conforme a tabela abaixo, até que receba o “Termo de Recebimento Definito (TRD)” sem ressalvas.

		Percentual do Valor Total do ITEM que será descontado até a regularização da(s) ressalva(s)			
ITEM I	**Sem TRD do respectivo serviço**	**Aceite com ressalvas às ferramentas de software**	**Aceite com ressalvas às integrações**	**Aceite com ressalvas à formação da equipe**	**Aceite sem ressalvas**
Implantação	Sem pagamento	Sem pagamento	Sem pagamento	Sem pagamento	100%
Serviços do ITEM I (CSIRT+GVUL+IRC)	Sem pagamento	30%	20%	50%	100%
ITEM II	**Sem TRD do respectivo serviço**	**Aceite com ressalvas às ferramentas de software**	**Aceite com ressalvas às integrações**	**Aceite com ressalvas à formação da equipe**	**Aceite sem ressalvas**
Implantação	Sem pagamento	Sem pagamento	Sem pagamento	Sem pagamento	100%
Serviços do ITEM II (CTI+DRP)	Sem pagamento	40%	20%	40%	100%

15.8.1.1. Um exemplo da situação acima, seria a CONTRATADA para o serviço do ITEM I, implantar as ferramentas de software e as integrações, devidamente verificadas pelo BNDES, mas não apresentar a equipe com a formação requerida. Nesse caso, a CONTRATADA faria jus ao pagamento mensal do serviço do ITEM I com desconto de 50% (cinquenta por cento) do valor do respectivo serviço, por até 90 (noventa) dias, sem prejuízo a descontos sobre o valor que estiver sendo pago em razão de eventual descumprimento de nível de serviço.
15.8.1.2. A CONTRATADA deverá sanar todas as pendências para obtenção do "Termo de Recebimento Definito (TRD)" sem ressalvas em até 90 (noventa) dias após a emissão do "Termo de Recebimento Definito (TRD)" com ressalvas. Caso esse prazo não seja observado, a CONTRATADA estará sujeita às penalidades previstas no item 23.1.3.
15.8.1.3. A CONTRATADA não fará jus a pagamento complementar retroativo ao período durante o qual o serviço foi aceito com ressalva ou não aceito.
15.9. A obtenção do TRD do respectivo ITEM é condição para o início dos pagamentos das parcelas mensais do respectivo serviço.
15.10. Nos primeiros 60 (sessenta) dias corridos após o início da prestação do serviço, após emissão do TRD, a CONTRATADA receberá do BNDES as instruções, diretrizes e informações pertinentes aos serviços prestados.
15.10.1. Durante o referido período, os indicadores de níveis de serviço serão apurados, mas não ensejarão ajustes de pagamento em caso de descumprimento dos níveis de serviço definidos, consistindo em período de adaptação.
15.10.2. Os compromissos quanto aos níveis de serviço previstos nos itens 17 e 18 serão exigidos pelo BNDES integralmente após o término do período de implantação
15.11. O Gestor do Contrato poderá alterar o prazo das etapas previstas na implantação, desde que o prazo máximo da implantação não ultrapasse 180 (cento e oitenta) dias e a alteração não prejudique as atividades do BNDES. Tal necessidade de ajuste pode decorrer dos parâmetros de implantação definidos durante a fase de planejamento desta, por exemplo.

Fases	Prazos	Responsável
Documentação inicial	15	CONTRATADA
Avaliação documentação inicial	15	BNDES
Autorização Implantação	20	BNDES
Emissão TRP	5	BNDES
Implantação	90	CONTRATADA
Avaliação implantação	30	BNDES
Emissão TRD	5	BNDES
Total	180	Até 6 meses

16. REGIME DE EXECUÇÃO – ITENS I e II

16.1. ITENS I e II
16.1.1. O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), acrescido de 24 horas, em caso de ano bissexto.
16.1.2. Durante todo o contrato, a CONTRATADA de forma ininterrupta em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), acrescido de 24 horas, em caso de ano bissexto, deverá assegurar a disponibilidade de canais de comunicação para imediato atendimento do BNDES e endereçamento das suas demandas.

16.1.2.1. Obrigatoriamente deverá disponibilizar um número de telefone no Brasil que permita o integral acionamento e validação das operações em andamento.
16.1.2.2. De maneira a complementar, para suporte aos processos alvos desta contratação, demais canais de comunicação, tais como ferramenta de ITSM definida pelo BNDES, WhatsApp, telefone, Microsoft Teams e e-mail, não se limitando a estas, também poderão ser utilizadas.
16.1.2.3. A definição do melhor uso e propósito de cada um deste canais será dado pelo BNDES. Uma proposta seria:
16.1.2.3.1. Telefone e ferramentas de comunicação instantânea para demandas urgentes;
16.1.2.3.2. Ferramenta de RTIR do BNDES - Fila específica para a CONTRATADA enviar as demandas para a equipe de ETIR do BNDES (situações novas que precisam de definição pelo BNDES etc);
16.1.2.3.3. Ferramenta de ITSM do BNDES (Remedy) para registro no módulo de problema das vulnerabilidades em ativos do BNDES, que deverão ser tratadas pela equipe de TIC do BNDES;
16.1.2.3.4. Ferramenta de ITSM da CONTRATADA para processos já definidos pelo BNDES (com playbook/runbook) e demandas não urgentes que serão tratados pela CONTRATADA e acompanhados pelo BNDES; e
16.1.2.3.5. E-mail para demais comunicações administrativas ou de maior complexidade.
16.1.2.4. A forma de execução e acompanhamento dos serviços devem ser desenvolvidas conforme os itens 17 e 18.
16.1.3. O BNDES e a CONTRATADA se reunirão periodicamente, no mínimo a cada mês, para avaliação técnica do andamento da execução contratual, apresentação de pontos de melhoria e transferência de conhecimentos. Reuniões de monitoramento dos serviços ou outras reuniões extraordinárias poderão ser convocadas pelo BNDES sendo obrigação da CONTRATADA atender às convocações.

17. CATÁLOGO DE SERVIÇOS – ITENS I e II

17.1. Neste item estão descritas as tarefas contínuas e sob demanda que os serviços descritos nas Especificações Técnicas compreendem, além dos respectivos níveis de serviço associados às tarefas. Também estão descritas as falhas relacionadas com a prestação dos serviços e as respectivas perdas de pontos associadas aos descumprimentos dos níveis de serviço (NMS, nível mínimo de serviço) e às ocorrências de falhas.
17.2. A tabela “NMS x Prazos x Perdas” estabelece os relacionamentos entre os “Identificadores NMS”, os “Prazos de Resolução” e as “Perdas de Pontos” conforme detalhado a seguir:

NMS x Prazos x Perdas de Pontos

Identificador NMS	Prazo de Resolução	Perda de Pontos por descumprimento do prazo
A01	15 minutos	0,01 por minuto
A02	30 minutos	0,01 por minuto
A03	60 minutos	0,01 por minuto
A04	90 minutos	0,01 por minuto
A05	120 minutos	0,01 por minuto
A06	150 minutos	0,01 por minuto
A07	180 minutos	0,01 por minuto
A08	210 minutos	0,01 por minuto
A09	240 minutos	0,01 por minuto
A10	1h	0,5 por hora
A11	2h	0,5 por hora
A12	4h	0,5 por hora
A13	8h	0,5 por hora
A14	12h	0,5 por hora
A15	24h	0,5 por hora
A16	1 dia	1 por dia
A17	1 minuto	0,01 por minuto
A18	2 dias	0,2 por dia
A19	4 dias	0,1 por dia
A20	7 dias	0,2 por dia

A21	7 dias	0,1 por dia
A22	15 dias	0,1 por dia
A23	30 dias	0,5 por dia
A24	45 dias	0,1 por dia
A25	60 dias	0,1 por dia
A26	2 dias	0,1 por dia

17.3. A Tabela abaixo lista as tarefas e níveis de serviço relacionados a cada atividade de cada ITEM desta Especificação Técnica.

Identificador	Descrição / Detalhamento / Exemplos	Nível Mínimo de Serviço (NMS)
APLICÁVEIS AOS ITENS I E II		
GER01	Indisponibilidade da solução da CONTRATADA	A03
GER02	Violação de um ou mais indicadores de desempenho da solução da CONTRATADA	A03
GER03	Falha de acesso e/ou Indisponibilidade e/ou funcionamento irregular de funcionalidade na solução da CONTRATADA, incluído as atividades de manutenção dos usuários do BNDES	A16
GER04	Indisponibilidade ou falta de atualização de feed de informação sobre ataques, ameaças, vulnerabilidades, base de conhecimento da solução da CONTRATADA etc.	A16
GER05	Configurar e/ou Alterar feed de informação sobre ataques, ameaças, vulnerabilidades etc.	A23
GER06	Ajuste do conteúdo de template/padrão de relatório, boletim/checklist etc.	A20
GER07	Indisponibilidade de integração entre componentes da solução da CONTRATADA e ambiente de TIC do BNDES	A13
GER08	Envio do boletim/checklist de segurança fora do horário agendado	A03
GER09	Aplicação de atualização de patches ou fixes na solução da CONTRATADA	A22
GER10	Aplicação de atualização major de versão ou troca da solução da CONTRATADA	A23
GER11	Ajuste ou criação de dashboard na solução da CONTRATADA	A20
GER12	Elaborar relatório analítico e/ou exportar dados contendo informações, indicadores e métricas relativos aos serviços prestados	A20
GER13	Retorno, pela CONTRATADA, de pedido de informação/orientação realizado pelo BNDES por qualquer meio de comunicação previsto	A03
GER14	Ajuste, solicitado pelo BNDES, de relatório, laudo ou outro tipo de documento/informação prestada pela CONTRATADA	A18
GER15	Utilização de cada conexão dedicada e/ou Internet/VPN superior a 90% por mais de 10 minutos	A17
GER16	Ajuste em requisitos de segurança como: controle de acesso a solução da CONTRATADA, configurações, guarda de logs, segurança física do CSOC, guarda e transmissão dos dados do BNDES, adequação a normativos etc.	A20
GER17	Realizar a remoção definitiva (de forma irrecuperável parcial ou totalmente) das informações manejadas durante a prestação dos serviços ou mediante solicitação do BNDES	A20
GER18	Substituição de profissional a partir da notificação pelo BNDES	A22
GER19	Demais solicitações do BNDES, não críticas, sem um nível de serviço específico	A20
GER20	Demais solicitações do BNDES, críticas, sem um nível de serviço específico	A11
APLICÁVEIS AO ITEM I		
GVUL01	Comunicar e registrar no ITSM/RTIR vulnerabilidade para ativo de TIC de criticidade 0 e/ou sem classificação de criticidade	A06
GVUL02	Comunicar e registrar no ITSM/RTIR vulnerabilidade para ativo de TIC de criticidade 1	A05

GVUL03	Comunicar e registrar no ITSM/RTIR vulnerabilidade para ativo de TIC de criticidade 2	A04
GVUL04	Comunicar e registrar no ITSM/RTIR vulnerabilidade para ativo de TIC de criticidade 3	A03
GVUL05	Comunicar e registrar no ITSM/RTIR vulnerabilidade para ativo de TIC de criticidade 4	A02
GVUL06	Comunicar e registrar no ITSM/RTIR vulnerabilidade com CVSS maior ou igual a 7 (sete)	A02
GVUL07	Executar levantamento de vulnerabilidades e gerar o relatório de vulnerabilidades - 10 ativos	A19
GVUL08	Executar levantamento de vulnerabilidades e gerar o relatório de vulnerabilidades - 1000 ativos	A20
GVUL09	Atualizar base de dados de ativos de TIC - BATIC	A20
GVUL10	Elaborar baseline de segurança, como CIS-Control ou outro	A23
GVUL11	Elaborar ação para correção de vulnerabilidade	A16
GVUL12	Executar auditoria de configuração de ativos de rede, regulação e/ou de sistemas operacionais com relatório - 10 ativos	A19
GVUL13	Executar auditoria de configuração de ativos de rede, regulação e/ou de sistemas operacionais com relatório - 1000 ativos	A20
CSIRT01	Atualização ou criação de regras de correlação no SIEM, incluindo a documentação do caso de uso	A20
CSIRT02	Atualização ou criação de automação no SOAR de caso de uso do SIEM, incluindo a documentação	A23
CSIRT03	Tratamento de incidentes de segurança (triagem, investigação, resposta, documentação etc) automatizados completamente pelo SOAR	A01
CSIRT04	Tratamento de incidentes de segurança (triagem, investigação, resposta, documentação etc) automatizados parcialmente pelo SOAR	A03
CSIRT05	Tratamento de incidentes de segurança (triagem, investigação, resposta, documentação etc) não automatizado	A16
CSIRT06	Tratamento de incidentes de segurança (triagem, investigação, resposta, documentação etc) não automatizado e não documentado	A18
CSIRT07	Comunicar sobre alteração da linha base de tráfego/logs enviados ao SIEM	A18
CSIRT08	Comunicado de ameaça crítica do tipo "zero day" pertinente ao ambiente do BNDES	A02
IRC01	Início da atuação remota	A03
IRC02	Início da atuação on-site	A12
IRC03	Retorno, pela CONTRATADA, de pedido de informação/orientação, durante crise de SI, realizado pelo BNDES por qualquer meio de comunicação previsto	A01
IRC04	Produção do Laudo sobre crise de SI com as devidas evidências	A20
APLICÁVEIS AO ITEM II		
THIN01	Comunicado de ameaça crítica do tipo "zero day" pertinente ao ambiente do BNDES	A02
THIN02	Comunicado de ameaça para grupo de ativos indicados como de interesse pelo BNDES (nome de pessoas, sigla da instituição, e-mails etc)	A05
THIN03	Comunicado de ameaça para demais ativos do BNDES (que possam ter relação com o negócio do BNDES, Sistema Financeiro, Bancos, Office 365 etc)	A16
DRP01	Configuração e/ou Alteração de monitoramento de ativo (nome de pessoas, sigla da instituição, e-mails etc) e/ou coletor da Honeynet	A16
DRP02	Realizar o serviço de TAKEDOWN	A16
DRP03	Comunicar achado para grupo de termos ou situações indicadas como críticas pelo BNDES	A05
DRP04	Produção de Relatório estratégico sobre TTPs mais relevantes na região e/ou seguimento de negócio do BNDES	A20
DRP05	Comunicar achado para demais situações envolvendo o BNDES	A16

17.4. Legenda das colunas:

17.4.1. A coluna “Identificador da tarefa” define uma identificação única alfanumérica para cada uma das tarefas.
17.4.2. A coluna “Descrição / Detalhamento / Exemplos / Itens referentes” contém as informações básicas para entendimento (não exaustivas) de cada tarefa que devem ser observadas na sua execução.
17.4.3. A coluna “Nível Mínimo de Serviço (NMS)” estabelece o nível de serviço requisitado para cada tarefa e o respectivo "Identificador NMS”.
17.4.4. A coluna “Perda de pontos por descumprimento do prazo” informa a quantidade de pontos que será perdida ao longo do tempo em caso de descumprimento dos prazos de resolução exigidos.
17.4.4.1. A perda máxima de pontos para cada tarefa solicitada (chamado) pelo BNDES no mês de referência será de 3 (três) pontos. O objetivo é evitar que apenas um chamado possa causar um ajuste de pagamento máximo na fatura correspondente.
17.4.4.2. Caso ocorram descumprimentos (em diferentes chamados) para um mesmo tipo de tarefa em 3 (três) meses consecutivos, a critério do BNDES, poderá ser aumentado o valor do limitador para 6 (seis) pontos para apenas esse tipo de tarefa a partir desse 3º (terceiro) mês consecutivo (inclusive). O retorno ao valor original poderá ocorrer quando o BNDES perceber uma evolução efetiva no processo de execução deste tipo de tarefa pela CONTRATADA.
17.4.4.3. Caso haja mais de um descumprimento (em diferentes chamados) para um mesmo tipo de tarefa, o limitador será aplicado para cada chamado descumprido de forma individual.
17.4.4.4. Caso uma mesma tarefa (chamado) continue ainda aberta (em execução) nos meses seguintes, haverá nova contabilização de perda de pontos em função do prazo decorrido para cada mês. Tal contabilização deverá obedecer ao limitador definido anteriormente no item 17.4.4.1. Deste modo, é possível, por exemplo, que um mesmo chamado provoque, por exemplo, a perda de 1,5 (um vírgula cinco) pontos em um mês e mais 1,5 (um vírgula cinco) pontos no mês seguinte, caso o descumprimento persista.
17.4.4.5. Para as tarefas que ocasionem a perda de pontos por tempo transcorrido, a perda dar-se-á mesmo em caso de uma fração do tempo transcorrido. Por exemplo: em caso de perda de 0,1 ponto por dia, ocorrerá a perda de 0,1 ponto caso a falha seja solucionada em até um dia após o tempo limite (isto é, pela fração do dia). Ainda no exemplo anterior, caso a falha seja solucionada em mais de 1 dia a até 2 dias após o tempo limite, ocorrerá a perda de 0,2 ponto.
17.4.5. Dada a natureza evolutiva do ambiente de TIC, tarefas poderão ser adicionadas e/ou removidas do Catálogo de Serviços durante a vigência do contrato mediante anuência da CONTRATADA. As novas tarefas, depois de incluídas no Catálogo de Serviços, farão parte do contrato automaticamente.
17.4.5.1. O BNDES enviará e-mail para o preposto do Contrato com o novo Catálogo de Serviços.
17.4.5.2. Após a inclusão de uma nova tarefa, esta passará por um período de amadurecimento, durante o qual a CONTRATADA elaborará seus respectivos procedimentos e ambientar-se-á com a sua adequada execução. Durante o período de amadurecimento, o não cumprimento dos níveis de serviço não ensejará ajustes de pagamento.
17.4.5.3. O período de amadurecimento será definido pelo BNDES no momento da inclusão de novas tarefas e terá duração de 15 (quinze) a 60 (sessenta) dias corridos de acordo com o grau de complexidade e de importância da tarefa. Opcionalmente, o BNDES poderá definir um período de amadurecimento de até, no máximo, a 3º (terceira) execução dessa nova tarefa incluída no Catálogo de Serviços.
17.4.5.4. O Nível de Serviço definido para a nova tarefa deverá ser compatível com o grau de complexidade e de importância dela, devendo também ser compatível com as tarefas e níveis de serviço similares já existentes.
17.4.5.5. A CONTRATADA também poderá propor a inclusão e/ou exclusão de tarefas do Catálogo de Serviços, visando melhoria e adequação dos serviços prestados. O BNDES analisará as propostas feitas pela CONTRATADA e, caso as julgue pertinentes, aprovará as alterações.
17.4.5.6. Somente após a comunicação do BNDES à CONTRATADA as novas tarefas poderão ser incluídas ou excluídas do Catálogo de Serviços.
17.5. A Tabela abaixo lista as falhas de qualidade que podem ser atribuídas pelo BNDES aos serviços prestados pela(s) CONTRATADA(s).

