COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR
Setor Bancário Norte (SBN), Quadra 2, Bloco L, Lote 06, Edifício Capes, 2º subsolo - Bairro Asa Norte, Brasília/DF, CEP 70040-031
Telefone: (61) 2022 6715 - www.capes.gov.br

CONTRATO Nº 45/2022

PROCESSO Nº 23038.008732/2021-59

TERMO DE CONTRATO N.º 45/2022 QUE ENTRE SI CELEBRAM A FUNDAÇÃO COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR – CAPES E A EMPRESA JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA.

A Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, com sede no Setor Bancário Norte Quadra 02 Bloco "L" Lote 06, na cidade de Brasília/DF, inscrita no CNPJ sob o nº 00.889.834/0001-08, neste ato representada pela Presidente **Sra. Claudia Mansani Queda de Toledo**, nomeada pela Portaria nº 318, de 15 de abril de 2021, publicada no DOU de 15 de abril de 2021, portadora da matrícula funcional nº [redacted] nomeado pela Portaria Casa Civil nº 1.633 de 08 de agosto de 2016, publicada no DOU de 09 de agosto de 2016 , portador da matrícula funcional nº 1436888 , doravante denominada CONTRATANTE, e a empresa JAMC Consultoria e Representação de Software LTDA , inscrita no CNPJ/MF sob o n.º 24.425.034/0001-96, com sede na SRTVN Quadra 701, conjunto C, Ala B, Parte V, Nº 124, Asa Norte, CEP nº 70.719-903, em Brasília-DF, doravante designada CONTRATADA, neste ato representada pelo Sócio Diretor de Operações **Sr. José André Mendes Coimbra**, portador da Carteira de Identidade nº [redacted], expedida pela SSP/DF, e CPF nº [redacted] tendo em vista o que consta no Processo nº 23038.008732/2021-59 e em observância às disposições da Lei Complementar n.º 123/2006, nas Leis n.º 8.666/93, 10.520/2002, 8.078/90 e 9.784/99 e nos Decretos n.º 7.892/2013, 8.538/2015 e 10.024/2019, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº 058/2021 (Tribunal Superior do Trabalho), mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto deste contrato é a aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento, conforme especificado na tabela abaixo, nos termos e condições constantes neste contrato, seus anexos e no edital.

Item	Especificação	Unidade	Quantidade	Valor Unitário R$	Valor Total R$
1	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não	Usuários	1.200	1.735,50	2.082.600,00

	estruturados, abrangendo centro de dados e endpoint				
2	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.	Usuários	1.200	385,50	462.600,00
TOTAL					**2.545.200,00**

1.1.1. As especificações técnicas do objeto constam no Anexo I deste contrato.

1.1.2. Do regime de contratação: o objeto do presente instrumento será executado por empreitada por preço global, em conformidade com o disposto na Lei n.º 8.666/1993.

2. CLAUSULA SEGUNDA – DA VIGÊNCIA

2.1. O prazo de vigência deste contrato é de 12 (doze) meses, contados da data da sua assinatura, e poderá ser prorrogado mediante termo aditivo por iguais e sucessivos períodos até o limite de 60 (sessenta) meses, com fundamento no art. 57, inc. II, da Lei n.º 8.666/93.

2.1.1. A pelo menos cento e vinte dias do término da vigência deste instrumento, o Contratante expedirá comunicado à Contratada para que esta manifeste, dentro de três dias contados do recebimento da consulta, seu interesse na prorrogação do contrato.

2.1.2. Se positiva a resposta, o Contratante providenciará, no devido tempo, o respectivo termo aditivo.

2.1.3. A resposta da Contratada terá caráter irretratável, portanto ela não poderá, após se manifestar num ou noutro sentido, alegar arrependimento para reformular a sua decisão.

2.1.4. Eventual desistência da Contratada após a assinatura do termo aditivo de prorrogação ou mesmo após sua expressa manifestação nesse sentido merecerá do Contratante a devida aplicação de penalidade, nos termos do caput da cláusula doze deste contrato.

2.1.5. Para fins de prorrogação a Contratada deverá comprovar todas as condições de habilitação exigidas na licitação, bem como atualizar a declaração apresentada no momento da assinatura do contrato, a qual deverá ser novamente firmada por todos os sócios que compõem o quadro societário da empresa, a fim de resguardar este órgão quanto à prática de nepotismo vedada pela Resolução nº 7, de 18/10/2005, com as alterações introduzidas pela Resolução 229, de 22/06/2016.

3. CLÁUSULA TERCEIRA – DO VALOR

3.1. O valor total deste contrato é de **R$ 2.545.200,00 (dois milhões, quinhentos e quarenta e cinco mil e duzentos reais).**

3.1.1. Já estão incluídas no preço total todas as despesas de impostos, taxas, fretes e demais encargos indispensáveis ao perfeito cumprimento das obrigações decorrentes deste contrato.

4. CLÁUSULA QUARTA – DO REAJUSTE

4.1. Somente para os itens em que é permitida a prorrogação, os preços poderão ser reajustados, respeitada a periodicidade mínima de um ano a contar da data da proposta ou do orçamento a que ela se refere ou da data do último reajuste, limitada à variação do Índice de Preços ao Consumidor Amplo - IPCA, ou de outro índice que passe a substituí-lo, com base na seguinte fórmula:

$$R = \frac{I - Io}{Io} *, \text{ onde:}$$

a) para o primeiro reajuste:

R = reajuste procurado;

I = índice relativo ao mês de reajuste;

Io = índice relativo ao mês de apresentação da proposta;

P = preço atual dos serviços.

b) para os reajustes subsequentes:

R = reajuste procurado;

I = índice relativo ao mês do novo reajuste;

Io = índice relativo ao mês do último reajuste efetuado;

P = preço do serviço atualizado até o último reajuste efetuado.

4.1.1. Sob nenhuma hipótese ou alegação será concedido reajuste retroativo à data em que a Contratada legalmente faria jus se ela não fizer o respectivo pedido de reajuste dentro da vigência do contrato.

4.1.2. Na hipótese de sobrevirem fatos imprevisíveis ou impeditivos da execução do ajustado, poderá ser admitida a revisão do valor pactuado, objetivando manter o equilíbrio econômicofinanceiro inicial do contrato.

4.1.3. O valor e a data do reajuste serão informados mediante apostila.

5. CLÁUSULA QUINTA – DA DOTAÇÃO ORÇAMENTÁRIA

5.1. As despesas oriundas deste contrato correrão à conta dos recursos orçamentários consignados ao Contratante, Programa de Trabalho: 12.122.0032.2000.0053, elemento de despesa 33.90.40.06 (Itens 1 e 2), nota de empenho 2021NE005854, emitida em 15/12/2022.

6. CLÁUSULA SEXTA – DOS PRAZOS

6.1. A Contratada deverá cumprir, para início da execução do objeto deste contrato, os seguintes prazos:

I - Itens 01 e 02 – em até 5 (cinco) dias úteis após a assinatura do contrato;

II - Em até 15 dias corridos após a reunião de planejamento, deverá ser apresentado o plano de instalação.

III - A seu critério, o Contratante poderá suspender a execução de prazos associados à instalação e ao treinamento e restabelecê-los em momento oportuno.

IV - A Contratada deverá se atentar, ainda, ao cumprimento dos prazos constantes do anexo I deste contrato.

6.1.1. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

6.1.2. Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: CAPES - Divisão de Contratos - DCON, SBN Quadra 02, Bloco L, Lote 6 Asa Norte, 2º Subsolo, CEP: 70040031, Brasília/DF, fones: (061) 2022-6715, e-mail: dcon@capes.gov.br.

6.1.3. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

6.1.4. Em casos excepcionais, autorizados pelo Contratante, o documento comprobatório do alegado poderá acompanhar a execução do objeto.

7. CLÁUSULA SÉTIMA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

7.1. A execução do objeto deste contrato será fiscalizada por um servidor, ou comissão de servidores, designados pela Administração, doravante denominado Fiscalização, com autoridade para exercer toda e qualquer ação de orientação geral durante a execução contratual.

7.1.1. São atribuições da Fiscalização, entre outras:

I - acompanhar, fiscalizar e atestar a execução contratual, bem assim indicar as ocorrências verificadas;

II - solicitar à Contratada e a seus prepostos ou obter da Administração todas as providências tempestivas necessárias ao bom andamento do contrato e anexar aos autos cópia dos documentos que comprovem essas solicitações;

III - manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;

IV - notificar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto para que sejam adotadas as medidas corretivas necessárias;

V - propor a aplicação de penalidades à Contratada e encaminhar à Divisão de Contratos - DCON os documentos necessários à instrução de procedimentos para possível aplicação de sanções administrativas.

7.1.2. A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

8. CLÁUSULA OITAVA – DO RECEBIMENTO E DA ACEITAÇÃO DO OBJETO

8.1. O objeto do presente contrato será recebido das seguintes formas:

I - itens 01 e 02 – Provisoriamente, mediante termo circunstanciado, imediatamente depois de efetuada a entrega das licenças de uso, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após o termo de aceite provisório;

8.1.1. Os objetos entregues ou os serviços prestados em desconformidade com o especificado neste contrato, no instrumento convocatório ou o indicado na proposta serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será notificada e obrigada a substituí-los ou refazê-los a suas expensas, no prazo contratual estabelecido, sob pena de incorrer em atraso quanto ao prazo de execução.

8.1.2. A notificação referida na subcláusula anterior suspende os prazos de recebimento e de pagamento até que a irregularidade seja sanada.

8.1.3. Independentemente da aceitação, a Contratada garantirá a qualidade de cada produto fornecido e instalado e estará obrigada a repor aquele que apresentar defeito no prazo estabelecido pelo Contratante.

8.1.4. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos serviços prestados, nem a ético-profissional pela perfeita execução contratual, dentro dos limites estabelecidos pela lei.

9. CLÁUSULA NONA – DO PAGAMENTO

9.1. O pagamento será efetuado em parcela única, em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo, mediante atesto da nota fiscal pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

9.1.1. As notas fiscais e os documentos exigidos no edital para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenação-Geral de Segurança e Infraestrutura de Informática - CGSII, situada no SBN Quadra 02, Bloco L, Lote 6 Asa Norte, Sobreloja, CEP: 70040031, Brasília/DF. Telefone (61) 2022-6103 E-mail: cgsii@capes.gov.br.

9.1.2. Durante o período da pandemia do Coronavírus, os documentos indicados na subcláusula anterior deverão ser encaminhados exclusivamente ao e-mail cgsii@capes.gov.br.

9.1.3. A Nota Fiscal deverá corresponder ao objeto entregue e a Fiscalização, no caso de divergência, especialmente quando houver adimplemento parcial, deverá notificar a Contratada a substituí-la em até três dias úteis, com suspensão do prazo de pagamento.

9.1.4. No decorrer da execução contratual, poderá ser alterado o local da entrega da nota fiscal, mediante prévia notificação à Contratada.

9.1.5. A Contratada deverá entregar todos os produtos e prestar todos os serviços solicitados por meio da nota de empenho, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento total da obrigação.