Lista de Falhas de Qualidade na Prestação dos Serviços e respectivas perda de pontos

Identificador da falha	Nome da falha	Descrição / Detalhamento / Exemplos / Itens referentes	Identificador e perda de pontos
F1	Falha ao indisponibilizar parcialmente ou totalmente equipamento ou serviço por ação ou inação.	Falha ao indisponibilizar parcialmente ou total de serviço por ação ou inação.	PP2 0,5 por falha
F2	Falha no processo de classificação e/ou encaminhamento dos	Falha ao classificar os incidentes de segurança observados no SIEM ou em outras ferramentas, falha ao seguir o playbook definido pelo BNDES	PP3 0,2 por falha

	incidentes de SI como falso positivo ou falso negativo	etc.	
F3	Fornecer informação incorreta ou incompleta	Ao responder consulta do BNDES, fornecer informação incompleta ou incorreta, não enriquecer ou enriquecer parcialmente os incidentes de segurança etc.	PP3 0,2 por falha
F4	Comunicado incorreto/falso positivo de vulnerabilidade e/ou ameaça descoberta e/ou falta de comunicação de vulnerabilidade e/ou ameaça conhecida	Em caso de comunicado incorreto/falso positivo de vulnerabilidade descoberta e/ou falta de comunicação de vulnerabilidade conhecida, a CONTRATADA sofrerá ajuste de qualidade. O mesmo se aplica à comunicação de ameaças e outras informações da atividade de Threat Intelligence e Digital Risk Protection.	PP2 0,5 por falha
F5	Falha na manutenção de base de dados	Não manter base de dados com dados atualizados. Exemplos: base de ativos de TIC, base de vulnerabilidades, base de endereços IPs comprometidos, feeds etc.	PP4 0,5 por falha
F6	Falha em um ou mais canais de comunicação com a CONTRATADA	Impossibilidade do BNDES entrar em contato com a CONTRATADA devido a falha de um ou mais canais de comunicação disponibilizados pela CONTRATADA.	PP3 0,2 por falha
F7	Falha no comparecimento de um profissional para atendimento presencial	Falha no comparecimento de um profissional em atendimento a crise de SI conforme demanda do BNDES	PP8 1 por dia
F8	Falha em apoiar a equipe do BNDES na operação das soluções da CONTRATADA	Não orientar adequadamente, sanar dúvidas, a equipe do BNDES no uso/obtenção de informações das ferramentas utilizadas pela CONTRATADA para prestação dos serviços	PP3 0,2 por falha
F9	Falha na composição da Equipe da CONTRATADA.	Falha na substituição de um profissional quando solicitado pelo BNDES em acordo com as regras contratuais, renovação de certificação, qualificação, ausência de profissionais com as qualificações requeridas devido a férias, doença etc.	PP8 1 por dia
F10	Envio do boletim/checklist de segurança com informações incorretas e/ou confusas.	Falha em caso do boletim/checklist ser enviado dentro do prazo mas com informações incorretas, desatualizadas, confusas, não formatadas, etc	PP3 0,2 por falha
F11	Falha de comunicação entre a CONTRATADA e sua equipe	Deixar de apresentar evidência de ciência da equipe sobre a PCSI do BNDES, cláusulas contratuais e demais procedimentos do BNDES	PP6 0,1 por dia
F12	Falha ao acompanhar ou fiscalizar os serviços pelo preposto técnico e/ou administrativo	No caso de o preposto não comparecer à reunião demandada pelo Gestor, não entregar plano de ação para correção de falhas, não manter os dados de contato da CONTRATADA atualizados ou outras demandas feitas a ele.	PP3 0,2 por falha
F13	Falha na emissão do “Relatório Mensal de Acompanhamento do Contrato”.	Falha na emissão do “Relatório Mensal de Acompanhamento do Contrato” conforme previsão contratual. Exemplo: fora do prazo, sem itens obrigatórios, sem assinatura etc.	PP7 0,5 por dia
F14	Falha em ajuste do “Relatório Mensal de Acompanhamento do Contrato”.	Continuidade de falha em ajuste do “Relatório Mensal de Acompanhamento do Contrato” para cada item que foi solicitado ajuste (correção ou complementação de informações ou algo afim) pelo BNDES.	PP7 0,5 por dia
F15	Falha na operação da infraestrutura de SI do BNDES	Falha na operação e administração dos sistemas conforme padrão definido pelo BNDES.	PP3 0,2 por falha
F16	Falha na manutenção de dados históricos	Falha na manutenção dos dados dos últimos 12 meses de forma online na solução da CONTRATADA	PP6 0,1 por dia
F17	Falha em procedimentos de segurança de acesso lógico e/ou físico, manipulação e armazenamento de dados do BNDES, disaster recovery, cumprimento de normativo, auditorias requeridas etc.	Falha em procedimento de segurança no controle de acesso a solução da CONTRATADA, segurança do CSOC, guarda e transmissão dos dados do BNDES, normativos etc.	PP1 1 por falha

F18	Falha de qualidade em geral	Demais falhas na prestação do serviço não especificadas anteriormente	PP3 0,2 por falha
F19	Falha na execução do processo de forense	Durante o processo de forense não empregar os métodos e ferramentas adequadas segundo a ABNT e GSI	PP1 1 por falha
F20	Falha no processo de transição dos serviços com empresa sucessora.	Durante os 60 (sessenta) dias corridos anteriores ao encerramento do Contrato, a CONTRATADA poderá participar, a critério do BNDES, do processo de transição dos serviços em conjunto com a sucessora e o BNDES. A CONTRATADA deverá disponibilizar todas as informações pertinentes aos serviços prestados. Cada omissão de informação, informação não transmitida ou transmitida de maneira incorreta, apontada pelo BNDES, será considerada uma falha.	PP6 0,1 por dia
F21	Falha no contato com o CSOC e/ou lista de acionamento/escalation list	Falta de resposta, em até 5 minutos, a mensagem enviada para os contatos informados pela CONTRATADA ou não atendimento a chamadas de voz e vídeo.	PP1 1 por falha
F22	Falha de licenciamento da solução da CONTRATADA	Utilização de ferramentas incorretamente licenciadas, com capacidade reduzida etc.	PP6 0,1 por dia
F23	Falha ao concluir tarefa de forma tempestiva.	Erro ou incapacidade para concluir tarefa à qual há necessidade pelo BNDES da conclusão imediata. Quando o BNDES solicitar uma tarefa, o SLA for descumprido e o BNDES considerar que a conclusão da tarefa não poderá mais ser postergada, o BNDES poderá solicitar a interrupção da execução pela CONTRATADA, aplicar o descumprimento de nível de serviço, realizar a tarefa por conta própria com sua equipe interna e adicionalmente aplicar esta falha, tendo em vista que a CONTRATADA não conseguiu realizar a tarefa e o BNDES não pode mais esperar. Esta falha também pode ser aplicada caso o BNDES seja obrigado a assumir uma tarefa ou um incidente por qualquer outra razão.	PP2 0,5 por falha

17.6. Legenda das colunas:
17.6.1. A coluna “Identificador da falha” define uma identificação única alfanumérica para cada um dos tipos de falhas.
17.6.2. A coluna “Nome da falha” é o nome definido para a falha neste Catálogo de Serviços.
17.6.3. A coluna “Descrição / Detalhamento / Exemplos / Itens referentes” contém informações mínimas necessárias para entendimento de cada falha que deve ser evitada na execução do contrato.
17.6.4. A coluna “Identificador e perda de pontos” define estabelece uma identificação única alfanumérica para cada um dos tipos de perdas de pontos e a perda de pontos associada a cada identificador.
17.6.4.1. A tabela “Identificador x Perdas” estabelece os relacionamentos entre os “Identificadores de perda de pontos” e as “Perdas de pontos” conforme detalhado a seguir:

Identificador x Perdas	
Identificador de perda de pontos	**Perda de pontos**
PP1	1,0 por falha
PP2	0,5 por falha
PP3	0,2 por falha
PP4	0,5 por mês
PP5	0,2 por mês
PP6	0,1 por dia
PP7	0,5 por dia
PP8	1 por dia

17.6.4.2. A coluna “Identificador de perda de pontos” estabelece uma identificação única alfanumérica para cada um dos tipos de perdas de pontos (conforme explicado anteriormente).
17.6.4.3. A coluna “Perda de pontos” informa a quantidade de pontos que será perdida de acordo com o tempo que ultrapassar o limite estabelecido ou de acordo com o tipo de falha.
17.6.4.4. Para as falhas que ocasionem a perda de pontos por tempo transcorrido, a perda dar-se-á mesmo em caso de uma fração do tempo transcorrido. Por exemplo: em caso de perda de 0,1 ponto por dia, ocorrerá a perda de 0,1 ponto caso a falha seja solucionada em até um dia após o tempo limite (isto é, pela fração do dia). Ainda no exemplo anterior, caso a falha seja solucionada em mais de 1 dia a até 2 dias após o tempo limite, ocorrerá a perda de 0,2 ponto.
17.6.4.5. Caso uma mesma falha continue sem resolução nos meses seguintes, haverá nova contabilização de perda de pontos em função da continuidade do problema em cada mês. Deste modo, é possível que uma mesma falha provoque, por exemplo, a perda de 1,5 (um vírgula cinco) pontos em um mês e mais 1,5 (um vírgula cinco) pontos no mês seguinte, caso o descumprimento persista.
17.6.4.6. Caso algum tipo de falha ocorra reiteradamente por 3 (três) meses consecutivos, a critério do BNDES, poderá ser duplicado o valor da perda de pontos para apenas este tipo de falha a partir desse 3º (terceiro) mês consecutivo (inclusive).
17.6.4.7. “Falha de qualidade em geral”, identificador F18 da “Lista de falhas e níveis de serviço associados”, poderá ocorrer, inclusive, em função das seguintes situações:
17.6.4.7.1. Execução de atividade sem respaldo técnico adequado ou fora dos requisitos técnicos especificados ou desalinhada com as diretrizes, normas, padrões, rotinas e procedimentos definidos pelo BNDES, fabricantes, entidades normativas e afins;
17.6.4.7.2. Entregas, em geral, incompletas, inconclusivas, sem objetividade e clareza, ou com inconsistências técnicas ou distorções de propósito ou conteúdo;
17.6.4.7.3. Planejamento superficial, incompleto, equivocado ou que venham a ignorar as prioridades e interdependências entre processos e atividades;
17.6.4.7.4. Não atendimento às solicitações da BNDES ou inobservância do atendimento na janela de manutenção adequada;
17.6.4.7.5. Ausência da geração, armazenamento e disponibilização de evidências da realização das tarefas;
17.6.4.7.6. Inconsistência ou erro no registro ou disponibilização de informações para gestão do contrato ou dos serviços;
17.6.4.7.7. Erro técnico em geral, por exemplo, ao configurar ou instalar ativos de TIC e equipamentos em geral;
17.6.4.7.8. Ausência de conhecimento especializado nas interações necessárias à execução do serviço que induzam ao BNDES ou à terceiros (parceiros, fornecedores e/ou fabricantes) a cometer erros;
17.6.4.7.9. Falha na atualização de manuais e procedimentos operacionais padrões acordados com o BNDES;
17.6.4.7.10. Remoção de trilhas de auditoria e logs em geral sem autorização do BNDES; e
17.6.4.7.11. Negligência, imprudência ou imperícia de profissionais da CONTRATADA.

18. NÍVEIS DE SERVIÇO – ITENS I e II

18.1. Condições Gerais
18.1.1. Para quaisquer indicadores de nível de serviço influenciados negativamente por eventos comprovadamente causados pelo BNDES não serão considerados os efeitos de tais eventos no cômputo do indicador de nível de serviço.
18.1.2. A contagem do prazo para o atendimento poderá ser interrompida ou estendida com a anuência do BNDES, desde que solicitada de forma justificada pela CONTRATADA antes do seu descumprimento ou identificado outro impeditivo pela equipe do BNDES.
18.1.2.1. O Gestor do Contrato também poderá suspender a contagem dos prazos unilateralmente, nos casos em que entender que o serviço não se encontra degradado ou prejudicando as atividades do BNDES.
18.1.2.2. Ao longo da vigência do contrato, o BNDES poderá definir regras para suspensão automática da contagem de tempo ou da falha para facilitar a gestão do contrato.
18.1.3. O momento de fim da medição do nível de serviço de cada atendimento/atividade do Catálogo solicitada à CONTRATADA será definido pela data e hora da solução e resposta da equipe da CONTRATADA pelo mesmo meio que foi registrado o atendimento ou outro definido pelo BNDES.
18.1.3.1. O BNDES analisará a corretude da resolução do atendimento para então aprovar ou recusar o fechamento do mesmo. O tempo gasto pelo BNDES para analisar o atendimento será considerado para efeito de cálculo do tempo de resolução caso a resolução seja recusada pelo BNDES.
18.1.4. Considerar-se-á como tempo de resolução, o período líquido compreendido entre o momento de início da falha/atendimento e a regularização da falha/ finalização do atendimento, descontado o tempo em que o mesmo ficou pendente de execução por outras equipes do BNDES.
18.1.4.1. Para ações da CONTRATADA/chamados que dependam de informações fornecidas por empresas e/ou entidades internacionais, será considerada, como início de contagem do nível de serviço, a data e hora da informação publicada no site da respectiva empresa e/ou entidade. Exemplo, no caso de uma

vulnerabilidade do tipo “zero-day”, a prioridade para definição do início da contagem do nível de serviço para comunicação ao BNDES será a data e hora da divulgação no sistema de alertas do fabricante da solução, sites de registro de vulnerabilidades (NIST, etc), outras fontes, nessa ordem de prioridade.
18.1.5. Os níveis de serviço em dias corridos consideram que o segundo dia em diante deverá ser computado a partir das primeiras 24 horas corridas da abertura do chamado/demanda, qualquer que seja o horário de sua abertura.
18.1.6. O momento de início da medição do nível de serviço de cada tarefa à CONTRATADA será definido pela data e hora da comunicação/solicitação enviada para a CONTRATADA e/ou agendamento de uma tarefa, por um dos meios definidos no item 16.1.2, ou detecção da falha/indisponibilidade pelo sistema de monitoramento do BNDES.
18.1.6.1. Para informações fornecidas por empresas e/ou entidades internacionais, será considerada a data e hora de início de contagem do nível de serviço publicada no site da respectiva empresa e/ou entidade. Exemplo, no caso de uma vulnerabilidade do tipo “zero-day”, a prioridade para definição do início da contagem do nível de serviço para comunicação ao BNDES será a data e hora da divulgação no sistema de alertas do fabricante da solução, sites de registro de vulnerabilidades (NIST, etc), outras fontes, nessa ordem de prioridade.
18.1.7. A CONTRATADA, após receber cada solicitação, necessitará enquadrá-la em uma ou mais tarefas definidas no Catálogo de Serviços, conforme item 17, caso a solicitação não tenha sido previamente enquadrada.
18.1.8. Após receber a solicitação de atendimento, a CONTRATADA deverá sempre abrir um ticket na plataforma definida de acordo com o item 16.1.2.3.
18.1.9. Caso ocorra algum enquadramento indevido pela CONTRATADA, o BNDES solicitará, quando observado, a alteração de modo que seja realizada a apuração correta do nível de serviço correspondente e tal modificação poderá acarretar ajuste de pagamento para a CONTRATADA.
18.1.10. Não há previsão de bônus ou pagamentos adicionais para os casos em que a CONTRATADA superar as metas previstas, ou caso seja necessária à alocação de maior número de profissionais para o alcance das metas.
18.2. Boletim/Checklist de Segurança
18.2.1. A CONTRATADA deverá enviar para a equipe do BNDES, via e-mail e em horário definido pelo BNDES, um boletim informativo com o resumo das ocorrências das últimas 12 (doze) horas, por exemplo, para cada serviço contratado pelo BNDES.
18.2.1.1. Exemplo 01: Supondo que o BNDES tenha agendado um boletim para as 9h e outro para as 21h e tenham sido divulgadas 10 vulnerabilidades no período das 22h às 6h, o boletim de 9h deve trazer essa lista com os detalhes pertinentes, sem prejuízo aos alertas individuais/tickets gerados nas ferramentas de ITSM.
18.2.1.2. Exemplo 02: Supondo que o BNDES tenha agendado um boletim para as 9h e outro para as 21h e tenham sido encontrados achados pelo serviço de DRP no período das 22h às 6h, o boletim de 9h deve trazer essa lista de achados com detalhes pertinentes, sem prejuízo aos alertas individuais/tickets gerados nas ferramentas de ITSM.
18.2.1.3. O objetivo o boletim é ser um resumo executivo para acompanhamento das ocorrências e ações de segurança desempenhadas pela CONTRATADA.
18.2.1.4. O conteúdo dos boletins será definido e ajustado ao longo da vigência do contrato de acordo com a relevância das informações demandadas pelos executivos do BNDES.
18.3. Disponibilidade da solução de software e hardware da CONTRATADA.
18.3.1. A disponibilidade dos serviços será medida pelo software de monitoramento do BNDES a cada 1 minuto.
18.3.2. O serviço será considerado como disponível se for possível:
18.3.2.1. Acessar a SOLUÇÃO DA CONTRATADA, a partir da rede do BNDES, esteja a solução remota ou local.
18.3.2.2. Fazer logon no produto.
18.3.2.3. Realizar buscas e visualizar informações com, no máximo, 5 (cinco) minutos do fato ocorrido em relação à data e hora correntes.
18.4. Desempenho da solução de software e hardware da CONTRATADA.
18.4.1. A infraestrutura instalada pela CONTRATADA no ambiente do BNDES deverá dispor de desempenho suficiente, sob pena de troca/complementação imediata pela CONTRATADA, para que a solução opere com tempos de resposta/desempenho adequados, durante toda a vigência do contrato. Para aferição de desempenho, além dos níveis de serviços estabelecidos para os serviços/atividades contratados, serão consideradas as medições abaixo:
18.4.1.1. Realizar buscas e visualizar informações com, no máximo, 1 (um) minuto de atraso em relação à data e hora corrente (tempo de processamento dos eventos).
18.4.1.2. A busca dos eventos das últimas 24 horas, com dados enriquecidos, respondida em até 3 (três) minutos (capacidade de I/O).
18.4.1.3. A execução da varredura de vulnerabilidades em, no máximo, 1 hora para 200 ativos (capacidade de processamento).
18.4.1.4. Utilização dos circuitos de comunicação com a CONTRATADA inferior a 90% medida a cada 1 (um)