9.1.6. A retenção dos tributos não será efetuada caso a Contratada apresente, no ato de assinatura deste contrato, declaração de que é regularmente inscrita no Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte - Simples Nacional, conforme exigido no inciso XI do art. 4º e modelo constante no anexo IV da Instrução Normativa RFB n.º 1.234, de 11 de janeiro de 2012.

9.1.7. O Contratante pagará à Contratada a atualização monetária sobre o valor devido entre a data do adimplemento das obrigações contratuais e a do efetivo pagamento, excluídos os períodos de carência para recebimento definitivo e liquidação das despesas, previstos neste contrato, e utilizará o índice publicado pela Fundação Getúlio Vargas que represente o menor valor acumulado no período, desde que a Contratada não tenha sido responsável, no todo ou em parte, pelo atraso no pagamento.

10. CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA

10.1. Na execução deste contrato, a Contratada se obriga a envidar todo o empenho necessário ao fiel e adequado cumprimento dos encargos que lhe são confiados e, ainda, a:

I - executar os serviços e entregar os produtos na forma e em prazo não superior ao máximo estipulado neste contrato;

a) os objetos deverão ser entregues na Coordenação-Geral de Segurança e Infraestrutura de Informática - CGSII, situada no SBN Quadra 02, Bloco L, Lote 6 Asa Norte, Sobreloja, CEP: 70040031, Brasília/DF. Telefone (61) 2022-6103 E-mail: cgsii@capes.gov.br.

b) por ocasião da entrega do objeto será requerido o fornecimento da documentação de suporte técnico e manutenção em garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente etc.).

II - reparar, corrigir, remover e substituir, a suas expensas, as partes do objeto deste contrato em que se verifiquem vícios, defeitos ou incorreções resultantes da execução dos serviços;

III - comunicar ao Contratante, por escrito, qualquer anormalidade referente à execução do objeto, bem como atender prontamente às suas observações e exigências e prestar os esclarecimentos solicitados;

IV - apresentar, no prazo de 15 dias a contar do início da vigência deste contrato, os Termos de Responsabilidade e Confidencialidade previstos no Anexo II;

V - atender prontamente as solicitações da fiscalização do contrato e da garantia, inerentes ao objeto, sem qualquer ônus adicional ao órgão Contratante.

VI - cumprir todos os requisitos descritos no contrato, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o Contratante.

VII - respeitar o sistema de segurança do Contratante e fornecer todas as informações por ele solicitadas, relativas ao cumprimento do objeto.

VIII - acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

IX - guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de

propriedade e uso exclusivo do Contratante, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros.

X - garantir a segurança das informações da CAPES e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido da CAPES no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

XI - utilizar padrões definidos pela Contratante (nomenclaturas, metodologias etc.).

XII - substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares da CAPES.

a) os profissionais disponibilizados pela Contratada para a prestação dos serviços deverão estar identificados com crachá de identificação dela, estando sujeitos às normas internas de segurança da CAPES, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.

b) os profissionais da Contratada deverão utilizar a conta que lhe for atribuída, de forma controlada e intransferível, mantendo secreta a sua respectiva senha, pois todas as ações efetuadas através desta, serão de responsabilidade do profissional da Contratada.

c) divulgar aos seus profissionais a Política de Segurança da Informação da CAPES e assegurar-se de sua observação e cumprimento no curso da prestação de serviços nesta Fundação. A Política de Segurança da Informação da CAPES está formalizada na Portaria nº 199, de 29 de Agosto de 2019 e pode ser consultada no endereço eletrônico: http://cad.capes.gov.br/ato-administrativo-detalhar?idAtoAdmElastic=2257#anchor

XIII - comunicar ao Contratante, no prazo máximo de dez dias úteis, eventuais mudanças de endereço, telefone e e-mail, juntando a documentação necessária a sua comprovação;

XIV - manter, durante todo o período de execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas;

XV - responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, os quais não têm nenhum vínculo empregatício com a CAPES;

XVI - responder, integralmente, por perdas e danos que vier a causar diretamente à CAPES ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

10.1.1. A Contratada não será responsável:

I - por qualquer perda ou dano resultante de caso fortuito ou de força maior;

II - por quaisquer obrigações, responsabilidades, trabalhos ou serviços não previstos neste contrato ou no edital.

10.1.2. O Contratante não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros, sejam fabricantes, representantes ou quaisquer outros.

11. CLÁUSULA DÉCIMA SEGUNDA - DAS OBRIGAÇÕES DO CONTRATANTE

11.1. O Contratante, durante a vigência deste contrato, compromete-se a:

I - proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitir o acesso dos funcionários da Contratada às dependências da CAPES, relacionadas à execução do objeto deste contrato;

II - promover os pagamentos nas condições e prazo estipulados; e

III - fornecer atestados de capacidade técnica, desde que atendidas as obrigações contratuais. Os requerimentos deverão ser protocolizados ou enviados por correspondência para a Coordenação-Geral de Segurança e Infraestrutura de Informática - CGSII, situada no SBN Quadra 02, Bloco L, Lote 6 Asa Norte, Sobreloja, CEP: 70040031, Brasília/DF. Telefone (61) 2022-6103 E-mail: cgsii@capes.gov.br.

12. CLÁUSULA DÉCIMA SEGUNDA – DAS PENALIDADES SOBRE A CONTRATADA

12.1. Fundamentado no artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 5 (cinco) anos, garantido o direito à ampla defesa, sem prejuízo das multas previstas no edital, neste contrato e das demais cominações legais, aquele que:

I - não entregar documentação exigida neste contrato;

II - apresentar documentação falsa;

III - causar o atraso na execução do objeto;

IV - não mantiver a proposta;

V - falhar ou fraudar na execução contratual;

VI - comportar-se de modo inidôneo;

VII - declarar informações falsas;

VIII - cometer fraude fiscal.