minuto (capacidade de tráfego).
18.4.1.5. A não ocorrência de alarmes de desempenho configurados de acordo com os padrões recomendados pelo fabricante da solução.
18.5. Atividades sob demanda
18.5.1. São as tarefas/atividades que requerem um chamado ou comunicação do BNDES com a CONTRATADA para serem iniciados. O BNDES poderá demandas várias tarefas /atividades em paralelo, cada uma com sua própria aferição de nível de serviço.
18.5.2. As atividades sob demanda terão seu nível de serviço medido a partir da data e hora agendada para o início da atividade pelo BNDES, se definida, ou a partir da data e hora da solicitação à CONTRATADA e seu limite de nível de serviço estabelecido para a entrega do resultado da atividade, devidamente aprovado pelo BNDES.
18.5.2.1. Caso o resultado não seja aprovado pelo BNDES, a contagem de tempo para fins de nível de serviço continuará correndo.
18.5.2.2. A CONTRATADA deverá adotar, previamente à data agendada para execução da atividade, todas as ações preparatórias para execução da atividade agendada a fim de cumprir os níveis de serviço.
18.5.2.2.1. Por padrão, para as atividades agendadas, a CONTRATADA terá 5 (cinco) dias para apresentar ao BNDES o planejamento da tarefa demandada, que fará a avaliação em até 5 (cinco) dias, quando poderá solicitar ajustes com registro ou não de falha de qualidade, se pertinente. Esses prazos poderão ser ajustados na demanda do BNDES por uma atividade.
18.5.2.3. Exemplo: caso seja solicitada uma atividade agendada com uma nível de serviço de 4 dia 05/10 para ser executada no dia 20/10 às 9h, a CONTRATADA, por padrão, terá até 10/10 para apresentar o planejamento, o BNDES terá até 15/10 para solicitar ajustes e a CONTRATADA terá o prazo para executar e concluir a demanda/entrega do relatório do dia 20/10 às 9h até 24/10 às 9h. Durante o planejamento, a CONTRATADA deverá combinar com o BNDES o escopo da atividade, verificar possíveis problemas etc.
18.5.2.4. O BNDES não possui um histórico do volume previsto para as atividades sob demanda.
18.6. Atividades continuadas
18.6.1. São as atividades continuadas que não requerem um comando do BNDES. Em geral, compreendem as atividades que envolvem monitoramento, tratamento de incidentes, proatividade e disponibilidade de serviços para o BNDES. Portanto, a CONTRATADA deve estar atuantes de acordo com o regime especificado no item 16.
18.6.2. A medição do nível de serviço é contínua e/ou se inicia automaticamente a cada ocorrência de um evento dentro do escopo do serviço que a CONTRATADA tenha que tratar automaticamente.
18.6.3. Mesmo nesses casos, se o resultado não for aprovado pelo BNDES, a contagem de tempo para fins de nível de serviço continuará correndo.
18.6.4. Exemplo: caso ocorra um incidente de segurança e a CONTRATADA aplique a resolução dentro do nível de serviço, mas de forma incorreta, o prazo resolução continuará correndo até que a CONTRATADA aplique a medida correta.
18.6.5. O BNDES não possui um histórico do volume previsto para as atividades continuada, como incidentes de segurança, dado que uma das atividades do futuro serviço será construir os casos de uso do SIEM para identificar incidentes de segurança. A CONTRATADA deverá utilizar sua experiência para estimar tais valores de acordo com as capacidades do SIEM do BNDES e volume de logs gerados diariamente.

19. RELATÓRIO DE ACOMPANHAMENTO MENSAL – ITENS I e II

19.1.1. O relatório deverá ser apresentado no formado PDF/A-3 e assinado digitalmente (via gov.br ou ICP Brasil/e-CPF) por toda a equipe habilitada junto ao BNDES para as certificações previstas no item 4.
19.1.1.1. Os arquivos fonte do relatório, documentos docx e xlsx também deverão ser entregues para serem utilizados pelo BNDES para facilitar a verificação do relatório.
19.1.2. Esse relatório deverá conter, no mínimo:
19.1.2.1. Parte Geral (ITENS I e II)
19.1.2.1.1. Dados do Contrato (número, vigência, gestor etc.), período de referência, descrição do objeto e principais atividades do período;
19.1.2.1.2. Lista dos técnicos envolvidos na prestação do serviço com nome e CPF. Os especialistas nas qualificações exigidas no item 4 e demais profissionais que tenham acesso a informações do ambiente do BNDES.
19.1.2.1.3. Lista das certificações com respectiva expiração, se houver, conforme requisitos do item 4.
19.1.2.1.4. Lista para acionamento 24x7 (escalation list) prevista para o próximo mês.
19.1.2.1.5. Diagrama e dados da solução da CONTRATADA.
19.1.2.1.6. Mapa de versões e atualizações disponíveis para a SOLUÇÃO DA CONTRATADA instalada no ambiente do BNDES.
19.1.2.1.7. Histórico de pagamentos e descontos.
19.1.2.1.8. Histórico do total de atendimentos por serviço.
19.1.2.1.9. Prévia do cálculo da Nota de Avaliação Mensal – NAM.
19.1.2.1.10. Lista de todos os serviços do catálogo prestados no período do relatório e o nível de serviço atingido para cada um com a respectiva perda de postos, se houver.

19.1.2.2. CSIRT (ITEM I)
19.1.2.2.1. Os 10 principais incidentes/alertas de segurança da informação, classificados por severidade, em seguida por quantidade, juntamente com proposta para mitigação do risco, caso não exista mitigação implementada. Para determinação dos principais incidentes, deverá ser levada em conta a criticidade (alta, média e baixa) seguido da quantidade, onde, o de maior criticidade, seguido da maior quantidade, deverá ser tratado com maior prioridade;
19.1.2.2.2. As 10 regras do SIEM com mais matches;
19.1.2.2.3. As 10 principais origens de eventos de segurança, endereços de destino das ameaças, atacantes, ataques etc.
19.1.2.2.4. Histórico de ocorrência de falsos positivos;
19.1.2.2.5. Lista de regras analíticas de identificação de ameaças sugeridas para serem adicionadas ou removidas do ambiente de SIEM, com breve justificativa;
19.1.2.2.6. Lista de playbooks de tratamento de incidentes criados e/ou ajustados, com breve justificativa;
19.1.2.2.7. Lista de ativos que tiveram o envio de logs interrompido ou degradado, com o respectivo baseline e breve justificativa;
19.1.2.2.8. Proposta de no mínimo um novo fluxo para automação do tratamento, com descrição e resumo da sua finalidade;
19.1.2.2.9. Sugestões de remoção de atividades automatizadas obsoletas;
19.1.2.2.10. Volume de incidentes identificados no SIEM e volume de incidentes tratados automaticamente pelo serviço de SOAR.
19.1.2.2.11. Lista de todos os eventos de segurança reportados no SIEM com seus respectivos tempos de tratamento pela CONTRATADA e tickets.
19.1.2.2.12. Lista de TTPs mais explorados de acordo com o framework MITRE ATT&CK.
19.1.2.2.13. Lista de casos de uso implementado no SIEM, automatizados no SOAR e pendentes de implementação e/ou automação.
19.1.2.2.14. Disponibilidade da solução de SOAR, feeds e demais componentes da CONTRATADA.
19.1.2.3. GVUL (ITEM I)
19.1.2.3.1. Lista de vulnerabilidades “zero day” informadas.
19.1.2.3.2. Total de vulnerabilidades reportadas classificadas por severidade, em seguida por quantidade de ativos.
19.1.2.3.3. Vulnerabilidades encontradas com status de resolução e ticket do ITSM.
19.1.2.3.4. Quantidade de ativos em conformidade e em não conformidade com a base de vulnerabilidades.
19.1.2.3.5. Lista de ajustes realizadas no BATIC.
19.1.2.3.6. Lista de baselines de segurança.
19.1.2.3.7. Quantidade e resultado das ações de levantamento de vulnerabilidades sob demanda realizadas.
19.1.2.3.8. Disponibilidade da solução de GVUL, versão das bases de vulnerabilidades e demais componentes da CONTRATADA.
19.1.2.4. IRC (ITEM I)
19.1.2.4.1. Histórico de acionamentos.
19.1.2.4.2. Laudos produzidos.
19.1.2.5. THREAT INTELLIGENCE (ITEM II)
19.1.2.5.1. Lista de fontes em uso e data da última atualização;
19.1.2.5.2. Histórico de achados.
19.1.2.5.3. Lista de vulnerabilidades “zero day” informadas.
19.1.2.5.4. Comunicados enviados por criticidade.
19.1.2.5.5. Proposta de melhoria pela CONTRATADA.
19.1.2.6. DRP (ITEM II)
19.1.2.6.1. Lista de ativos monitorados e capacidade ainda disponível;
19.1.2.6.2. Lista de fontes em uso e data da última atualização;
19.1.2.6.3. Histórico de achados por ativo monitorado.
19.1.2.6.4. Quantidade e lista de achados por ativo monitorado.
19.1.2.6.5. Comunicados enviados por categoria (informação, aviso, exceção).
19.1.2.6.6. Proposta de melhoria pela CONTRATADA.

20. NOTA DE AVALIAÇÃO MENSAL – ITENS I e II

20.1. O cálculo da Nota de Avaliação Mensal (NAM) será realizado conforme fórmula abaixo:
20.1.1. Nota de Avaliação Mensal (NAM) = 10,0 – (∑ pontos perdidos pela CONTRATADA na prestação dos serviços ao BNDES no período de referência).
20.1.2. Os critérios de perda de pontos encontram-se detalhados Catálogo de Serviços, conforme item 17.
20.1.3. A Nota de Avaliação Mensal (NAM) será convertida em um Fator de Correção Mensal utilizado para efetuar o ajuste de pagamento referente ao período de apuração conforme tabela a seguir:

NAM	Ajustes de Pagamento	Fator de Correção Mensal (FCM)
NAM ≥ 9,0	Sem ajustes de pagamento;	1
2,0 ≤ NAM < 9,0	Ajuste de pagamento de (1 – FCM) x 100% no pagamento do mês de referência;	(0,2 x NAM + 5,2) / 7 (arredondar para 4 casas decimais)
NAM < 2,0	Ajuste de pagamento de 30% no pagamento do mês de referência;	0,7

20.1.3.1. Caso a NAM mensurada seja um valor entre 2 (dois) e algo inferior a 9 (nove) haverá um ajuste de pagamento correspondente, calculado conforme fórmula indicada na tabela anterior. Assim, por exemplo, sendo a NAM igual a 5,5 (cinco e meio) teremos um ajuste de pagamento de 10% (dez por cento) e FCM igual a 0,9 (nove décimos).
20.1.4. O somatório dos valores de todos os ajustes do está limitado a 30% do valor total mensal do respectivo ITEM.
20.1.4.1. O somatório dos valores de todos os ajustes está limitado a 30% do valor total mensal do respectivo ITEM. Caso este somatório seja superior a 30% (trinta por cento), poderá ser aplicada penalidade.
20.1.4.2. Adicionalmente, a CONTRATADA poderá estar sujeita, além dos ajustes de pagamentos, à multa prevista no item 23, de acordo com a avaliação do Gestor do Contrato e resultado de Processo Administrativo Punitivo - PAP, considerando os seguintes fatores, individualmente ou em conjunto:
20.1.4.2.1. O prejuízo causado ao BNDES tenha superado a esfera potencial;
20.1.4.2.2. A CONTRATADA tenha apresentado um plano de ação, aprovado pelo Gestor do Contrato, para aumento da qualidade dos serviços prestados.
20.1.5. Caso o descumprimento de qualquer obrigação prevista perdure no mês subsequente, será:
20.1.5.1. Descontado da NAM o número de pontos perdidos no mês corrente para cálculo da NAM no mês corrente.
20.1.5.2. Nos meses subsequentes será descontado da NAM o número de pontos perdidos no respectivo mês, até o cumprimento da obrigação que ensejou a perda de pontos.

21. CONDIÇÕES DE PAGAMENTO – ITENS I e II

21.1. O pagamento apenas será realizado após a aprovação do "Relatório Mensal de Acompanhamento do Contrato", conforme item 19, para os ITENS I e II, quando o gestor do Contrato autorizará o faturamento do respectivo período pela CONTRATADA. A aprovação do relatório constitui condição indispensável para o pagamento do valor ajustado.
21.1.1. A CONTRATADA só deverá emitir qualquer documento de cobrança após aprovação do "Relatório Mensal de Acompanhamento do Contrato" pelo BNDES.
21.2. A CONTRATADA deverá apresentar mensalmente, entre os dias 1 e 10 de cada mês o relatório referente ao mês anterior.
21.3. O relatório deverá ser apresentado e discutido em reunião mensal, com presença do preposto técnico e do preposto administrativo, conforme definido no item 4.
21.3.1. O BNDES poderá realizar uma reunião de acompanhamento mensal do Contrato para que a CONTRATADA apresente o relatório, o que ocorrerá até 10 (dez) dias após o recebimento do relatório da CONTRATADA.
21.3.2. Na reunião, obrigatoriamente, deverão estar presentes os prepostos técnico e administrativo. Por demanda do BNDES, poderá ser necessária a presença de toda ou parte da equipe técnica signatária do relatório. Também por opção do BNDES, a participação poderá ser remota ou presencial.
21.3.3. A CONTRATADA deverá elaborar a ata de reunião, a qual deverá ser encaminhada por e-mail até 5 (cinco) dias da reunião para possíveis considerações do BNDES.
21.4. O BNDES verificará a conformidade das informações contidas no relatório mensal, por amostragem de dados, e solicitará os devidos ajustes nos casos de inconformidade. A CONTRATADA deverá realizar os ajustes em até 3 (três) dias após a solicitação do BNDES.
21.5. A apuração dos indicadores será realizada mensalmente a partir do "Relatório Mensal de Acompanhamento do Contrato", elaborado pela CONTRATADA, baseado em informações do Software de Gerenciamento de Serviços de TIC (atualmente BMC Remedy IT Service Management), do Software de Gerenciamento de Incidentes de SI (atualmente RTIR) e das ferramentas empregadas no escopo deste contrato, conforme definido no item 16.1.2.3 pelo BNDES.
21.5.1. Para os indicadores cujo acompanhamento não se mostrar possível por meio dos softwares mencionados anteriormente, deverá ser utilizada uma planilha eletrônica para controle manual, elaborada pela CONTRATADA e validada pelo BNDES.
21.6. A apuração dos níveis de serviço será realizada do primeiro ao último dia do respectivo mês do faturamento e deverá contemplar todos os serviços do respectivo ITEM.
21.7. Conforme definido no item 20, a CONTRATADA terá uma Nota de Avaliação Mensal (NAM)

calculada em função do seu desempenho em relação aos diversos níveis de serviço estabelecidos no Catálogo de Serviços, conforme item 17.
21.8. O valor do pagamento dos serviços prestados estará sujeito a ajustes de pagamento na respectiva fatura, quando não forem atingidos os Níveis de Serviço estabelecidos.
21.9. O "valor de pagamento mensal" a ser pago para a CONTRATADA obedecerá a seguinte fórmula:
21.9.1. [Valor Mensal] = {[Valor total mensal do ITEM I ou II x Fator de Correção Mensal]}, onde:
21.9.2. [Valor total mensal do ITEM I ou II] – Representa o custo mensal total previsto para o respectivo ITEM sem o valor da implantação, paga uma única vez após emissão do TRD. Adicionalmente, no caso do ITEM I que possui atividades sob demandas, será considerado o valor total do ITEM sem considerar o valor dessas atividades nos meses em que não houver consumo delas.
21.9.3. [Fator de Correção Mensal] – Representa o fator de correção, calculado mensalmente, para definir o ajuste de pagamento sobre o valor do pagamento mensal na fatura referente à prestação dos serviços em função do desempenho da CONTRATADA. Esse fator é obtido a partir da Nota de Avaliação Mensal (NAM) calculada em virtude de falhas e de descumprimentos pela CONTRATADA dos níveis de serviço exigidos no contrato, conforme itens 17 e 18.
21.10. Os ajustes de pagamentos serão efetuados na fatura com vencimento no mês imediatamente subsequente ao mês de ocorrência dos eventos de descumprimento ou posteriormente, caso, a critério do BNDES, não seja possível aplicar o desconto no mês imediatamente subsequente ao mês de ocorrência do descumprimento, à exceção da fatura referente ao último mês de vigência do contrato de prestação dos serviços, quando o desconto deverá, obrigatoriamente, ser aplicado na fatura do mês de ocorrência da violação.

22. PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO – ITENS I e II

22.1. Durante os 60 (sessenta) dias corridos anteriores ao encerramento do Contrato, seja por fim da vigência ou rescisão antecipada, a CONTRATADA do respectivo item deverá participar, a critério do BNDES, do projeto de transição dos serviços contratados em conjunto com a empresa sucessora e o BNDES, em especial na documentação das regras e alertas desenvolvidos para o BNDES, sem prejuízo à prestação do serviço e sem custo adicional para o BNDES.
22.2. A CONTRATADA deverá disponibilizar, em formatos padronizados de mercado como XML, JSON, CSV etc, caso sejam solicitadas pelo BNDES, todas as informações pertinentes aos serviços prestados, os documentos e artefatos da base de conhecimento com dados do BNDES, construída durante o período de prestação do serviço, conforme exigido nestas Especificações Técnicas.
22.3. Caso a CONTRATADA faça uso de softwares livres de licenciamento (licenças GPL, Apache etc) durante a prestação do serviço, todas as parametrizações dos respectivos softwares deverão ser compartilhadas com o BNDES, para que esse continue utilizando os softwares livres de licenciamento. Adicionalmente, rotinas de código, conhecidas como scripts ou equivalentes, também deverão ser compartilhados com o BNDES que poderá utilizá-los e modificá-los livremente.
22.4. Fica a CONTRATADA obrigada a assegurar o retorno integral dos dados e informações sob sua custódia ao BNDES, no caso de término do contrato, além da exclusão segura dos mesmos.

23. PENALIDADES – ITENS I e II

23.1. Em caso de descumprimento das exigências expressamente formuladas pelo BNDES ou inobservância de quaisquer das demais obrigações contratuais e/ou legais, sem motivo justificado, a CONTRATADA ficará sujeita às seguintes penalidades, dentre outras previstas no Contrato:
23.1.1. Advertência;
23.1.2. Multa de até 20% (vinte por cento) sobre o valor global do Contrato, a critério da autoridade competente do BNDES, caso o descumprimento dos prazos de nível de serviço estabelecidos enseje ajustes de pagamento superiores aos limites para descontos previstos;
23.1.3. Multa de até 1% (um por cento) por dia de atraso na implantação dos serviços, a critério da autoridade competente do BNDES. A referida multa terá como base o valor global referente ao ITEM descumprido;
23.1.4. Multa de até 20% (vinte por cento) sobre o valor global do Contrato, a critério da autoridade competente do BNDES, em razão de qualquer descumprimento das demais obrigações contratuais, não previstas nos itens acima.
23.1.5. Suspensão temporária de participação em licitação e impedimento de contratar com o BNDES, por prazo não superior a 2 (dois) anos, apurado em razão da natureza e gravidade da infração cometida.
23.2. O total das multas aplicadas não poderá exceder o montante de 30% (trinta por cento) do valor global do Contrato.
23.3. O valor da multa poderá ser descontado da nota fiscal ou de crédito existente no BNDES em relação à CONTRATADA. Caso o valor da multa seja superior ao crédito existente, a diferença será cobrada na forma da lei.
23.4. Em qualquer hipótese de aplicação de penalidades, serão assegurados à CONTRATADA o contraditório e a ampla defesa.

24. VIGÊNCIA CONTRATUAL – ITENS I e II

24.1. O prazo de vigência de cada CONTRATO deverá ser de:

24.1.1. até 6 (seis) meses, contados da assinatura do contrato, para execução da implantação, incluindo todas as fases até a emissão do Termo de Recebimento Definitivo - TRD; e

24.1.2. 60 (sessenta) meses a contar da emissão do Termo de Recebimento Definitivo - TRD, com opção de rescisão por parte do BNDES a partir do 30º (trigésimo) mês de vigência, desde que comunicada com antecedência de 180 (cento e oitenta) dias.

24.1.2.1. A opção de rescisão antecipada deverá ser formalizada em autorização escrita e fundamentada pelo BNDES, mediante aviso prévio por escrito, com antecedência mínima de 180 (cento e oitenta) dias ou de prazo menor a ser negociado pelas partes à época da rescisão. A CONTRATADA fará jus ao pagamento do serviço até a data definida para interrupção da prestação do mesmo.

25. GARANTIA CONTRATUAL – ITENS I e II

25.1. A CONTRATADA deverá prestar garantia contratual no montante de 5% (cinco por cento) do valor total da contratação, no prazo de até 15 (quinze) dias após convocação pelo gestor do contrato, nas modalidades que vier a escolher, dentre as previstas no parágrafo primeiro do artigo 70, da Lei nº 13.303/2016.

26. EQUILÍBRIO ECONÔMICO-FINANCEIRO - ITENS I e II

26.1. O equilíbrio econômico-financeiro do Contrato será mantido, conforme o caso, pela revisão ou pelo reajuste, observados os limites e condições constantes da minuta de Contrato e as a seguir listadas.

26.2. O Contrato poderá ser reajustado anualmente como forma de compensação dos efeitos das variações dos custos, decorridos 12 (doze) meses a contar da data da apresentação da proposta, de acordo com o art. 3º da Lei nº 10.192, de 14 de fevereiro de 2001, ou a contar do fato gerador anterior.

26.3. O reajuste do preço estará limitado ao Índice de Custo de Tecnologia da Informação - ICTI, divulgado pelo Instituto de Pesquisa Econômica Aplicada – IPEA, ou outro índice que vier a substituí-lo, na forma prevista no Contrato.

26.4. O reajuste observará a legislação vigente e a disciplina contratual adotada pelos instrumentos padrão da Área de Administração do BNDES.

26.5. Será incumbência da CONTRATADA a iniciativa e o encargo do cálculo de cada reajuste anual, a ser submetido à aprovação do BNDES, juntando-se os respectivos documentos comprobatórios exigidos pela legislação.

27. OBRIGAÇÕES ADICIONAIS DA CONTRATADA – ITENS I e II

27.1. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação.

27.2. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

27.3. Fornecer todas as informações necessárias para a utilização do serviço CONTRATADO pelo BNDES;

27.4. Manter, durante toda a vigência do Contrato, o escalation list, para o serviço de suporte, atualizado até o nível de direção da empresa;

27.5. Informar e manter atualizados o CPF e nome completo dos prepostos técnico e administrativo e do DPO da CONTRATADA perante o BNDES. Os prepostos deverão comparecer ao BNDES para reuniões presenciais sempre que requerido pelo Gestor do Contrato;

27.6. Assumir inteira responsabilidade técnica e administrativa em relação ao objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas na prestação dos serviços;

27.7. Manter sigilo relativamente ao objeto contratado, bem como sobre dados, documentos, especificações técnicas ou comerciais, não tornadas públicas pelo BNDES, de que venha a ter conhecimento em virtude da contratação, bem como a respeito da execução e resultados obtidos na prestação de serviços, inclusive após o término do prazo de vigência do CONTRATO, sendo vedada a divulgação dos referidos resultados a terceiros em geral, e em especial a quaisquer meios de comunicação públicos e/ou privados;

27.8. Adotar medidas de segurança adequadas, no âmbito das atividades sob seu controle, para a manutenção do sigilo referido no subitem anterior;

27.9. Não efetuar a compilação reversa, montagem reversa ou engenharia reversa de qualquer programa aplicativo do BNDES ou de terceiros a que venha ter acesso por força do serviço;

27.10. Devolver, impreterivelmente, ao término do CONTRATO, ou a qualquer tempo a pedido do BNDES, todos os documentos que o BNDES a tenha fornecido;

27.11. Indicar seus dados de endereço, telefone e endereço de correio eletrônico, mantendo-os atualizados perante o BNDES durante toda a vigência do Contrato;

27.12. Notificar o BNDES, por escrito, quaisquer fatos que possam pôr em risco a execução do presente

objeto;
27.13. Propriedade intelectual
27.13.1. A Contratada deverá documentar e repassar para os responsáveis técnicos do BNDES todo o conhecimento adquirido ou produzido na execução dos serviços.
27.13.2. Todos os softwares desenvolvidos, por exemplo, scripts para a automação de tarefas, durante a prestação dos serviços ao longo da vigência do contrato serão de propriedade do BNDES, sendo vedada a comercialização ou cessão a terceiros, sem sua expressa autorização, por escrito.
27.13.3. Todas as bases de dados, documentos, metodologias, procedimentos, programas, códigos fonte e correlatos que sejam gerados ou alterados durante a prestação dos serviços serão de propriedade exclusiva do BNDES.
27.14. Além das obrigações usualmente aplicadas à CONTRATADA, permitir ao Banco Central do Brasil acesso a termos firmados, documentos e informações atinentes aos serviços prestados, bem como às suas dependências, nos termos do § 1º do artigo 33 da Resolução CMN n° 4.557 de 23/02/2017 atualizada pela Resolução CMN n° 4.745 de 29/8/2019;
27.15. Apresentar, por ocasião da formalização do Contrato, o(s) Termo(s) de Confidencialidade, conforme as instruções abaixo:
27.15.1. Termo de Confidencialidade – Modelo A (Representante Legal), conforme minuta constante do Edital, assinado por seu(s) representante(s) legal(is) de cada vencedora do respectivo Item do Certame, e, no caso de Consórcio, pelo(s) representante(s) legal(is) de cada consorciada;
27.15.2. Termo de Confidencialidade – Modelo B (Profissionais), conforme modelo anexados ao Edital, assinado pelos profissionais;
27.16. Prestar todos os esclarecimentos que lhe forem solicitados pelo BNDES;
27.17. Aceitar, por parte do BNDES, em todos os aspectos, a fiscalização no cumprimento do objeto contratado;
27.18. Responder pelos danos comprovadamente causados ao BNDES ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução do objeto contratado. A fiscalização ou o acompanhamento do BNDES não excluirá ou reduzirá essa responsabilidade da CONTRATADA;
27.19. Assegurar durante a execução do objeto desta contratação, a utilização das melhores técnicas para garantir o respeito à privacidade e à proteção de dados pessoais eventualmente nela processados, em conformidade com a legislação, devendo:
27.20. Zelar pelas garantias, direitos e deveres, notadamente os previstos na Resolução nº 4.658, de 26 de abril de 2018, do Conselho Monetário Nacional (Política de Segurança Cibernética), na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e no restante da legislação vigente relativa ao tema;
27.21. Promover e cooperar com mecanismos de correção de falhas ocasionadas pelo sistema que possam gerar violação à LGPD, auxiliando, inclusive, na eventual prestação de informações aos órgãos de controle e às autoridades competentes como, por exemplo, a Agência Nacional de Proteção de Dados (ANPD);
27.22. Prover mecanismos para preservar o caráter confidencial de informações coletadas, zelando sempre pela proteção dos dados pessoais e do sigilo das informações quando protegidas por lei, nos termos da legislação aplicável;
27.23. Informar imediatamente ao BNDES, a partir do momento em que tomar ciência, sobre a ocorrência de falhas ou violações de sistema decorrentes de sua ação ou omissão, bem como de seus empregados, prepostos e prestadores de serviço e/ou qualquer pessoa natural ou jurídica envolvida na execução do objeto contratual, que possam acarretar violação à LGPD.
27.24. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de scripts e aplicações, os modelos de dados e as bases de dados ao BNDES sem ônus;
27.25. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização do BNDES.

28. VALOR ESTIMADO DA LICITAÇÃO

28.1. O valor global máximo estimado para cada ITEM é de até:
28.1.1. ITEM I - R$ 6.989.847,28 (seis milhões e novecentos e oitenta e nove mil e oitocentos e quarenta e sete reais e vinte e oito centavos).
28.1.2. ITEM II - R$ 1.835.303,06 (um milhão e oitocentos e trinta e cinco mil e trezentos e três reais e seis centavos).

Planilha de Composição de Custos e Formação de Preço					
ITEM I	**Valor por Unidade**	**Unidade**	**Meses**	**Valor Total**	**Observações**
A1 - Implantação	R$ -	Não se aplica	Não se aplica	R$ -	**Valor Total limitado ao**

					valor unitário de (A2+A3)*6
A2 - CSIRT - Computer Security Incident Response Team	R$ -	Mês	60	R$ -	
A3 - GVUL - Levantamento e Gestão de Vulnerabilidades	R$ -	Mês	60	R$ -	
A4 - IRC - Incident Response Consulting - Atendimento remoto	R$ -	Pacote de 40h	52	R$ -	**Atividade remunerada apenas quando demandada. Horas da equipe multidisciplinar.**
A5 - IRC - Incident Response Consulting - Atendimento presencial	R$ -	Pacote de 40h	52	R$ -	**Atividade remunerada apenas quando demandada. Horas da equipe multidisciplinar.**
Total ITEM I (A)				**R$ 6.989.847,28**	**(A1+A2+A3+A4+A5)**
ITEM II	**Valor por Unidade**	**Unidade**	**Meses**	**Valor Total**	**Observações**
B1 - Implantação	R$ -	Não se aplica	Não se aplica	R$ -	**Valor Total limitado ao valor unitário de (B2+B3)*6**
B2 - CTI - Cyber Threat Intelligence	R$ -	Mês	60	R$ -	
B3 - DRP - Digital Risk Protection	R$ -	Mês	60	R$ -	
Total ITEM II (B)				**R$ 1.835.303,06**	**(B1+B2+B3)**
Total Geral (A+B)				**R$ 8.825.150,34**	**(A+B)**

28.2. Os valores das fases de implantação (A1 e B1) estão limitados ao valor unitário de 6 (seis) meses dos respectivos serviços do ITEM, conforme as seguintes fórmulas: A1 = (unitário de A2 + unitário de A3) x 6 e B1 = (unitário de B2 + unitário de B3) x 6.

28.3. Os valores totais de cada ITEM são os máximos aceitáveis pelo BNDES.

PREGÃO ELETRÔNICO Nº 007/2024 – BNDES
ANEXO II – PROPOSTA COMERCIAL

LICITANTE: _____

CNPJ:_____

ENDEREÇO: _____

TELEFONE: (___) _____ **E-MAIL:** _____

REPRESENTANTE LEGAL: _____

NACIONALIDADE: _____ **ESTADO CIVIL:** _____

PROFISSÃO: _____ **FUNÇÃO NA SOCIEDADE:** _____

RG: _____ **CPF:** _____

ESTABELECIMENTOS VINCULADOS À EXECUÇÃO CONTRATUAL (MATRIZ/FILIAL):

RAZÃO SOCIAL: _____ **CNPJ:** _____

ENDEREÇO: _____

RAZÃO SOCIAL: _____ **CNPJ:** _____

ENDEREÇO: _____

DESCRIÇÃO DO OBJETO OFERTADO: Contratação de serviços continuados, sem dedicação exclusiva de mão-de-obra, especializados em segurança cibernética para o Banco Nacional de Desenvolvimento Econômico e Social – BNDES.

ITEM I – serviço técnico operacional especializado em segurança cibernética prestado por Centro de Operações de Segurança Cibernética (Cyber Security Operation Center – CSOC); e

ITEM II – serviço técnico de inteligência especializado em segurança cibernética.

Planilha de Composição de Custos e Formação de Preço					
ITEM I	**Valor por Unidade**	**Unidade**	**Meses**	**Valor Total**	**Observações**
A1 - Implantação	R$ -	Não se aplica	Não se aplica	R$ -	**Valor Total limitado ao valor unitário de (A2+A3)*6**
A2 - CSIRT - Computer Security Incident Response Team	R$ -	Mês	60	R$ -	
A3 - GVUL - Levantamento e Gestão de Vulnerabilidades	R$ -	Mês	60	R$ -	
A4 - IRC - Incident Response Consulting - Atendimento remoto	R$ -	Pacote de 40h	52	R$ -	**Atividade remunerada apenas quando demandada. Horas da equipe multidisciplinar.**
A5 - IRC - Incident Response Consulting - Atendimento presencial	R$ -	Pacote de 40h	52	R$ -	**Atividade remunerada apenas quando demandada. Horas da equipe multidisciplinar.**
Total ITEM I (A)				**R$**	**(A1+A2+A3+A4+A5)**
ITEM II	**Valor por Unidade**	**Unidade**	**Meses**	**Valor Total**	**Observações**
B1 - Implantação	R$ -	Não se aplica	Não se aplica	R$ -	**Valor Total limitado ao valor unitário de (B2+B3)*6**
B2 - CTI - Cyber Threat Intelligence	R$ -	Mês	60	R$ -	
B3 - DRP - Digital Risk Protection	R$ -	Mês	60	R$ -	
Total ITEM II (B)				**R$**	**(B1+B2+B3)**
Total Geral (A+B)				**R$**	**(A+B)**

A planilha em formato excel está disponível no site do BNDES.

O Licitante _____ declara ter ciência e aceitar todas as exigências do Edital do Pregão em referência, bem como todas as condições de execução do objeto, propondo sua execução pelo valor global de R$ ___ (___), observados os valores unitários cotados na planilha acima.

Declara, outrossim, que o valor proposto inclui todas as despesas e custos, diretos e indiretos (tais como tributos, encargos sociais e trabalhistas, contribuições, transporte, viagens, seguro e insumos), necessários ao cumprimento integral do objeto.

Por fim, o Licitante _____ informa que a validade da presente proposta é de ___ (___) dias.

Rio de Janeiro, ___ de _____ de ___.

_____

(Representante Legal do Licitante)

Obs.: O Licitante deverá observar o prazo mínimo de validade da proposta estabelecido no item 3.3 do edital .

Obs.: O arquivo eletrônico contendo o(s) modelo(s) da(s) planilha(s) de preços poderá ser obtido pelo Licitante que assim solicitar pelo e-mail licitacoes@bndes.gov.br.

PREGÃO ELETRÔNICO Nº 007/2024 – BNDES
ANEXO III – MINUTA DE CONTRATO

CONTRATO OCS Nº ___/___
CONTRATO SAP Nº _____

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL – BNDES E _____, NA FORMA ABAIXO:

O **BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL – BNDES**, empresa pública federal, com sede em Brasília - DF e serviços no Rio de Janeiro – RJ, na Av. República do Chile, n° 100, CEP nº 20.031-917, inscrito no Cadastro Nacional de Pessoas Jurídicas sob o n° 33.657.248/0001-89, doravante denominado simplesmente **BNDES**, neste ato representado na forma do seu Estatuto Social; e _____, com sede em ___, inscrito(a) no Cadastro Nacional de Pessoas Jurídicas sob o nº ___ / inscrito(a) no Cadastro de Pessoas Físicas sob o nº ___, doravante denominado(a) simplesmente **CONTRATADO**, neste ato representado na forma de seus atos constitutivos, em conformidade com o procedimento do Pregão Eletrônico nº 007/2024 - **BNDES**, autorizado em 22/04/2024, por intermédio da IP AIC/DEROP nº 01/2024, de 17/04/2024, conforme previsão orçamentária sob rubrica n° 3101700040, centro de custo nº BN00004000, observado o disposto na Lei nº 13.303/2016 e no Regulamento Licitações e Contratos do Sistema **BNDES**, têm, entre si, justo e contratado o que se contém nas Cláusulas seguintes:

(para o item I)
CLÁUSULA PRIMEIRA – OBJETO
O presente Contrato tem por objeto a prestação de serviços continuados, sem dedicação exclusiva de mão-de-obra, especializados em segurança cibernética para o Banco Nacional de Desenvolvimento Econômico e Social – BNDES, de serviço técnico operacional especializado em segurança cibernética prestado por Centro de Operações de Segurança Cibernética (Cyber Security Operation Center – CSOC), conforme especificações constantes do Termo de Referência (Anexo I do Edital do Pregão Eletrônico nº 007/2024 – **BNDES**) e da proposta apresentada pelo **CONTRATADO**, respectivamente, Anexos I e II deste Contrato.