12.1.1. O atraso injustificado na execução contratual implicará multa correspondente a 1% (um por cento) por dia de atraso, calculada sobre o valor do objeto em atraso, até o limite de 30% (trinta por cento) do respectivo valor total.

12.1.2. Na hipótese mencionada na subcláusula anterior, o atraso injustificado por período superior a 30 (trinta) dias caracterizará o descumprimento total da obrigação, punível com a sanção prevista no caput desta cláusula, como também a inexecução total do contrato.

12.1.3. Para os itens 1 a 4, caso a conclusão do atendimento técnico em garantia ultrapasse o prazo descrito neste instrumento, será aplicada multa de 0,1% (um centésimo por cento) do valor do objeto faturado na nota fiscal entregue ao Contratante, por hora de atraso, para cada objeto em que houver atraso, até o limite de 10% (dez por cento) do valor do contrato.

12.1.4. Para os itens 5 a 23, caso a conclusão do atendimento técnico ultrapasse o prazo descrito neste instrumento, será aplicada multa de 0,5% (meio por cento) do valor do objeto faturado na nota fiscal entregue ao Contratante, por hora de atraso, para cada objeto em que houver atraso, até o limite de 30% (trinta por cento) do valor do contrato.

12.1.5. O atraso injustificado na entrega do plano de instalação sujeitará a aplicação de multa de 1% (um por cento), calculada sobre o valor do serviço de instalação, por dia corrido de atraso na entrega do plano além do prazo máximo definido, até o percentual máximo de 30% (trinta por cento) do referido valor do serviço de instalação.

12.1.6. O atraso injustificado na realização dos treinamentos sujeitará a aplicação de multa de 1% (um por cento), calculada sobre o valor do serviço de treinamento, por dia corrido de atraso além do prazo máximo definido, até o percentual máximo de 30% (trinta por cento) do referido valor do serviço de treinamento.

12.1.7. Poderão ser aplicadas subsidiariamente as sanções de advertência e declaração de inidoneidade previstas nos artigos 86 e 87 da Lei n.º 8.666/93, concomitantemente à sanção de multa.

12.1.8. Sanções pecuniárias aplicáveis à Contratada poderão ser substituídas pela penalidade de advertência, tendo em vista as circunstâncias da execução contratual, garantida a prévia defesa, na forma da lei.

13. CLÁUSULA DÉCIMA TERCEIRA – DAS CONDIÇÕES DE HABILITAÇÃO DA CONTRATADA

13.1. A Contratada declara, no ato de celebração deste contrato, estar plenamente habilitada à assunção dos encargos contratuais e assume o compromisso de manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação.

14. CLÁUSULA DÉCIMA QUARTA – DA PUBLICAÇÃO

14.1. A publicação resumida deste contrato na Imprensa Oficial, que é condição indispensável para sua eficácia, será providenciada pelo Contratante, nos termos do parágrafo único do artigo 61 da Lei n.º 8.666/93.

15. CLÁUSULA DÉCIMA QUINTA – DAS ALTERAÇÕES DO CONTRATO

15.1. Compete a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei n.º 8.666/93 e em outras disposições legais pertinentes, realizar, via termo aditivo, as alterações contratuais que julgarem convenientes.

16. CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO

16.1. Constituem motivos incondicionais para rescisão do contrato as situações previstas nos artigos 77 e 78, na forma do artigo 79, inclusive com as consequências do artigo 80, da Lei n.º 8.666/93.

17. CLÁUSULA DÉCIMA SÉTIMA – DA UTILIZAÇÃO DO NOME DO CONTRATANTE

17.1. A Contratada não poderá, salvo em curriculum vitae, utilizar o nome do Contratante ou sua qualidade de Contratada em quaisquer atividades de divulgação profissional como, por exemplo, em cartões de visita, anúncios diversos, impressos etc., sob pena de imediata rescisão deste contrato.

Subcláusula única. A Contratada não poderá, também, pronunciar-se em nome do Contratante à imprensa em geral sobre quaisquer assuntos relativos às atividades deste, bem como a sua atividade profissional, sob pena de imediata rescisão contratual e sem prejuízo das demais cominações cabíveis.

18. CLÁUSULA DÉCIMA OITAVA – DA PROTEÇÃO DE DADOS

18.1. As partes envolvidas deverão observar as disposições da Lei 13.709, de 14/08/2018, Lei Geral de Proteção de Dados, quanto ao tratamento dos dados pessoais que lhes forem confiados, em especial quanto à finalidade e boa-fé na utilização de informações pessoais para consecução dos fins a que se propõe o presente contrato.

18.1.1. O Contratante figura na qualidade de Controlador dos dados quando fornecidos à Contratada para tratamento, sendo esta enquadrada como Operador dos dados. A Contratada será Controlador dos dados com relação a seus próprios dados e suas atividades de tratamento.

18.1.2. As partes estão obrigadas a guardar o mais completo sigilo por si, por seus empregados ou prepostos, nos termos da Lei Complementar nº 105, de 10 de janeiro de 2001 e da Lei Geral de Proteção de Dados (LGPD), cujos teores declaram ser de seu inteiro conhecimento, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma ou modo venham tomar conhecimento ou ter acesso, em razão deste contrato, ficando, na forma da lei, responsáveis pelas consequências da sua divulgação indevida e/ou descuidada ou de sua incorreta utilização, sem prejuízo das penalidades aplicáveis nos termos da lei.

18.1.3. Em caso de necessidade de coleta de dados pessoais indispensáveis à própria prestação do serviço, esta será realizada mediante prévia aprovação do Contratante, responsabilizando-se a Contratada por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins.