(para o item II)
CLÁUSULA PRIMEIRA – OBJETO
O presente Contrato tem por objeto a prestação de serviços continuados, sem dedicação exclusiva de mão-de-obra, especializados em segurança cibernética para o Banco Nacional de Desenvolvimento Econômico e Social – BNDES, de serviço técnico de inteligência especializado em segurança cibernética, conforme especificações constantes do Termo de Referência (Anexo I do Edital do Pregão Eletrônico nº 007/2024 - **BNDES**) e da proposta apresentada pelo **CONTRATADO**, respectivamente, Anexos I e II deste Contrato.

CLÁUSULA SEGUNDA – VIGÊNCIA

O prazo de vigência do presente Contrato será de até 60 (sessenta) meses a contar da data de sua assinatura, sendo de:

I. até 6 (seis) meses, contados da assinatura do contrato, para execução da implantação, incluindo todas as fases até a emissão do Termo de Recebimento Definitivo;

II. até 60 (sessenta) meses a contar da emissão do Termo de Recebimento Definitivo, com opção de rescisão por parte do BNDES a partir do 30º (trigésimo) mês de vigência, desde que comunicada com antecedência de 180 (cento e oitenta) dias.

CLÁUSULA TERCEIRA – LOCAL, PRAZO E CONDIÇÕES DE EXECUÇÃO DO OBJETO

A execução do objeto contratado respeitará as especificações constantes do Termo de Referência e da proposta apresentada pelo **CONTRATADO**, respectivamente, Anexos I e II deste Contrato.

CLÁUSULA QUARTA – NÍVEIS DE SERVIÇO

Os serviços contratados deverão ser executados de acordo com os padrões de qualidade, disponibilidade e desempenho estipulados pelo **BNDES**, observados os níveis de serviço descritos no Anexo I (Termo de Referência) deste Contrato.

Parágrafo Único

O descumprimento dos níveis de serviço acarretará a aplicação dos índices de redução do preço previstos no Anexo I (Termo de Referência) deste Contrato, sem prejuízo da aplicação das penalidades previstas neste Contrato, quando cabíveis.

CLÁUSULA QUINTA – RECEBIMENTO DO OBJETO

O **BNDES** efetuará o recebimento do objeto, através do Gestor do Contrato, mencionados na Cláusula de Obrigações do **BNDES** deste Contrato, observado o disposto no Anexo I (Termo de Referência) deste Contrato.

CLÁUSULA SEXTA – PREÇO

O **BNDES** pagará ao **CONTRATADO**, pela execução do objeto contratado, o valor de até R$ ___ (___), conforme proposta apresentada (Anexo II deste Contrato), observado o disposto na Cláusula de Pagamento deste Instrumento.

Parágrafo Primeiro

No valor ajustado no *caput* desta Cláusula estão incluídos todos os insumos, encargos trabalhistas e tributos, inclusive contribuições fiscais e parafiscais, bem como quaisquer outras despesas necessárias à execução deste Contrato.

Parágrafo Segundo

Na hipótese de o objeto ser, a critério do **BNDES**, parcialmente executado e recebido, os valores previstos nesta Cláusula serão proporcionalmente reduzidos, sem prejuízo da aplicação das penalidades cabíveis.

Parágrafo Terceiro

Caso o **BNDES** não demande o total do objeto previsto neste Contrato, não será devida indenização ao **CONTRATADO**.

Parágrafo Quarto
O **CONTRATADO** deverá arcar com os ônus decorrentes de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso os quantitativos previstos inicialmente em sua proposta não sejam satisfatórios para o atendimento ao objeto deste Contrato;

Parágrafo Quinto
O **BNDES** não se compromete à utilização do total estimado de horas extraordinárias, sendo pagas somente as que efetivamente forem realizadas, que serão aferidas através de planilhas a serem apresentadas, mensalmente, pelo **CONTRATADO**.

CLÁUSULA SÉTIMA – PAGAMENTO
O **BNDES** efetuará o pagamento referente ao objeto deste Contrato, mensalmente, por meio de crédito em conta bancária, em até 10 (dez) dias úteis, a contar da data de apresentação do documento fiscal ou equivalente legal (prioritariamente nota fiscal, e nos casos de dispensa da nota fiscal: fatura, boleto bancário com código de barras, recibo de pagamento a autônomo), desde que tenha sido efetuado o ateste pelo Gestor do Contrato das obrigações contratuais assumidas pelo **CONTRATADO**, observado o disposto no Anexo I (Termo de Referência) deste Instrumento.

Parágrafo Primeiro
O documento fiscal ou equivalente legal deverá ser apresentado ao **BNDES** no mês de sua emissão e até o dia 25 (vinte e cinco) do mesmo – ou data anterior que viabilize o tempestivo recolhimento de ISS possibilitando o cumprimento, pelo **BNDES,** das obrigações fiscais principais e acessórias decorrentes deste Contrato. Havendo impedimento legal para o cumprimento desse prazo, o documento fiscal ou equivalente legal deverá ser apresentado até o primeiro dia útil do mês seguinte, seguinte da prestação do serviço/fornecimento do bem.

Parágrafo Segundo
A apresentação do documento de cobrança fora do prazo previsto nesta cláusula poderá implicar em sua rejeição e no direito do **BNDES** se ressarcir, preferencialmente, mediante desconto do valor a ser pago ao **CONTRATADO**, por qualquer penalidade tributária incidente pelo atraso.

Parágrafo Terceiro
O primeiro documento fiscal ou equivalente legal terá como objeto de cobrança o período compreendido entre o dia de início da prestação dos serviços e o último dia desse mês, e os documentos fiscais ou equivalentes legais subsequentes terão como referência o período compreendido entre o primeiro e o último dia de cada mês. O último documento fiscal ou equivalente legal, por seu turno, referir-se-á ao período compreendido entre o primeiro dia do último mês da prestação dos serviços e o último dia de serviço prestado. Em todos os casos, o documento fiscal ou equivalente legal só poderá ser emitido e apresentado ao **BNDES** após a efetiva prestação do serviço, respeitado o disposto no Parágrafo anterior.

Parágrafo Quarto
Para toda efetivação de pagamento, o Contratado deverá encaminhar o documento fiscal ou equivalente em meio digital para caixa postal eletrônica ou protocolar em sistema eletrônico próprio do **BNDES**, considerando as orientações do Contratante vigentes na ocasião do pagamento. No caso de emissão de documento fiscal exclusivamente em meio físico o mesmo deverá ser encaminhado ao protocolo do **BNDES** para devido registro de recebimento.

Parágrafo Quinto
O documento fiscal ou equivalente legal deverá respeitar a legislação tributária e conter, minimamente, as seguintes informações:

I. número da Ordem de Compra/Serviço – OCS;
II. número SAP do Contrato;
III. número do pedido SAP, a ser informado pelo Gestor do Contrato;
IV. número da Folha de Registro de Serviços (FRS), a ser informado pelo Gestor do Contrato;
V. descrição detalhada do objeto executado e dos respectivos valores;
VI. período de referência da execução do objeto;
VII. nome e número do CNPJ do **CONTRATADO**, cuja regularidade fiscal tenha sido avaliada na fase de habilitação, bem como o número de inscrição na Fazenda Municipal e/ou Estadual, conforme o caso;
VIII. nome, telefone e *e-mail* do responsável pelo documento fiscal ou equivalente legal;
IX. nome e número do banco e da agência, bem como o número da conta corrente da **CONTRATADO**, vinculada ao CNPJ constante do documento fiscal ou equivalente legal, com respectivos dígitos verificadores;
X. tomador do serviço: Banco Nacional de Desenvolvimento Econômico e Social – **BNDES**;
XI. CNPJ do tomador do serviço: 33.657.248/0001-89;
XII. local de execução do objeto, emitindo-se um documento fiscal ou equivalente legal para cada Município em que o serviço seja prestado, se for o caso;
XIII. código do serviço, nos termos da lista anexa à Lei Complementar nº 116/2003, em concordância com as informações inseridas na Declaração de Informações para Fornecimento - DIF; e
XIV. destaque das retenções tributárias aplicáveis, conforme estabelecido na DIF.

Parágrafo Sexto
Os pagamentos a serem efetuados em favor do **CONTRATADO** estarão sujeitos, no que couber, às retenções de tributos, nos termos da legislação tributária e com base nas informações prestadas pelo **CONTRATADO**. Em casos de dispensa ou benefício fiscal que implique em redução ou eliminação da retenção de tributos, o **CONTRATADO** fornecerá todos os documentos comprobatórios.

Parágrafo Sétimo
Caso o **CONTRATADO** emita documento fiscal ou equivalente legal autorizado por Município diferente daquele onde se localiza o estabelecimento do **BNDES** tomador do serviço e destinatário da cobrança, deverá providenciar o cadastro junto à Secretaria Municipal de Fazenda ou órgão equivalente do Município do estabelecimento tomador, salvo quando se aplicar uma das exceções constantes dos incisos do artigo 3º da Lei Complementar Federal nº 116/03. A inexistência desse cadastro ou o cadastro em item diverso do faturado não constitui impeditivo ao processo de pagamento, mas um ônus a ser suportado pelo **CONTRATADO**, uma vez que o **BNDES** está obrigado a reter na fonte a quantia equivalente ao ISS dos serviços faturados, conforme legislação aplicável.

Parágrafo Oitavo
O documento fiscal ou equivalente legal emitido pelo **CONTRATADO** deverá estar em conformidade com a legislação do Município onde o **CONTRATADO** esteja estabelecido, cuja regularidade fiscal foi avaliada na etapa de habilitação, e com as normas regulamentares aprovadas pela Secretaria da Receita Federal do Brasil, especialmente no que tange à retenção de tributos,

sob pena de devolução do documento e interrupção do prazo para pagamento.

Parágrafo Nono
Ao documento fiscal ou equivalente legal deverão ser anexados:

I. certidões de regularidade fiscal exigidas na fase de habilitação;

II. comprovante de que o **CONTRATADO** é optante do Simples Nacional, se for o caso;

III. em caso de isenção/imunidade tributária, documentos comprobatórios com a indicação do dispositivo legal que ampara a isenção/imunidade; e

IV. demais documentos solicitados pelo Gestor do Contrato, necessários ao pagamento do objeto contratado.

Parágrafo Décimo
Caso sejam verificadas divergências, o **BNDES** devolverá o documento fiscal ou equivalente legal ao **CONTRATADO** ou solicitará a emissão de carta de correção, quando cabível, interrompendo-se o prazo de pagamento até que este providencie as medidas saneadoras ou comprove a correção dos dados contestados pelo **BNDES**.

Parágrafo Décimo Primeiro
Além de outras hipóteses previstas em lei ou no Contrato, o **BNDES** poderá descontar, do montante expresso no documento fiscal ou equivalente legal, os valores referentes a multas, indenizações apuradas em processo administrativo, bem como qualquer obrigação que decorra do descumprimento da legislação pelo **CONTRATADO**.

Parágrafo Décimo Segundo
Caso o **BNDES** não efetue o pagamento na forma prevista nesta Cláusula, em decorrência de fato não atribuível ao **CONTRATADO**, aos valores devidos serão acrescidos juros de mora de 0,5% (meio por cento) ao mês, *pro rata tempore*, calculados desde o dia do vencimento até a data da efetiva liquidação.

Parágrafo Décimo Terceiro
Fica assegurado ao **BNDES** o direito de deduzir do pagamento devido ao **CONTRATADO**, por força deste Contrato ou de outro contrato mantido com o **BNDES**, o valor correspondente aos pagamentos efetuados a maior ou em duplicidade.

CLÁUSULA OITAVA – EQUILÍBRIO ECONÔMICO-FINANCEIRO DO CONTRATO
O **BNDES** e o **CONTRATADO** têm direito ao equilíbrio econômico-financeiro do Contrato, em consonância com o inciso XXI, do artigo 37, da Constituição Federal, a ser realizado mediante reajuste ou revisão de preços.

Parágrafo Primeiro
O reajuste de preços, na forma prevista na legislação, poderá ser requerido pelo **CONTRATADO** a cada período de 12 (doze) meses, sendo o primeiro contado do dia ___/___/___, data de apresentação da proposta (Anexo II deste Contrato), e os seguintes, do fato gerador anterior, adotando-se para tanto a aplicação do Índice de Custo de Tecnologia da Informação - ICTI acumulado sobre o preço referido na Cláusula de Preço deste Instrumento.

Parágrafo Segundo
A revisão de preços poderá ser realizada por iniciativa do **BNDES** ou mediante solicitação do

CONTRATADO, quando ocorrer fato imprevisível ou previsível, porém, de consequências incalculáveis, retardador ou impeditivo da execução do Contrato, ou ainda em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual, que onere ou desonere as obrigações pactuadas no presente Instrumento, sendo, porém, vedada nas hipóteses em que o risco seja alocado ao **CONTRATADO** nos termos da Cláusula de Matriz de Riscos, respeitando-se o seguinte:

I. o **CONTRATADO** deverá formular ao **BNDES** requerimento para a revisão do Contrato, comprovando a ocorrência do fato gerador;

II. a comprovação será realizada por meio de documentos, tais como, atos normativos que criem ou alterem tributos, lista de preço de fabricantes, notas fiscais de aquisição de matérias-primas, de transporte de mercadorias, alusivas à época da elaboração da proposta ou do último reajuste e do momento do pedido de revisão; e

III. com o requerimento, o **CONTRATADO** deverá apresentar planilhas de custos unitários, comparativas entre a data da formulação da proposta ou do último reajuste e o momento do pedido de revisão, contemplando os custos unitários envolvidos e evidenciando o quanto o aumento de preços ocorrido repercute no valor pactuado.

Parágrafo Terceiro
Independentemente de solicitação, o **BNDES** poderá convocar o **CONTRATADO** para negociar a redução dos preços, mantendo o mesmo objeto contratado, na quantidade e nas especificações indicadas na proposta, em virtude da redução dos preços de mercado, ou de itens que compõem o custo, cabendo ao **CONTRATADO** apresentar as informações solicitadas pelo **BNDES**.

Parágrafo Quarto
O **CONTRATADO** deverá solicitar o reajuste e/ou a revisão de preços até o encerramento do Contrato, hipótese em que os efeitos financeiros serão concedidos de modo retroativo a partir do fato gerador, observando-se, ainda, que:

I. caso o fato gerador do reajuste e/ou da revisão de preços ou a divulgação do índice de reajuste ocorra com antecedência inferior a 60 (sessenta) dias do encerramento do Contrato, o **CONTRATADO** terá o prazo de 60 (sessenta) dias, a contar do fato gerador ou da data de divulgação do índice, para solicitar o reajuste e/ou a revisão de preços;

II. caso a divulgação do índice de reajuste ocorra após o encerramento do Contrato, o **CONTRATADO** terá o prazo de 60 (sessenta) dias, a contar da data de divulgação do índice, para solicitar o reajuste de preços;

III. o **BNDES** deverá analisar o pedido de reajuste e/ou revisão de preços em até 60 (sessenta) dias, contados da solicitação e da entrega pelo **CONTRATADO** dos comprovantes de variação dos custos, ficando este prazo suspenso, a critério do **BNDES**, enquanto o **CONTRATADO** não apresentar a documentação solicitada para a comprovação da variação de custos; e

IV. caso o **CONTRATADO** não solicite o reajuste e/ou revisão de preços nos prazos fixados acima, operar-se-á a renúncia a eventual direito ao reajuste e/ou à revisão.

CLÁUSULA NONA – MATRIZ DE RISCOS
O **BNDES** e o **CONTRATADO**, tendo como premissa a obtenção do melhor custo contratual mediante a alocação do risco à parte com maior capacidade para geri-lo e absorvê-lo, identificam os riscos decorrentes da relação contratual e, sem prejuízo de outras previsões contratuais, estabelecem os respectivos responsáveis na Matriz de Riscos constante do Anexo III deste Contrato.

Parágrafo Primeiro
O reajuste de preço aludido na Matriz de Riscos deve respeitar o disposto na Cláusula de Equilíbrio Econômico-Financeiro deste Contrato.

Parágrafo Segundo
É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na Matriz de Riscos, como de responsabilidade do **CONTRATADO**.

CLÁUSULA DÉCIMA – GARANTIA CONTRATUAL
O **CONTRATADO** prestará, no prazo de até 15 (quinze) dias úteis, contados da convocação, garantia contratual, sob pena de aplicação de penalidade nos termos deste Contrato, observadas as condições para sua aceitação estipuladas nos incisos abaixo, no valor de R$ ___ (___), que lhe será devolvida após a verificação do cumprimento fiel, correto e integral dos termos contratuais.

I. Caução em dinheiro: deverá ser depositada em favor do **BNDES**, de acordo com as orientações que serão fornecidas quando da referida convocação;

II. Seguro Garantia: a Apólice de Seguro deverá ser emitida por Instituição autorizada pela SUSEP a operar no mercado securitário, que não se encontre sob regime de Direção Fiscal, Intervenção, Liquidação Extrajudicial ou Fiscalização Especial, e que não esteja cumprindo penalidade de suspensão imposta pela SUSEP;

a) O Instrumento de Apólice de Seguro deve prever expressamente:

a.1) responsabilidade da seguradora por todas e quaisquer multas de caráter sancionatório aplicadas ao **CONTRATADO**;

a.2) vigência pelo prazo contratual;

a.3) prazo de 90 (noventa) dias, contados a partir do término da vigência contratual, para apuração de eventual inadimplemento do **CONTRATADO** - ocorrido durante a vigência contratual -, e para a comunicação da expectativa de sinistro ou do efetivo aviso de sinistro, observados os prazos prescricionais pertinentes.

III. Fiança Bancária: a Carta de Fiança deverá ser emitida por Instituição Financeira autorizada pelo Banco Central do Brasil - BACEN para funcionar no Brasil e que não se encontre em processo de liquidação extrajudicial ou de intervenção do BACEN.

a) O Instrumento de Fiança deve prever expressamente:

a.1) renúncia expressa, pelo fiador, ao benefício de ordem disposto no artigo 827 do Código Civil;

a.2) vigência pelo prazo contratual;

a.3) prazo de 90 (noventa) dias, contados a partir do término da vigência contratual, para apuração de eventual inadimplemento do **CONTRATADO** - ocorrido durante a vigência contratual -, e para a comunicação do inadimplemento à Instituição Financeira, observados os prazos prescricionais pertinentes.