I - eventualmente, as partes podem ajustar que o Contratante será responsável por obter o consentimento dos titulares, observadas as demais condicionantes desta subcláusula.

18.1.4. A Contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula contratual, inclusive no tocante à Política de Privacidade da CAPES, cujos

princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata a presente cláusula.

18.1.5. Os dados pessoais tratados e operados serão eliminados após o término deste contrato, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

18.1.6. O Encarregado indicado pela Contratada manterá contato formal com o Encarregado pelo contrato indicado pelo Contratante, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, para que este possa adotar as providências devidas, na hipótese de questionamento das autoridades competentes.

18.1.7. Os casos omissos em relação ao tratamento dos dados pessoais que forem confiados à Contratada, e não puderem ser resolvidos com amparo na LGPD, deverão ser submetidos à Fiscalização para que decida previamente sobre a questão.

19. CLÁUSULA DÉCIMA NONA – DOS CASOS FORTUITOS, DE FORÇA MAIOR OU OMISSOS

19.1. Tal como prescrito na lei, o Contratante e a Contratada não serão responsabilizados por fatos comprovadamente decorrentes de casos fortuitos ou de força maior, ocorrências eventuais cuja solução se buscará mediante acordo entre as partes.

20. CLÁUSULA VIGÉSIMA – DAS DISPOSIÇÕES FINAIS

20.1. A Administração do Contratante analisará, julgará e decidirá, em cada caso, as questões alusivas a incidentes que se fundamentem em motivos de caso fortuito ou de força maior.

20.1.1. Para os casos previstos no caput desta cláusula, o Contratante poderá atribuir a uma comissão, por este designada, a responsabilidade de apurar os atos e fatos comissivos ou omissivos que se fundamentem naqueles motivos.

20.1.2. Os agentes públicos responderão, na forma da lei, por prejuízos que, em decorrência de ação ou omissão dolosa ou culposa, causarem à Administração no exercício de atividades específicas do cumprimento deste contrato, inclusive nas análises ou autorizações excepcionais constantes nestas disposições finais.

20.1.3. As exceções aqui referenciadas serão sempre tratadas com máxima cautela, zelo profissional, senso de responsabilidade e ponderação, para que ato de mera e excepcional concessão do Contratante, cujo objetivo final é o de atender tão-somente ao interesse público, não seja interpretado como regra contratual.

20.1.4. Para assegurar rápida solução às questões geradas em face da perfeita execução deste contrato, a Contratada fica desde já compelida a avisar, por escrito e de imediato, qualquer alteração em seu endereço ou telefone.

20.1.5. No curso do contrato, é admitida a fusão, cisão ou incorporação da empresa, bem assim sua alteração social, modificação da finalidade ou da estrutura, desde que não prejudique a execução do contrato, cabendo à Administração decidir pelo prosseguimento ou rescisão do contrato.

20.1.6. Quaisquer tolerâncias entre as partes não importarão em novação de qualquer uma das cláusulas ou condições estatuídas neste contrato, as quais permanecerão íntegras.

20.1.7. Em consonância com a Resolução 229, de 22 de junho de 2016, do Conselho Nacional da Justiça, é vedada a contratação de empresas que tenha em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores

ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação.

I - A vedação constante nesta subcláusula se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

21. CLÁUSULA VIGÉSIMA - DO FORO

21.1. Fica eleito o foro da cidade de Brasília, DF, como competente para dirimir quaisquer questões oriundas deste contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

Brasília/DF.

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES

Claudia Mansani Queda de Toledo

Presidente

JAMC Consultoria e Representação de Software LTDA

José André Mendes Coimbra

Sócio Diretor de Operações

TESTEMUNHAS:

1 -

2 -

ANEXO I

DOS REQUISITOS TÉCNICOS E FUNCIONAIS

3.6.1 Grupo 01, Item 01 - Licença de uso de software e garantia para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.

3.6.2 Considerações Gerais

3.6.2.1 Os produtos de softwares que irão compor a solução poderão ser licenciados no modelo de direito de uso, desde que:

3.6.2.1.1 não perca suas funcionalidades quando da expiração da licença;

3.6.2.1.2 o direito de uso da licença e a garantia deverão ser de, no mínimo, 12 meses.

3.6.2.2 Caso a licença ofertada seja perpétua, a garantia deverá ser de, no mínimo, 12 meses.

3.6.2.3 A solução ofertada poderá ser composta por mais de um software, desde que o conjunto atenda a todos os requisitos Técnicos e Funcionais;

3.6.2.4 A solução deverá contemplar todas as licenças necessárias para o atendimento de todos os requisitos exigidos nesta especificação técnica.

3.6.2.5 Ainda que a solução seja composta por mais de um produto de software, os consoles de administração deverão compartilhar as seguintes características:

3.6.2.5.1 Permitir autenticação de usuários por meio de senha integrada ao Microsoft Active Directory, AD, ou a outros serviços de diretórios que sejam compatíveis com o protocolo *Lightweight Directory Access Protocol* em sua versão 3 ou superior, LDAP v3, e sua versão segura, LDAPS;

3.6.2.5.2 O console de administração deve permitir a configuração de diversos perfis com permissões e restrições de acesso dos usuários às funcionalidades da solução, de forma a segregar o acesso de analistas, equipe de suporte e usuários finais;

3.6.2.5.3Deverá permitir que os perfis de permissões e restrições de acesso sejam determinados por grupos na estrutura do AD e LDAP.

3.6.2.6 A solução deverá ser instalada nos sistemas operacionais Windows Server em sua versão 2012 R2 ou superior ou Enterprise Linux, em suas versões Red Hat 7 ou superior, CentOS 7 ou superior ou, Oracle Linux 7 ou superior.

3.6.2.7 A solução poderá utilizar a infraestrutura de banco de dados da CONTRATANTE caso seja compatível com Oracle em sua versão 11.2.0.4 e superiores, executando em RAC, ou PostgreSQL em sua versão 11 e superiores.

3.6.2.8 Caso a solução não esteja em acordo com os requisitos de banco disponibilizados pela CONTRATADA, caberá a CONTRATADA fornecer as licenças necessárias para o banco de dados utilizado e garantir o seu funcionamento por toda vigência da garantia e direito de uso dos softwares.

3.6.2.9 Caso seja necessária instalação de agentes nos ativos monitorados, o processo de instalação não poderá gerar indisponibilidade.

3.6.2.10 A solução deve permitir o acesso a, no mínimo, 5 anos de dados de auditoria capturados e armazenados.

3.6.2.11 A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes e deve ser compatível com o ambiente de virtualização VMware vSphere no mínimo nas versões 6.4, e 7.0 e Red Hat KVM 2.12.

3.6.2.12 A solução deverá possuir escalabilidade suficiente para atender a quantidade de usuários descrito em contrato, sem perda de desempenho e sem acréscimo de licenciamento.

3.6.2.13 A solução deverá ser capaz de auditar um volume de, pelo menos 270TB de dados.

3.6.2.14 Os softwares que compõem a solução deverão ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação, como a ISO/IEC 27.001 ou similares para integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade de as informações serem utilizadas para investigações e perícia.

3.6.2.15 A solução deve ser capaz de auditar, controlar, monitorar e gerenciar, no mínimo, 35.000 objetos de controladores de domínio usuários sem comprometer o desempenho da solução.

3.6.2.16 A solução ofertada deve oferecer, com rotinas automatizadas, relatórios agendados e sob demanda, em diversos formatos de arquivos, exportados no momento da geração, ou enviados por e-mail, ou armazenados em um compartilhamento de arquivos através de agendamentos customizáveis.

3.6.2.17 A documentação relativa às especificações técnicas da solução deverá ser fornecida preferencialmente em português. Caso não exista em português, poderá ser apresentada em língua inglesa. Não há outra possibilidade de língua aceita.

3.6.2.18 A solução deve permitir o acesso de, pelo menos, 50 colaboradores a todas as suas funcionalidades administrativas. Para funcionalidades que são disponibilizadas a todos os usuários da CONTRATANTE, a solução deve permitir o acesso de todos os usuários contratados.

3.6.2.19 A solução deve possuir interface nos idiomas português ou inglês.

3.6.3 Das funcionalidades relacionadas à base de autenticação de usuários e servidores de arquivos.

3.6.3.1 A solução ofertada deve possuir as seguintes funcionalidades relacionadas a auditoria e monitoramento de servidores de arquivos:

3.6.3.1.1 Auditar acesso, modificação e remoção de pastas e arquivos em servidores de arquivos;

3.6.3.1.2 Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;

3.6.3.1.3 Gerar alerta com base nas informações auditadas;

3.6.3.1.4 Automatizar tarefas repetitivas, comum ou complexas;

3.6.3.1.5 Monitorar e analisar comportamentos suspeitos de usuários.

3.6.3.2 Referente a auditoria no serviço de diretório (AD ou OpenLDAP), a solução deve:

3.6.3.2.1 Auditar ações sobre objetos;

3.6.3.2.2 Executar ações proativas com base na auditoria, inclusive

para múltiplos objetos;

3.6.3.2.3 Gerar alerta com base nas informações auditadas;

3.6.3.2.4 Automatizar tarefas repetitivas, comum ou complexas;

3.6.3.2.5 Monitorar e analisar comportamentos suspeitos de usuários.

3.6.3.3 Deverá realizar auditoria, no mínimo, nos seguintes serviços de diretório:

3.6.3.3.1 Microsoft *Active Directory* (AD) na versão 2012 R2 em diante, ou;

3.6.3.3.2 OpenLDAP na versão 2.4 em diante.

3.6.3.4 A CONTRATANTE fará a opção entre auditoria dos seguintes servidores de arquivos:

3.6.3.4.1 Microsoft Windows Server na versão 2012 R2 em diante, ou;

3.6.3.4.2 Samba em sua versão 3 ou superior implementado em Linux baseados em Red Hat (Red Hat Linux, CentOS e Oracle Linux).

3.6.3.5 A solução deverá suportar o monitoramento do NAS DELL/EMC ISILON com OneFS na versão 8 em diante. Para esse item, o software que entregará essa funcionalidade deverá constar na matriz de compatibilidade do fabricante DELL/EMC.

3.6.3.6 A solução deverá apresentar em sua interface todos os usuários e grupos de segurança dos diferentes domínios monitorados, assim como os usuários e grupos de segurança locais de cada servidor ou plataforma monitorada.

3.6.3.7 A solução deverá permitir a busca por uma pasta nos servidores monitorados e apresentar todos os usuários e grupos de segurança que têm permissões e quais permissões esses objetos têm na pasta.

3.6.3.8 A solução deverá consolidar as permissões NTFS e *Share* de cada pasta e demonstrar a permissão efetiva dos usuários e grupos.

3.6.3.9 A solução deverá utilizar os eventos coletados pela auditoria para realizar a análise comportamental automática dos usuários de maneira a fazer recomendações de revogação de acesso aos dados não estruturados dos servidores monitorados.

3.6.3.10 Além da visibilidade de permissões, usuários e grupos de segurança, a solução deverá permitir que os administradores realizem alterações de permissionamento dos usuários e grupos de segurança nas pastas e diretórios dos servidores monitorados através da interface gráfica da solução.