Parágrafo Primeiro
O prazo previsto para a apresentação da garantia poderá ser prorrogado, por igual período, quando solicitado pelo **CONTRATADO** durante o respectivo transcurso, e desde que ocorra motivo justificado e aceito pelo **BNDES**.

Parágrafo Segundo

Havendo majoração do preço contratado, decorrente de reajuste, repactuação ou revisão de preços causada por alterações na legislação tributária, fica dispensada a atualização da garantia, salvo se o valor da atualização for igual ou superior ao patamar referenciado no inciso II do artigo 91 do Regulamento de Licitações e Contratos do **SISTEMA BNDES**.

Parágrafo Terceiro

Nos demais casos que demandem a complementação ou renovação da garantia, tais como alteração do objeto (aditivo quantitativo ou qualitativo), prorrogação contratual, dentre outros, o **CONTRATADO** deverá providenciá-la no prazo estipulado pelo **BNDES**.

Parágrafo Quarto

Sempre que o contrato for garantido por fiança bancária ou seguro garantia, o **CONTRATADO** deve obter do garantidor anuência em relação à manutenção da garantia, no prazo de 10 (dez) dias úteis a contar da assinatura do aditivo ou recebimento de carta de apostilamento ou aditivo epistolar, conforme o caso. Recusando-se o garantidor a manter a garantia, cabe ao **CONTRATADO** obter nova garantia no mesmo prazo, prorrogável por igual período a critério do **BNDES**.

Parágrafo Quinto

A garantia contratual deverá cobrir:

I. todas as obrigações decorrentes do objeto contratual, assim como eventuais danos decorrentes de seu descumprimento;

II. todas as obrigações relacionadas ao objeto principal, ainda que decorrentes de sua manutenção e/ou refazimento, bem como das medidas necessárias à prevenção ordinária de sinistros, prejuízos e danos em geral;

III. prejuízos decorrentes de atos de corrupção praticados sem participação dolosa do **BNDES** ou de seus representantes;

IV. prejuízos diretos causados ao **BNDES** decorrentes de culpa ou dolo durante a execução do Contrato;

V. multas moratórias e/ou punitivas aplicadas pelo **BNDES** ao **CONTRATADO**;

VI. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pelo **CONTRATADO**, quando o objeto contratual demandar cessão de mão de obra com dedicação exclusiva.

Parágrafo Sexto

Em caso de prorrogação da vigência ou alteração do objeto contratual, o **CONTRATADO** deverá notificar a entidade fiadora/seguradora, conforme o caso, no prazo de até 10 (dez) dias úteis, contados da formalização do respectivo Instrumento Contratual.

Parágrafo Sétimo

Por se tratar de garantia contratual prestada em benefício de uma Estatal, caso os documentos de caução, fiança ou seguro façam referência à Lei nº 8.666/1993 e/ou à Lei nº 14.133/2021, aplicam-se as disposições respectivas da Lei nº 13.303/2016, no que couber.

CLÁUSULA DÉCIMA PRIMEIRA – OBRIGAÇÕES DO CONTRATADO

Além de outras obrigações estabelecidas neste Instrumento, em seus anexos ou nas leis vigentes, particularmente na Lei nº 13.303/2016, ou que entrarem em vigor, constituem obrigações do **CONTRATADO**:

I. manter durante a vigência deste Contrato todas as condições de habilitação e a ausência de impedimentos exigidas quando da contratação, comprovando-as sempre que solicitado pelo **BNDES**;

II. comunicar a imposição, de penalidade que acarrete o impedimento de contratar com o **BNDES**, bem como a eventual perda dos pressupostos para a licitação;

III. reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções decorrentes da execução;

IV. reparar todos os danos e prejuízos causados ao **BNDES** ou a terceiros, não restando excluída ou reduzida esta responsabilidade pela presença de fiscalização ou pelo acompanhamento da execução por parte do Gestor do Contrato;

V. pagar todos os encargos e tributos, que incidam ou venham a incidir, direta ou indiretamente, sobre o objeto deste Contrato, podendo o **BNDES**, a qualquer momento, exigir do **CONTRATADO** a comprovação de sua regularidade;

VI. assumir a responsabilidade integral por quaisquer ônus que venham a ser impostos ao **BNDES** em virtude de documento fiscal que seja emitido em desacordo com a legislação aplicável;

VII. providenciar, perante a Receita Federal do Brasil - RFB, comprovando ao **BNDES**, sua exclusão obrigatória do Simples Nacional, no prazo estipulado pelo artigo 30 da Lei Complementar nº 123/2006, se o **CONTRATADO**, quando optante:

a) extrapolar o limite de receita bruta anual previsto no artigo 3º da Lei Complementar nº 123/2006, ao longo da vigência deste Contrato; ou

b) enquadrar-se em alguma das situações previstas no artigo 17 da Lei Complementar nº 123/2006;

VIII. permitir vistorias e acompanhamento da execução do objeto pelo Gestor do Contrato;

IX. obedecer às instruções e aos procedimentos, estabelecidos pelo **BNDES**, para a adequada execução do Contrato;

X. designar 01 (um) preposto como responsável pelo Contrato firmado com o **BNDES**, para participar de eventuais reuniões e ser o interlocutor do **CONTRATADO**, zelando pelo fiel cumprimento das obrigações previstas neste Instrumento;

XI. Fornecer informações para o gerenciamento, por parte do BNDES, de riscos social, ambiental ou climático, relacionados ao objeto do contrato.

XI. apresentar, em até 10 (dez) dias úteis após a convocação, a Declaração de Informações para Fornecimento - DIF, adequadamente preenchida, sob pena de instauração de procedimento punitivo para aplicação de penalidade, e de retenção tributária, pelo **BNDES**, nos casos previstos em lei, da alíquota que entender adequada;

a) as informações inseridas na Declaração de Informações para Fornecimento – DIF não deverão divergir das constantes do documento fiscal ou equivalente legal.

CLÁUSULA DÉCIMA SEGUNDA – CONDUTA ÉTICA DO CONTRATADO E DO BNDES

O **CONTRATADO** e o **BNDES** comprometem-se a manter a integridade nas relações público-privadas, agindo de boa-fé e de acordo com os princípios da moralidade administrativa e da impessoalidade, além de pautar sua conduta por preceitos éticos e, em especial, por sua responsabilidade socioambiental.

Parágrafo Primeiro

Em atendimento ao disposto no *caput* desta Cláusula, o **CONTRATADO** obriga-se, inclusive, a:

I. não oferecer, prometer, dar, autorizar, solicitar ou aceitar, direta ou indiretamente, qualquer vantagem indevida, seja pecuniária ou de outra natureza, consistente em fraude, ato de corrupção ou qualquer outra violação de dever legal, relacionada com este Contrato, bem como a tomar todas as medidas ao seu alcance para impedir administradores, empregados, agentes, representantes, fornecedores, contratados ou subcontratados, seus ou de suas controladas, de fazê-lo;

II. impedir o favorecimento ou a participação de empregado ou dirigente do Sistema **BNDES** (**BNDES** e suas subsidiárias) na execução do objeto do presente Contrato;

III. providenciar para que não sejam alocados, na execução dos serviços, familiares de dirigente ou empregado do Sistema **BNDES**, considerando-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

IV. observar a Política para Transações com Partes Relacionadas e o Código de Ética do Sistema **BNDES** vigentes ao tempo da contratação, bem como a Política Corporativa de Integridade do Sistema **BNDES**, assegurando-se de que seus representantes, administradores, todos os profissionais envolvidos na execução do objeto e eventuais subcontratados pautem seu comportamento e sua atuação pelos princípios neles constantes;

V. adotar, na execução dos serviços, boas práticas de sustentabilidade ambiental, de otimização de recursos, de redução de desperdícios e de redução da poluição;

VI. informar imediatamente ao **BNDES** a ocorrência de potencial situação de conflito de interesses, comunicando na mesma oportunidade as medidas que serão adotadas para o tratamento da questão; e

VII. notificar imediatamente o **BNDES** sobre qualquer investigação ou procedimento iniciado por autoridade governamental relacionado à violação de Leis Anticorrupção (nacional ou estrangeira) e/ou de obrigações da empresa, de seus administradores, diretores, prepostos, empregados, representantes ou terceiros a seu serviço, incluindo subcontratados, referentes a este Contrato.

Parágrafo Segundo
O **BNDES** recomenda, ao **CONTRATADO**, considerar em suas práticas de gestão a implantação de programa de integridade estruturado, voltado à prevenção, detecção e remediação da ocorrência de fraudes e atos de corrupção.

Parágrafo Terceiro
Verificada uma das situações mencionadas nos incisos II e III do Parágrafo Primeiro desta Cláusula, compete ao **CONTRATADO** afastar imediatamente da execução do Contrato os agentes que impliquem a ocorrência dos impedimentos e favorecimentos aludidos, além de comunicar tal fato ao **BNDES**, sem prejuízo de apuração de sua responsabilidade, caso tenha agido de má-fé.

Parágrafo Quarto
O **CONTRATADO** declara ter conhecimento do Código de Ética do Sistema **BNDES**, bem como da Política Corporativa de Integridade do Sistema **BNDES**, que poderão ser consultados por intermédio do sítio eletrônico *www.bndes.gov.br* ou requisitados ao Gestor do Contrato.

Parágrafo Quinto
Eventuais irregularidades ou descumprimentos das normas internas do **BNDES** ou da legislação vigente podem ser denunciados à Ouvidoria por qualquer cidadão através dos seguintes canais: página na *internet* (www.bndes.gov.br/ouvidoria); correio (Caixa Postal 15054, CEP 20031-120, Rio de Janeiro – RJ); e telefone (0800 702 6307).

CLÁUSULA DÉCIMA TERCEIRA – SIGILO DAS INFORMAÇÕES

Cabe ao **CONTRATADO** cumprir as seguintes regras de sigilo e assegurar a aceitação e adesão às mesmas por profissionais que integrem ou venham a integrar a sua equipe na prestação do objeto deste Contrato, as quais perdurarão, inclusive, após a cessação do vínculo contratual e da prestação dos serviços:

I. cumprir as diretrizes e normas da Política Corporativa de Segurança da Informação do **BNDES**, necessárias para assegurar a integridade e o sigilo das informações;

II. não acessar informações sigilosas do **BNDES**, salvo quando previamente autorizado por escrito;

III. sempre que tiver acesso às informações mencionadas no inciso anterior:

a) manter sigilo dessas informações, não podendo copiá-las, reproduzi-las, retê-las ou praticar qualquer outra forma de uso que não seja imprescindível para a adequada prestação do objeto deste Contrato;

b) limitar o acesso às informações aos profissionais envolvidos na prestação dos serviços objeto deste Contrato, os quais deverão estar cientes da natureza sigilosa das informações e das obrigações e responsabilidades decorrentes do uso dessas informações; e

c) informar imediatamente ao **BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como dos profissionais envolvidos, adotando todas as orientações do **BNDES** para remediar a violação;

IV. entregar ao **BNDES**, ao término da vigência deste Contrato, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa e registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, assumindo o compromisso de não utilizar qualquer informação sigilosa a que teve acesso no âmbito deste Contrato;

V. apresentar, na Reunião Preliminar, Termos de Confidencialidade, conforme minuta constante do Anexo V (Minuta de Termo de Confidencialidade para Profissionais) deste Contrato, assinados pelos profissionais que acessarão informações sigilosas, devendo referida obrigação ser também cumprida por ocasião de substituição desses profissionais; e

VI. observar o disposto no Termo de Confidencialidade assinado por seu Representante Legal, constante do Anexo IV (Termo de Confidencialidade para Representante Legal) deste Contrato.

CLÁUSULA DÉCIMA QUARTA – ACESSO E PROTEÇÃO DE DADOS PESSOAIS

As partes assumem o compromisso de proteger os direitos fundamentais de liberdade e de privacidade, relativos ao tratamento de dados pessoais, nos meios físicos e digitais, devendo, para tanto, adotar medidas de boa governança sob o aspecto técnico, jurídico e administrativo, inclusive de segurança, e observar que:

I. Eventual tratamento de dados pessoais em razão do presente Contrato deverá ser realizado conforme os parâmetros previstos na legislação, especialmente na Lei n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais - LGPD, dentro de propósitos legítimos, específicos, explícitos e informados ao titular;

II. O tratamento será limitado às atividades necessárias ao atingimento das finalidades contratuais e, caso seja necessário, ao cumprimento de suas obrigações legais ou regulatórias, sejam de ordem principal ou acessória, observando-se que, em caso de necessidade de coleta de dados pessoais diretamente pelo **CONTRATADO**, esta será realizada mediante prévia aprovação do **BNDES**,

responsabilizando-se o **CONTRATADO** por obter o consentimento dos titulares, salvo nos casos em que a legislação dispense tal medida;

III. O **CONTRATADO** deverá seguir as instruções recebidas do **BNDES** em relação ao tratamento de dados pessoais;

IV. No caso de tratamento de dados pessoais realizado pelo **CONTRATADO** para cumprimento de suas obrigações legais ou para atendimento de suas próprias finalidades, o **BNDES** não será considerado "Controlador de Dados Pessoais" e, sim, o **CONTRATADO**;

V. Os dados coletados somente poderão ser utilizados pelas partes, seus representantes, empregados e prestadores de serviços diretamente alocados na execução contratual, sendo que, em hipótese alguma, poderão ser compartilhados ou utilizados para outros fins, sem a prévia autorização do **BNDES**, ou caso haja alguma ordem judicial, observando-se as medidas legalmente previstas para tanto;

VI. O **CONTRATADO** deve manter a confidencialidade dos dados pessoais obtidos em razão do presente contrato, devendo adotar as medidas técnicas e administrativas adequadas e necessárias, visando assegurar a proteção dos dados, nos termos do artigo 46 da LGPD, de modo a garantir um nível apropriado de segurança e a prevenção e mitigação de eventuais riscos;

VII. Os dados deverão ser armazenados de maneira segura pelo **CONTRATADO,** que utilizará recursos de segurança da informação e tecnologia adequados, inclusive quanto a mecanismos de detecção e prevenção de ataques cibernéticos e incidentes de segurança da informação.

VIII. O **CONTRATADO** dará conhecimento formal para seus empregados e/ou prestadores de serviço acerca das disposições previstas nesta Cláusula e na Cláusula de Sigilo das Informações, responsabilizando-se por eventual uso indevido dos dados pessoais, bem como por quaisquer falhas nos sistemas por ela empregados para o tratamento dos dados.

IX. O **BNDES** possui direito de regresso em face do **CONTRATADO** em razão de eventuais danos causados por este em decorrência do descumprimento das responsabilidades e obrigações previstas no âmbito deste contrato e da Lei Geral de Proteção de Dados Pessoais;

X. O **CONTRATADO** deverá disponibilizar ao titular do dado um canal ou sistema em que seja garantida consulta facilitada e gratuita sobre a forma, a duração do tratamento e a integralidade de seus dados pessoais.

XI. O **CONTRATADO** deverá informar imediatamente ao **BNDES** todas as solicitações recebidas em razão do exercício dos direitos pelo titular dos dados relacionados a este Contrato, seguindo as orientações fixadas pelo **BNDES** e pela legislação em vigor para o adequado endereçamento das demandas.

XII. O **CONTRATADO** deverá manter registro de todas as operações de tratamento de dados pessoais que realizar no âmbito do Contrato disponibilizando, sempre que solicitado pelo **BNDES**, as informações necessárias à produção do Relatório de Impacto de Dados Pessoais, disposto no artigo 5º, XVII, da Lei Geral de Proteção de Dados Pessoais.

XIII. Qualquer incidente ao qual o **CONTRATADO** tiver dado causa e que implique em violação ou risco de violação ou vazamento de dados pessoais deverá ser prontamente comunicado ao **BNDES**, informando-se também todas as providências adotadas e os dados pessoais eventualmente afetados, cabendo ao **CONTRATADO** disponibilizar as informações e documentos solicitados e colaborar com qualquer investigação ou auditoria que venha a ser realizada.

XIV. Ao final da vigência do Contrato, o **CONTRATADO** deverá eliminar de sua base de informações todo e qualquer dado pessoal que tenha tido acesso em razão da execução do objeto contratado, salvo quando tenha que manter a informação para o cumprimento de obrigação legal.

Parágrafo Primeiro

As Partes reconhecem que, se durante a execução do Contrato armazenarem, coletarem, tratarem ou de qualquer outra forma processarem dados pessoais, no sentido dado pela legislação vigente aplicável, o **BNDES** será considerado "Controlador de Dados", e o **CONTRATADO** "Operador" ou "Processador de Dados", salvo nas situações expressas em contrário nesse Contrato. Contudo, caso o **CONTRATADO** descumpra as obrigações prevista na legislação de proteção de dados ou as instruções do **BNDES**, será equiparado a "Controlador de Dados", inclusive para fins de sua responsabilização por eventuais danos causados.

Parágrafo Segundo

Cada uma das Partes será controladora independente, para os fins desse **CONTRATO**, cabendo definir individualmente as bases legais apropriadas e diretrizes para as operações de tratamento, em relação aos seguintes dados pessoais: (i) que vierem a coletar diretamente junto aos respectivos titulares, desde que essa operação de tratamento se dê com base em suas próprias decisões; (ii) oriundos de suas próprias bases de dados; e (iii) relativos ao seu corpo de colaboradores, funcionários e/ou prepostos envolvidos para a regular execução deste Contrato.

Parágrafo Terceiro

Caso o **CONTRATADO** disponibilize dados de terceiros, além das obrigações no *caput* desta Cláusula, deve se responsabilizar por eventuais danos que o **BNDES** venha a sofrer em decorrência de uso indevido de dados pessoais por parte do **CONTRATADO**, sempre que ficar comprovado que houve falha de segurança técnica e administrativa, descumprimento de regras previstas na legislação de proteção à privacidade e dados pessoais, e das orientações do **BNDES**, sem prejuízo das penalidades deste Contrato.

Parágrafo Quarto

A assinatura deste Contrato importa na manifestação de inequívoco consentimento do titular, seja ele pessoa física direta ou indiretamente relacionada ao **CONTRATADO**, inclusive sócios, representantes legais, empregados, contratados e/ou terceirizados, quando for o caso, dos dados pessoais que tenham se tornados públicos como condição para participação na licitação e para contratação, para tratamento pelo **BNDES**, na forma da Lei nº 13.709/2018. Poderão ser solicitados pelo **BNDES** dados pessoais adicionais a fim de viabilizar o cumprimento de obrigação legal.