3.6.3.11 A solução deverá permitir a visualização das alterações e o histórico das alterações de usuários, grupos e permissões realizadas através da

console. Deverá oferecer ainda a possibilidade de restaurar alterações realizadas.

3.6.3.12 A solução deverá, em sua interface gráfica, apresentar todos os logs de auditoria de acessos a diretórios, pastas e arquivos dos servidores monitorados, e acessos aos objetos do AD/LDAP organizados e agrupados por recurso monitorado:

3.6.3.12.1 Pasta ou diretório: demonstrar todos os eventos para a pasta,

subpastas e arquivos;

3.6.3.12.2 Unidade organizacional: demonstrar os eventos ocorridos em determinada OU;

3.6.3.12.3 Usuário ou grupo de segurança: demonstrar todos os eventos gerados ou sofridos por determinado usuário ou grupo.

3.6.3.13 Os eventos de auditoria coletados pela solução deverão conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto acessado, caminho dos arquivos, pastas e objetos, identificação do domínio, arquivo, pasta ou objeto impactado e nome do usuário que realizou a ação.

3.6.3.14 As consultas aos logs através da console da solução poderão ser customizadas pela aplicação de filtros, de forma que seja simples e rápida a obtenção de dados necessários para auditoria sobre os arquivos, pastas, usuários e grupos de segurança dos servidores monitorados sem a necessidade de customização através de linguagem de programação.

3.6.3.15 Todos os eventos dos diferentes servidores monitorados deverão ser apresentados na mesma console gráfica da solução onde também deverão ser apresentadas as informações de permissionamento desses mesmos servidores monitorados.

3.6.3.16 A solução deverá fornecer resumo gráfico das atividades auditadas, incluindo, no mínimo:

3.6.3.16.1 Quantidade de eventos por dia;

3.6.3.16.2 Visualização dos usuários mais e menos ativos nos servidores monitorados;

3.6.3.16.3 Visualização dos diretórios mais e menos acessados nos servidores monitorados;

3.6.3.16.4 Visualização dos diretórios e pastas acessadas por um usuário ou grupo de segurança.

3.6.3.17 A solução deverá indicar graficamente ou por relatório usuários ativos e inativos, usuários habilitados e desabilitados no serviço de diretório.

3.6.3.18 A solução deverá suportar a auditoria dos eventos do serviço de diretório, tais como:

3.6.3.18.1 Criação e deleção de todos os objetos;

3.6.3.18.2 Alteração de membros de grupos;

3.6.3.18.3 Alteração nas propriedades dos objetos do serviço de diretório;

3.6.3.18.4 Requisições de acesso;

3.6.3.18.5 Autenticação de conta;

3.6.3.18.6 Reconfiguração de senhas;

3.6.3.18.7 Bloqueio e desbloqueio de conta;

3.6.3.18.8 Criação e deleção de conta;

3.6.3.18.9 Habilitação e desativação de conta;

3.6.3.18.10 Eventos de permissão adicionada ou removida de objeto;

3.6.3.18.11 Proprietário alterado;

3.6.3.18.12 Modificação de configuração de GPOs;

3.6.3.18.13 Criação de link de GPO;

3.6.3.18.14 Deleção de link de GPO;

3.6.3.18.15 Modificação de link de GPO.

3.6.3.19 A solução deverá permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada.

3.6.3.20 A solução deverá permitir que os alertas sejam enviados por e-mail, syslog e SNMP.

3.6.3.21 A solução deverá permitir a configuração e execução de ações pré- configuradas ou através de scripts a partir de qualquer alerta gerado.

3.6.3.22 A solução deverá possuir regras de alertas pré-configurados pelo fornecedor atualizadas frequentemente de eventos suspeitos tais como:

3.6.3.22.1 Atividades suspeitas em arquivos e pastas;

3.6.3.22.2 Grupos de segurança, GPO's e outros objetos do serviço de diretório modificados ou removidos;

3.6.3.22.3 Detecção de ferramentas de intrusão ou malwares;

3.6.3.22.4 Acesso suspeitos a dados sensíveis;

3.6.3.22.5 Escalações de privilégios;

3.6.3.22.6 Modificação de permissões;

3.6.3.22.7 Inclusão e exclusão de grupos e usuários no serviço de diretório;

3.6.3.22.8 Acessos negados;

3.6.3.22.9 Ataques de sequestro de dados (*ransomware*).

3.6.3.23 A solução deverá aprender o comportamento padrão dos recursos monitorados e alertar em tempo real quando houver anomalias nestes comportamentos.

3.6.3.24 A solução deverá ser capaz de identificar desvios de comportamentos quantitativos e desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados por um recurso, assim como identificar eventos suspeitos que tenham ocorrido nas plataformas monitoradas.

3.6.3.25 Através da análise comportamental, solução deverá realizar a descoberta automática de contas privilegiadas como usuários administrativos e contas de serviço.

3.6.3.26 A solução deve entregar painel web que permita análise dos comportamentos e eventos suspeitos listados.

3.6.3.27 A solução deverá apresentar informações como:

3.6.3.27.1 Quantidade de alertas e suas severidades em determinado período;

3.6.3.27.2 Usuários que geraram comportamentos suspeitos;

3.6.3.27.3 Tipos de alertas mais detectados;

3.6.3.27.4 Máquinas mais utilizadas para as ações suspeitas;

3.6.3.27.5 Servidores e pastas que mais sofrem ações suspeitas.

3.6.3.28 A solução deverá apresentar página com todos os alertas de comportamentos suspeitos gerados pelos usuários, permitindo que seja identificado o cenário do possível ataque.