Parágrafo Quinto

Os representantes legais signatários do presente autorizam a divulgação dos dados pessoais expressamente contidos nos documentos decorrentes do procedimento de licitação, tais como nome, CPF, e-mail, telefone e cargo, para fins de publicidade das contratações administrativas no site institucional do **BNDES** e em cumprimento à Lei nº 12.527/ 2011 (Lei de Acesso à Informação).

Parágrafo Sexto
As partes comprometem-se a coletar o consentimento, quando necessário, conforme previsto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), bem como informar aos titulares dos dados pessoais mencionados no presente instrumento, para as finalidades descritas no parágrafo acima.

CLÁUSULA DÉCIMA QUINTA – OBRIGAÇÕES DO BNDES
Além de outras obrigações estipuladas neste Instrumento, em seus anexos ou nas leis vigentes, particularmente na Lei nº 13.303/2016, ou que entrarem em vigor, constituem obrigações do **BNDES**:

I. realizar os pagamentos devidos ao **CONTRATADO**, nas condições estabelecidas neste Contrato;

II. designar, como Gestor do Contrato, _____, que atualmente exerce a função de _____, a quem caberá o acompanhamento, a fiscalização e a avaliação da execução dos serviços, bem como a liquidação da despesa e o atestado de cumprimento das obrigações assumidas;

III. designar, como substituto do Gestor do Contrato, para atuar em sua eventual ausência, _____, que atualmente exerce a função de _____;

IV. alterar, quando conveniente, o Gestor do Contrato e/ou o seu substituto, por outro profissional, mediante comunicação escrita ao **CONTRATADO**;

V. fornecer ao **CONTRATADO**, quando solicitado ao Gestor do Contrato, acesso ao Código de Ética do Sistema **BNDES**, da Política Corporativa de Integridade do Sistema **BNDES** e da Política Corporativa de Segurança da Informação do **BNDES**;

VI. colocar à disposição do **CONTRATADO** todas as informações necessárias à perfeita execução dos serviços objeto deste Contrato; e

VII. comunicar ao **CONTRATADO**, por escrito:

a) quaisquer instruções ou procedimentos sobre assuntos relacionados ao Contrato;

b) a abertura de procedimento administrativo para a apuração de condutas irregulares do **CONTRATADO**, concedendo-lhe prazo para defesa; e

c) a aplicação de eventual penalidade, nos termos deste Contrato.

CLÁUSULA DÉCIMA SEXTA – EQUIDADE DE GÊNERO E VALORIZAÇÃO DA DIVERSIDADE
O **CONTRATADO** deverá comprovar, sempre que solicitado pelo **BNDES**, a inexistência de decisão administrativa final sancionadora, exarada por autoridade ou órgão competente, em razão da prática de atos, pelo próprio **CONTRATADO** ou dirigentes, administradores ou sócios majoritários, que importem em discriminação de raça ou gênero, exploração irregular, ilegal ou criminosa do trabalho infantil ou prática relacionada ao trabalho em condições análogas à escravidão, e de sentença condenatória transitada em julgado, proferida em decorrência dos referidos atos, e, se for o caso, de outros que caracterizem assédio moral ou sexual e importem em crime contra o meio ambiente.

Parágrafo Primeiro
Na hipótese de ter havido decisão administrativa e/ou sentença condenatória, nos termos referidos no *caput* desta Cláusula, a execução do objeto contratual poderá ser suspensa pelo **BNDES** até a comprovação do cumprimento da reparação imposta ou da reabilitação do **CONTRATADO** ou de seus dirigentes, conforme o caso.

Parágrafo Segundo
A comprovação a que se refere o *caput* desta Cláusula será realizada por meio de declaração, sem prejuízo da verificação do sistema informativo interno do **BNDES** – Sistema de Gerenciamento do Cadastro de Entidades (N02), acerca da inexistência de sanção em face do **CONTRATADO** e/ou de seus dirigentes, administradores ou sócios majoritários que impeça a contratação.

CLÁUSULA DÉCIMA SÉTIMA – CESSÃO DE CONTRATO OU DE CRÉDITO, SUCESSÃO CONTRATUAL E SUBCONTRATAÇÃO
É vedada a cessão deste Contrato, total ou parcialmente, ou de qualquer crédito dele decorrente, bem como a emissão, por parte do **CONTRATADO**, de qualquer título de crédito em razão do mesmo.

Parágrafo Primeiro
É admitida a sucessão contratual nas hipóteses em que o **CONTRATADO** realizar as operações societárias de fusão, cisão ou incorporação, condicionada aos seguintes requisitos:

I. aquiescência prévia do **BNDES**, que analisará eventuais riscos ou prejuízos decorrentes de tal alteração contratual; e
II. manutenção de todas as condições contratuais e requisitos de habilitação originais.

Parágrafo Segundo
Caso ocorra a sucessão contratual admitida no Parágrafo anterior, o sucessor assumirá integralmente a posição do sucedido, passando a ser responsável pela execução do presente Contrato, fazendo, por conseguinte, jus ao recebimento dos créditos dele decorrentes.

Parágrafo Terceiro
É vedada a subcontratação para a execução do objeto deste Contrato.

CLÁUSULA DÉCIMA OITAVA – PENALIDADES
Em caso de inexecução total ou parcial do Contrato, inclusive de descumprimento de exigência expressamente formulada pelo **BNDES** ou de inobservância de qualquer obrigação legal, bem como em caso de mora, sem motivo justificado, o **CONTRATADO** ficará sujeito às seguintes penalidades:

I. advertência;

II. multa, de acordo com o Anexo I (Termo de Referência); e

III. suspensão temporária de participação em licitação e impedimento de contratar com o **BNDES**, por prazo não superior a 2 (dois) anos, apurado de acordo com a gravidade da infração.

Parágrafo Primeiro
As penalidades serão aplicadas observadas as normas do Regulamento de Licitações e Contratos do **SISTEMA BNDES**.

Parágrafo Segundo
Contra a decisão de aplicação de penalidade, o **CONTRATADO** poderá requerer a reconsideração para a decisão de advertência, ou interpor o recurso cabível para as demais penalidades, na forma e no prazo previstos no Regulamento de Licitações e Contratos do **SISTEMA BNDES**.

Parágrafo Terceiro
A imposição de penalidade prevista nesta Cláusula não impede a extinção do Contrato pelo **BNDES**, nos termos da legislação aplicável e da Cláusula de Extinção do Contrato.

Parágrafo Quarto
A multa poderá ser aplicada juntamente com as demais penalidades.

Parágrafo Quinto
A multa aplicada ao **CONTRATADO** e os prejuízos causados ao **BNDES** serão deduzidos de quaisquer créditos a ele devidos, assim como da garantia prestada, ressalvada a possibilidade de cobrança judicial da diferença eventualmente não coberta pelos mencionados créditos.

Parágrafo Sexto
No caso de atos lesivos à Administração Pública, nacional ou estrangeira, observar-se-ão os termos da Lei nº 12.846/2013.

Parágrafo Sétimo
A celebração de Termo de Ajustamento de Conduta prevista no Regulamento de Licitações e Contratos do Sistema BNDES não importa em renúncia às penalidades prevista neste Contrato e no Anexo I (Termo de Referência).

Parágrafo Oitavo
A sanção prevista no inciso III desta Cláusula também poderá ser aplicada às sociedades ou profissionais que:

I. tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II. tenham praticado atos ilícitos visando frustrar os objetivos da licitação;

III. demonstrem não possuir idoneidade para contratar com o **BNDES** em virtude de atos ilícitos praticados.

CLÁUSULA DÉCIMA NONA – ALTERAÇÕES CONTRATUAIS
O presente Contrato poderá ser alterado, por acordo entre as partes, nas hipóteses disciplinadas no art. 81 da Lei nº 13.303/2016, entre outras legal ou contratualmente previstas, observando-se que:

I. as alterações devem preservar o equilíbrio econômico-financeiro do Contrato; e

II. é vedada a modificação contratual que desnature o objeto da contratação ou afete as condições essenciais previstas no Termo de Referência (Anexo I deste Contrato).

Parágrafo Primeiro
Em atenção aos princípios que regem as relações contratuais, nas hipóteses em que for imprescindível a alteração deste Contrato para viabilizar sua plena execução, conforme demonstrado em processo administrativo, não caberá a recusa das partes à respectiva formalização, salvo em caso de justo motivo, devidamente comprovado pela parte que o alegar.

Parágrafo Segundo
A parte que, injustificadamente, se recusar a promover a alteração contratual indicada no Parágrafo anterior, deverá responder pelos danos eventualmente causados, sem prejuízo das demais consequências previstas neste Instrumento e na legislação vigente.

Parágrafo Terceiro
As alterações contratuais serão formalizadas mediante instrumento aditivo, ressalvadas as hipóteses legais que admitem a alteração por apostilamentos ajustes necessários à eventual correção de erros materiais ou à alteração de dados acessórios do Contrato e alterações de preços decorrentes decorrente de reajuste, repactuação ou revisão de preços causada por alterações na legislação tributária, que poderão ser celebrados por meio epistolar.

CLÁUSULA VIGÉSIMA – EXTINÇÃO DO CONTRATO
O presente Contrato poderá ser extinto de acordo com as hipóteses previstas na legislação, e ainda:

I. consensualmente, formalizada em autorização escrita e fundamentada do **BNDES**, mediante aviso prévio por escrito, com antecedência mínima de 90 (noventa) dias ou de prazo menor a ser negociado pelas partes à época da rescisão;

II. em razão do inadimplemento total ou parcial de qualquer de suas obrigações, cabendo à parte inocente notificar a outra por escrito, assinalando-lhe prazo razoável para o cumprimento das obrigações, quando o mesmo não for previamente fixado neste instrumento ou em seus anexos;

III. na ausência de liberação, por parte do **BNDES**, de área, local ou objeto necessário para a sua execução, nos prazos contratuais;

IV. em virtude da suspensão da execução do Contrato, por ordem escrita do **BNDES**, por prazo superior a 120 (cento e vinte) dias ou ainda por repetidas suspensões que totalizem o mesmo prazo;

V. quando for decretada a falência do **CONTRATADO**;

VI. caso o **CONTRATADO** perca uma das condições de habilitação exigidas quando da contratação;

VII. na hipótese de descumprimento do previsto na Cláusula de Cessão de Contrato ou de Crédito, Sucessão Contratual e Subcontratação;

VIII. caso o **CONTRATADO** seja declarada inidôneo pela União, por Estado ou pelo Distrito Federal;

IX. em função da suspensão do direito de o **CONTRATADO** licitar ou contratar com o **BNDES**;

X. na hipótese de caracterização de ato lesivo à Administração Pública, nos termos da Lei nº 12.846/2013, cometido pelo **CONTRATADO** no processo de contratação ou por ocasião da execução contratual;

XI. em razão da dissolução do **CONTRATADO**;

XII. quando da ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditivo da execução do Contrato;

XIII. por iniciativa do **BNDES**, a partir do 30º (trigésimo) mês de vigência, devendo ser formalizada pelo **BNDES** em autorização escrita e fundamentada, mediante aviso prévio por escrito, com antecedência mínima de 180 (cento e oitenta) dias ou de prazo menor a ser negociado pelas partes à época da rescisão.

Parágrafo Primeiro
Caracteriza inadimplemento das obrigações de pagamento pecuniário do presente Contrato, a mora superior a 90 (noventa) dias.

Parágrafo Segundo
Os casos de extinção contratual convencionados no *caput* desta Cláusula deverão ser precedidos

de notificação escrita à outra parte do Contrato, e de oportunidade de defesa, dispensada a necessidade de interpelação judicial.

CLÁUSULA VIGÉSIMA PRIMEIRA – DISPOSIÇÕES FINAIS

Este Contrato representa todo o acordo entre as partes com relação ao objeto nele previsto.

Parágrafo Primeiro

Integram o presente Contrato:
Anexo I - Termo de Referência do Pregão Eletrônico nº 007/2024 - BNDES
Anexo II - Proposta
Anexo III - Matriz de Risco
Anexo IV - Termo de Confidencialidade para Representante Legal
Anexo V - Minuta de Termo de Confidencialidade para Profissionais

Parágrafo Segundo

A omissão ou tolerância quanto à exigência do estrito cumprimento das obrigações contratuais ou ao exercício de prerrogativa decorrente deste Contrato não constituirá renúncia ou novação nem impedirá as partes de exercerem os seus direitos a qualquer tempo.

CLÁUSULA VIGÉSIMA SEGUNDA – FORO

É competente o foro da cidade do Rio de Janeiro para solucionar eventuais litígios decorrentes deste Contrato, afastado qualquer outro, por mais privilegiado que seja.

As partes consideram, para todos os efeitos, a data da última assinatura digital como a data de formalização jurídica deste instrumento.

As folhas deste Contrato foram revisadas por _____, advogado(a) do **BNDES**, por autorização do representante legal que o assina.

Rio de Janeiro, _____ de _____ de _____.

_____

BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL – BNDES

_____

CONTRATADO

PREGÃO ELETRÔNICO Nº 007/2024 – BNDES
ANEXO IV – MATRIZ DE RISCOS

Categoria do Risco	Descrição	Consequência	Medidas Mitigadoras	Alocação do Risco
Risco Atinente ao Tempo da Execução	Atraso na execução do objeto contratual por culpa da Contratada.	Período sem cobertura dos serviços, aplicação de penalidades e contingenciamento do suporte por equipe interna do BNDES.	Diligência da Contratada na execução contratual.	Contratada
	Fatos retardadores ou impeditivos da execução do Contrato próprios do risco ordinário da atividade empresarial ou da execução.	Período sem cobertura dos serviços, aplicação de penalidades e contingenciamento do suporte por equipe interna do BNDES.	Planejamento empresarial.	Contratada
	Atraso na execução do objeto contratual por culpa do BNDES.	Período sem cobertura de suporte e atualização de parte dos serviços da plataforma e contingenciamento do suporte por equipe interna do BNDES.	Cumprimento pelo BNDES das atividades necessárias a regular execução contratual.	BNDES
	Fatos retardadores ou impeditivos da execução do Contrato que não estejam na sua álea ordinária, tais como fatos do príncipe, caso fortuito ou de força maior, bem como o retardamento determinado pelo BNDES, que comprovadamente repercuta no preço contratado, observada a disciplina contratual.	Aumento do custo do serviço.	Revisão de preço.	BNDES.
Risco da Atividade Empresarial	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro da Contratada na avaliação da hipótese de incidência tributária.	Aumento ou diminuição do lucro da Contratada.	Planejamento tributário.	Contratada.
	Variação da taxa de câmbio.	Aumento ou diminuição do custo do produto e/ou do serviço.	Instrumentos financeiros de proteção cambial (hedge).	Contratada.

Categoria do Risco	Descrição	Consequência	Medidas Mitigadoras	Alocação do Risco
	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra.	Aumento do custo do produto e/ou do serviço.	Reajuste anual de preço.	BNDES
	Elevação dos custos operacionais definidos na linha anterior, quando superior ao índice de reajuste previsto na Cláusula de Equilíbrio Econômico Financeiro do Contrato.	Aumento do custo do produto e/ou do serviço.	Planejamento empresarial.	Contratada
Riscos Trabalhista e Previdenciário	Responsabilização do BNDES por verbas trabalhistas e previdenciárias dos profissionais da Contratada alocados na execução do objeto contratual.	Geração de custos trabalhistas e/ou previdenciários para o BNDES, além de eventuais honorários advocatícios, multas e verbas sucumbenciais.	Contratação como serviço sem mão-de-obra dedicada ao BNDES	Contratada
Risco Tributário e Fiscal (não tributário).	Responsabilização do BNDES por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa do BNDES.	Débito ou crédito tributário ou fiscal (não tributário).	Ressarcimento, pela Contratada, ou retenção de pagamento e compensação com valores a este devidos, da quantia despendida pelo BNDES.	Contratada
Risco Tributário e Fiscal	Majoração de alíquotas dos tributos incidentes sobre a prestação dos serviços objeto do contrato.	Aumento do valor total do contrato.	Reequilíbrio contratual.	BNDES

PREGÃO ELETRÔNICO Nº 007/2024 – BNDES
ANEXO V – MODELOS DE DECLARAÇÃO

MODELO A

DECLARAÇÃO DE INEXISTÊNCIA DE IMPEDIMENTOS DE PARTICIPAÇÃO E DE CONTRATAÇÃO

Ref.: Pregão Eletrônico nº 007/2024 - **BNDES**

_____, CNPJ nº ___, sediada em _____, por intermédio de seu Representante Legal, o(a) Sr(a). _____, inscrito no CPF sob o nº _____, DECLARA, sob as penas da lei, a inexistência de impedimentos normativos à contratação com o BNDES ou suas subsidiárias[3], declarando que:

I. em relação ao art. 38 da Lei n.º 13.303/2016:

a) não possui administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social que seja diretor ou empregado do BNDES ou de suas subsidiárias;

b) não está cumprindo penalidade de suspensão temporária de participação em licitação e impedimento de contratar com o BNDES ou com suas subsidiárias;

c) não foi declarada inidônea pela União, por Estado ou pelo Distrito Federal, enquanto perdurarem os efeitos da sanção;

d) não possui sócio ou administrador que seja sócio de outra empresa que está suspensa, impedida ou declarada inidônea;

e) não possui sócio ou administrador que tenha sido sócio ou administrador de outra empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

f) que não tem, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea; e

g) que não possui sócio que tenha terminado seu prazo de gestão ou rompido seu vínculo com o BNDES ou suas subsidiárias há menos de 6 (seis) meses.

II. não está proibido de licitar e contratar com a Administração Pública, bem como de receber incentivos, subsídios, subvenções, doações ou empréstimos de pessoas jurídicas de direito público ou de pessoas jurídicas controladas pelo Poder Público[4];

[3] BNDES Participações S/A – BNDESPAR e a Agência Especial de Financiamento Industrial – FINAME

[4] Este inciso alcança todas as sanções de impedimento de licitar e contratar previstas nos demais dispositivos legais, tais como as decorrentes da Lei nº 8.429/1992, da Lei nº 9.605/1998, da Lei nº 9.504/1997 e as decorrentes de práticas lesivas à Administração Pública nos termos da Lei nº 12.846/2013.

III. em relação à Política de Equidade de Gênero e Valorização da Diversidade do Sistema BNDES (Res. CA nº 08/2020 - BNDES)[5], inexiste decisão administrativa final sancionadora, exarada por autoridade ou órgão competente, em razão da prática de atos, pela sociedade ou por seus dirigentes, que importem em discriminação de raça ou gênero, exploração irregular, ilegal ou criminosa do trabalho infantil ou prática relacionada ao trabalho em condições análogas à escravidão, e/ou de sentença condenatória transitada em julgado, proferida em decorrência dos referidos atos, ou ainda, de outros que caracterizem assédio moral ou sexual, ou importem em crime contra o meio ambiente.;

IV. em relação à Política para Transações com Partes Relacionadas (Res. CA nº 15/2021 – BNDES):

a) não é controlada por Superintendente, Diretor ou membro de Órgão previsto no estatuto social das empresas do Sistema BNDES;

b) não é controlada por cônjuge, companheiro ou parentes, consanguíneos ou afins, até o 2º grau, de qualquer pessoa referida no inciso (i) acima;

V. não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, salvo na condição de aprendiz a partir dos quatorze anos;

VI. disporá, no momento da contratação, de todos os recursos humanos e operacionais necessários à execução do objeto contratado;

VII. se compromete a informar ao BNDES, a qualquer tempo, a alteração das condições declaradas acima;

VIII. está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la; e

IX. não designará, para a execução dos serviços ora contratados, profissionais que sejam cônjuge, companheiro(a) ou parente, em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, de empregado ou dirigente do Sistema BNDES.

Local, data.

Assinatura do representante legal.

[5] Disponível em *https://ri.bndes.gov.br/governanca-corporativa/estatutos-codigo-e-politicas*.

MODELO B

DECLARAÇÃO DE INFORMAÇÕES PARA FORNECIMENTO – DIF

Instruções para Preenchimento:

1) Antes de começar a preencher,favor ler a aba Instruções Gerais deste arquivo;
2) Preencher apenas os campos hachurados em azul. O restante da planilha está bloqueado;
3) Cada campo tem comentários para auxiliar o preenchimento. Passe o mouse para acessar os comentários;
4) Preencher uma DIF para cada unidade econômica do fornecedor (matriz e/ou filiais), que vierem a efetivamente fornecer o produto e/ou prestar o serviço. Nesse caso, os documentos de cobrança deverão ser emitidos por estas unidades econômicas; e
5) Preencher uma DIF para cada subcontratado do fornecedor que emitir documentos de cobrança contra o BNDES.

1) CONTRATANTE

Banco Nacional de Desenvolvimento Econômico e Social - BNDES — CNPJ: 33.657.248/0001-89 — Inscr. Mun.: 047.146-1
Endereço: Avenida República do Chile, 100, Centro, CEP 20031-917 — Rio de Janeiro - RJ

2) DADOS CADASTRAIS DO FORNECEDOR OU DO(S) SUBCONTRATADO(S)

☐ FORNECEDOR ☐ SUBCONTRATADO

Razão Social/Nome:

Endereço Completo:

DADOS*	PESSOA JURÍDICA				PESSOA FÍSICA
CNPJ/CPF					
NIT/PIS/PASEP					
Natureza Jurídica					
Entidade Sem Fins Lucrativos	☐	Sim	☐	Não	
Entidade Beneficente de Assistência Social	☐	Sim	☐	Não	
CÓDIGO CNAE(i) - Atividade Principal / Nº CBO(ii)					
CÓDIGO CNAE da Atividade do fornecimento:					
Inscrição Estadual					
Inscrição Municipal					
Código CFOP(iii)					
Classificação NCM(iv)					
Optante SIMPLES NACIONAL	☐	Optante	☐	Não optante	
Optante pelo SIMEI(v)	☐	Optante	☐	Não optante	

(i) CNAE - Classificação Nacional de Atividades Econômicas; (ii) CBO - Classificação Brasileira de Ocupações; (iii) CFOP - Código Fiscal de Operações e Prestações; (iv) NCM - Nomenclatura Comum do Mercosul; e (v) SIMEI - Sistema de recolhimento em valores fixos mensais dos tributos abrangidos pelo Simples Nacional, devidos pelo Microempreendedor Individual (MEI).

3) OBJETO DO FORNECIMENTO

☐ PRODUTO ☐ SERVIÇO ☐ PRODUTO E SERVIÇO

OBJETO:

4) CONDIÇÕES DO FORNECIMENTO

PRODUTO/SERVIÇO	VALOR BRUTO (R$)	MUNICÍPIO(S) DA ENTREGA E/OU PRESTAÇÃO
PRODUTO		
SERVIÇO		
TOTAL	-	

Valor Bruto é o valor referente ao escopo desta DIF, sem nenhuma dedução de tributos. Não considerar valores de fornecimento de outras unidades econômicas ou subcontratações.

☐ **Subcontratação** (para os casos permitidos na Lei 8.666/93) **Nº de subcontratações:** ☐

TIPO DE DOCUMENTO A SER ENCAMINHADO*:

NF ☐ NF-e ☐ NFS-e ☐ DANFE ☐ RPCI ☐ RECIBO ☐ OUTROS ☐ QUAIS? .....

* As siglas mencionadas neste campo têm o significado a seguir: (i) NF - Nota Fiscal; (ii) NF-e - Nota Fiscal Eletrônica; (iii) NFS-e - Nota Fiscal de Serviço Eletrônica; (iv) DANFE - Documento Auxiliar da Nota Fiscal Eletrônica; e (v) RPCI - Recibo de Pagamento a Contribuinte Individual (antigo RPA - Recibo de Pagamento a Autônomo).

5) INCIDÊNCIAS TRIBUTÁRIAS

Diretrizes básicas para preenchimento:

1) IRPJ, CSLL, PIS/PASEP e COFINS:

1.1) Observar o art. 34 da Lei nº 10.833/03, que trata da obrigação das empresas públicas (BNDES) em efetuar as retenções na fonte, a que se referem o art. 64 da Lei nº 9.430/96; e

1.2) Observar a IN RFB nº 1.234/12.

2) RETENÇÃO PREVIDENCIÁRIA (INSS) - aplicável aos casos de cessão de mão-de-obra ou empreitada:

2.1) Observar a IN RFB nº 971/09, em especial a partir do art. 112, bem como o art. 7º da Lei nº 12.546/11; e

2.2) Observar a CNAE da atividade principal, bem como a CNAE da atividade relacionada à prestação do serviço (CNAE principal ou secundário).

3) ISS:

3.1) Observar a Lei Complementar (LC) nº 116/03, em especial a regra geral contida no caput do art. 3º, que o ISS é devido "no município do estabelecimento do prestador do serviço";

3.2) Verificar se a categoria de serviço prestado se enquadra nas exceções previstas no art. 3º da LC nº 116/03, em que o ISS é devido no "local da prestação";

3.3) Consultar os regulamentos de ISS específicos de cada município do(s) local(is) da prestação do serviço, tendo em vista a previsão contida no art. 6º da LC nº 116/2003, especialmente o regulamento do município competente para a cobrança do ISS; e

3.4) Considerar os registros nos cadastros municipais de empresas prestadoras de outros municípios, se aplicável (verificar CEPOM/Rio de Janeiro).

4) SIMPLES NACIONAL, ENTIDADE SEM FINS LUCRATIVOS e ENTIDADE BENEFICENTE DE ASSISTÊNCIA SOCIAL:

4.1) Optante pelo Simples Nacional (salvo os serviços de construção civil, paisagismo, vigilância, limpeza ou conservação, e serviços advocatícios) ou Entidade Beneficente de Assistência Social **NÃO** estão sujeitos à retenção da Contribuição Previdenciária (INSS), (conforme art. 18, § 5º-C da LC 123/06 ou art. 149 da IN RFB nº 971/09, respectivamente); e

4.2) Optante pelo Simples Nacional, Entidade Sem Fins Lucrativos ou Entidade Beneficente de Assistência Social **NÃO** estão sujeitos à retenção dos Tributos Federais (IRPJ, CSLL, PIS/PASEP e COFINS), observado o art. 6º da IN RFB nº 1.234/12, devendo enviar a declaração prevista no Anexo II, III ou IV; conforme enquadramento. No caso de Entidade Beneficente de Assistência Social, que atue nas áreas da saúde, da educação e/ou da assistência social, será necessário adicionalmente enviar o Certificado de Entidade Beneficente de Assistência Social (CEBAS), conforme art. 6º, § 6º e 7º da IN RFB 1.234/12, alterada pela IN RFB 1.540/15. Nos termos do § 7º do art. da 6º da IN RFB nº 1.243/2012, não serão aceitos comprovantes de protocolos de requerimento de concessão ou renovação do CEBAS.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS DOS PRODUTOS A SEREM FORNECIDOS

Preencher os valores dos produtos/mercadorias faturados diretamente contra o BNDES

TRIBUTO	VALOR DO PRODUTO R$ (A)	BENEFÍCIO FISCAL MARQUE COM "X" (B)		BASE DE CÁLCULO R$ (C)	ALÍQUOTA % (D)	VALOR A SER RETIDO R$ E=(C x D)	BASE LEGAL DO BENEFÍCIO FISCAL (SE APLICÁVEL)
IRPJ	-	SIM	NÃO				
CSLL		SIM	NÃO		1,00%		
PIS/PASEP		SIM	NÃO		0,65%		
COFINS		SIM	NÃO		3,00%		
ICMS		SIM	NÃO				

Observação 1: O BNDES NÃO é contribuinte do ICMS, por isso, NÃO se aplicam alíquotas interestaduais.

Observação 2: Se o fornecimento implicar em produtos que estejam sujeitos a enquadramentos tributários distintos, preencha uma DIF para cada caso.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS DOS SERVIÇOS A SEREM PRESTADOS

Conferir o enquadramento do serviço na LC nº 116/03 (campos "COD LC 116/03" e "DESCRIÇÃO"), e informar a inscrição no Cadastro de Empresas Prestadoras de Outros Municípios - CEPOM/Rio de Janeiro, se aplicáveis:

CÓD LC 116/03	DESCRIÇÃO	CÓD CEPOM/RJ

Enquadrar o serviço como cessão de mão de obra / empreitada:

Marque com **"X"** as respostas ao lado das quatro perguntas a seguir, para determinação de existência de retenção previdenciária.

a) Os serviços, no todo ou em parte, podem ser enquadrados no Anexo I? (veja aba "Anexos I e II" deste arquivo)	Sim	Não
b) Os serviços, no todo ou em parte, podem ser enquadrados no Anexo II? (veja aba "Anexos I e II" deste arquivo)	Sim	Não
c) Os serviços serão prestados nas dependências do BNDES ou em local por ele estabelecido?	Sim	Não
d) Os serviços contratados são de necessidade contínua do BNDES?	Sim	Não

Se as respostas "a" e "c" forem SIM, haverá retenção previdenciária.

Se as respostas "b", "c" e "d" forem SIM, haverá retenção previdenciária.

Caso não sejam satisfeitas as combinações acima, não haverá retenção previdenciária.

De acordo com as respostas acima, haverá retenção previdenciária? (conforme IN RFB nº 971/2009)

Preencher com os valores referentes aos serviços faturados diretamente contra o BNDES

TRIBUTO	VALOR DO SERVIÇO R$ (A)	BENEFÍCIO FISCAL MARQUE COM "X" (B)		BASE DE CÁLCULO R$ (C)	ALÍQUOTA % (D)	VALOR A SER RETIDO R$ E=(C x D)	BASE LEGAL DO BENEFÍCIO FISCAL (SE APLICÁVEL)
IRPJ	-	SIM	NÃO				
CSLL		SIM	NÃO		1,00%		
PIS/PASEP		SIM	NÃO		0,65%		
COFINS		SIM	NÃO		3,00%		
ICMS		SIM	NÃO				
ISS		SIM	NÃO				
INSS		SIM	NÃO				

Observação 1: O BNDES NÃO é contribuinte do ICMS, NÃO se aplicando a alíquota interestadual.

Observação 2: Se o fornecimento implicar em serviços que estejam sujeitos a enquadramentos tributários distintos, preencha uma DIF para cada caso.

Declaro para os devidos fins que são verdadeiras todas as informações aqui prestadas ao contratante pelo que me responsabilizo civil e criminalmente, bem como que a apresentação desta declaração não dispensa a minha obrigação como fornecedor/subcontratado de apresentar outras declarações eventualmente exigidas pela legislação.

Nome: **CPF:** **Função na Empresa:**

Local e data: ..... , ___ de _____ de _____ .

Assinatura do representante legal do fornecedor /subcontratado

Contador: **CRC:**

Assinatura do contador do fornecedor / subcontratado

MINUTA A - TERMO DE CONFIDENCIALIDADE PARA REPRESENTANTE LEGAL

_____*(Identificação da empresa – CNPJ, Razão Social, etc)*_____, por intermédio de seu representante legal, _____*(identificação do representante legal – Nome e CPF)*_____, doravante designado simplesmente **RESPONSÁVEL**, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

Cláusula Primeira

O **RESPONSÁVEL** reconhece que, em razão da sua prestação de serviços às **EMPRESAS DO SISTEMA BNDES** – Contrato OCS nº _____/_____, celebrado em _____/_____/ , estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES**, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES** e do **RESPONSÁVEL**, sem a expressa e escrita autorização do representante legal signatário do Contrato ora referido.

Cláusula Segunda

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas ou confidenciais a que venha a ter acesso;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Documentos e informações utilizados na execução dos serviços do contrato OCS nº ___/_____.

Cláusula Terceira

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza confidencial de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal das **EMPRESAS DO SISTEMA BNDES**, signatário do Contrato OCS nº ___/_____, a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

Cláusula Quarta

O **RESPONSÁVEL** recolherá, ao término do Contrato OCS nº _____/_____, para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse seja de seus empregados, prepostos, prestadores de serviço seja de fornecedores, com vínculo empregatício ou eventual com o **RESPONSÁVEL**, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial, dado pessoal a que teve acesso enquanto contratado pelas **EMPRESAS DO SISTEMA BNDES**.

Parágrafo Único

O **RESPONSÁVEL** determinará a todos os seus empregados, prepostos e prestadores de serviço que estejam, direta ou indiretamente, envolvidos com a prestação de serviços objeto do Contrato OCS nº _____/_____, a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

Cláusula Quinta

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

Cláusula Sexta

O RESPONSÁVEL obriga-se a tratar os dados pessoais que tiver acesso em razão de seu relacionamento com as EMPRESAS DO SISTEMA BNDES unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD, observando a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver, por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

Cláusula Sétima

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação, bem como do **RESPONSÁVEL**, no que for cabível.

Cláusula Oitava

As obrigações a que alude este instrumento perdurarão inclusive após a cessação do vínculo contratual entre o **RESPONSÁVEL** e as **EMPRESAS DO SISTEMA BNDES** e abrangem as informações presentes e futuras.

[OBS.: A Cláusula abaixo deve ser incluída quando for possível delimitar os profissionais que irão prestar os serviços objeto do Contrato]

Cláusula Nona

O **RESPONSÁVEL** se compromete no âmbito do Contrato objeto do presente Termo, a apresentar às **EMPRESAS DO BNDES** declaração individual de adesão e aceitação das cláusulas do **Termo de Confidencialidade para Profissionais Terceirizados**, de cada integrante ou participante da equipe que prestar ou vier a prestar os serviços especificados no Contrato OCS nº _____/_____.

De Acordo,

Rio de Janeiro, ___ de _____ de ___.

_____

RESPONSÁVEL

Nome: _____ Cargo/Função: _____
CPF: _____ Telefone: _____ E-mail: _____
Documento de Identidade (número, data, emissor): _____

MINUTA B - TERMO DE CONFIDENCIALIDADE PARA PROFISSIONAIS

(identificação – Nome e CPF) _____, doravante designado simplesmente **RESPONSÁVEL**, compromete-se, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

Cláusula Primeira

O **RESPONSÁVEL** reconhece que, em razão da sua prestação de serviços às **EMPRESAS DO SISTEMA BNDES** – Contrato OCS nº _____/_____, celebrado em ____/____/_____, estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES**, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES** e do **RESPONSÁVEL**, sem a expressa e escrita autorização do representante legal signatário do Contrato ora referido.

Cláusula Segunda

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas ou confidenciais a que venha a ter acesso enquanto contratado por empresa que preste serviço às **EMPRESAS DO SISTEMA BNDES**;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Dados pessoais, especialmente de pessoa natural identificada ou identificável;

VI. Documentos e informações utilizados na execução dos serviços do contrato OCS nº ____/_____.

Cláusula Terceira

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham a ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza confidencial de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal das **EMPRESAS DO SISTEMA BNDES**, signatário do Contrato OCS nº __ /_____, a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

Cláusula Quarta

O **RESPONSÁVEL** recolherá, ao término do Contrato OCS nº ____/_____, para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade destas, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial e dados pessoais a que teve acesso enquanto contratado pelas **EMPRESAS DO SISTEMA BNDES**.

Parágrafo Único

O **RESPONSÁVEL** adotará todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

Cláusula Quinta

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

Cláusula Sexta

O **RESPONSÁVEL** obriga-se a tratar os dados pessoais a que tiver acesso em razão do Contrato OCS nº _____/_____, com as EMPRESAS DO SISTEMA BNDES unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD, observando a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver, por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de

obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, as EMPRESAS DO SISTEMA BNDES, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

Cláusula Sétima

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Cláusula Oitava

As obrigações a que alude este instrumento perdurarão inclusive após a cessação da prestação de serviços objeto do Contrato OCS nº _____/_____, e abrangem as informações presentes e futuras.

De Acordo,

Rio de Janeiro, ___ de _____ de ___.

Profissionais da Equipe:

_____

Nome: _____ Cargo/Função: _____
CPF: _____ Telefone: _____ E-mail: _____
Documento de Identidade (número, data, emissor): _____

PREGÃO ELETRÔNICO Nº 007/2024 – BNDES
ANEXO VII – MODELO DE DECLARAÇÃO DE ATENDIMENTO AOS REQUISITOS

Referência: *(número da Licitação)*

Data: __ /__ /202_

Empresa: *(nome da Licitante)*

Declaro, na qualidade de representante legal da empresa _____, que a proposta comercial referente ao pregão ____/_____ atende a todos os prazos e requisitos previstos nas Especificações Técnicas (ANEXO I) do Edital.

_____ (nome e assinatura) _____

Nome completo, CPF, telefone e e-mail