3.6.3.29 No painel, a partir de um alerta selecionado, a solução deverá exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos

deve ser personalizável podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.

3.6.3.30 A solução deverá fazer análise prévia dos alertas e correlacionar com outras informações e eventos do usuário alertado, dispositivo usado no momento do alerta, horário do evento.

3.6.3.31 O painel deve possuir página com os principais indicadores de performance dos servidores e recursos monitorados (Servidores de Diretório e de Sistemas de Arquivos) com informações essenciais para a gestão e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas de no mínimo:

3.6.3.31.1 Quantidade total de usuários;

3.6.3.31.2 Quantidade total de grupos de segurança;

3.6.3.31.3 Quantidade de usuários inativos;

3.6.3.31.4 Quantidade de usuários desabilitados;

3.6.3.31.5 Quantidade de usuários com senhas que não expiram;

3.6.3.31.6 Quantidade de usuários com recomendação de revogação de permissão excessiva feita pela auditoria;

3.6.3.31.7 Quantidade de arquivos;

3.6.3.31.8 Quantidade de pastas;

3.6.3.31.9 Quantidade de arquivos sensíveis;

3.6.3.31.10 Quantidade de dados parados;

3.6.3.31.11 Quantidade de dados superexpostos.

3.6.3.32 A solução deverá fornecer ao menos os seguintes relatórios com detalhamento dos eventos (data e hora, metadados do usuário que realizou a ação e metadados do objeto se sofreu a ação):

3.6.3.32.1 Todos os acessos dos usuários aos arquivos e pastas;

3.6.3.32.2 Todas as modificações de objetos do serviço de diretório;

3.6.3.32.3 Todas as modificações de permissionamento de objetos dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de domínio;

3.6.3.32.4 Alterações em grupos de segurança dos domínios monitorados;

3.6.3.32.5 Histórico de membros de grupos de segurança;

3.6.3.32.6 Estatísticas de autenticação e falha de autenticação;

3.6.3.32.7 Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental;

3.6.3.32.8 Informações sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs dos domínios monitorados;

3.6.3.32.9 Todas as pastas que um usuário tem permissão;

3.6.3.32.10 Todos os usuários que têm permissões em uma pasta;

3.6.3.32.11 Todas as pastas do servidor que tenham permissão direta aplicada a usuários;

3.6.3.32.12 Todas as pastas superexpostas;

3.6.3.32.13 Dados inativos ou sem utilização;

3.6.3.32.14 Histórico de permissões nas pastas e diretórios monitorados.

3.6.3.33 A solução deverá permitir que, a partir da console, os administradores façam alterações de permissionamento das pastas dos repositórios monitorados.

3.6.3.34 A solução deverá fornecer funcionalidade de ajuste aos diretórios com herança quebrada de permissões.

3.6.3.35 A interface gráfica da solução deverá permitir a busca por um usuário ou grupo de segurança e deverá apresentar suas permissões nas pastas dos servidores monitorados de forma integrada. As informações apresentadas devem incluir:

3.6.3.35.1 Identificação de herança de permissão ativada/desativada;

3.6.3.35.2 Indicação de existência de compartilhamento;

3.6.3.35.3 A fonte da permissão, ou seja, de que grupo o usuário está herdando a permissão.

3.6.3.36 A console de gerenciamento do módulo de classificação e identificação de informação sensível deverá ser totalmente integrada à console de acesso às funcionalidades de permissionamento, visualização de logs a fim de fornecer maiores detalhes sobre as informações armazenadas no ambiente monitorado.

3.6.3.37 A solução deverá inspecionar o conteúdo dos arquivos em escopo em busca de palavras, termos, expressões regulares, valores, e identificar informações sensíveis para o negócio.

3.6.3.38 A solução deverá possuir regras de identificação e classificação de conteúdos sensíveis pré-definidas pelo fornecedor que possem ser utilizadas ou não;

3.6.3.39 A solução deverá permitir a criação de novas regras de identificação e classificação de conteúdos sensíveis de forma gráfica através de sua console com a adição de filtros, sem a necessidade de programação;

3.6.3.40 A solução deverá exibir na mesma interface gráfica as informações sobre os permissionamentos, ACL's, quantidade de informações sensíveis e qual tipo de informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos.

3.6.3.41 A solução deverá gerar, em forma de relatórios, dados sobre a classificação das informações.

3.6.3.42 A solução deverá permitir a inclusão de filtros relativos à classificação dos dados nas pesquisas dos logs.

3.6.3.43 A solução deverá permitir a inclusão de filtros relativos à classificação dos dados nos relatórios de acesso.

3.6.3.44 A solução deverá demonstrar, diretamente na console, os dados descobertos dentro do arquivo marcado como sensível.

3.6.3.45 A solução deverá integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.

3.6.3.46 A ferramenta deverá permitir integração com ferramentas de DLP (*Data Loss Prevention*) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução.

3.6.3.47 A solução deverá permitir a definição de agendamento da classificação com hora de início e fim, frequência em que a busca ocorrerá e a data em que deve parar, para que não haja impacto no ambiente.

3.6.3.48 A solução deverá permitir a priorização da busca por arquivos sensíveis para otimização da classificação. Pois desta forma, serão encontrados primeiro os arquivos nos locais mais relevantes.

3.6.4 Das funcionalidades relacionadas ao monitoramento e auditoria dos *endpoints*.

3.6.4.1 A solução deve prover detecção automatizada dos incidentes de segurança fornecendo informações detalhadas sobre o incidente ou vulnerabilidade para pronta ação de contenção e resposta, disponibilizando a informação em seus níveis de criticidade tanto no dashboard em tempo real, quanto em seu histórico por meio de relatórios.

3.6.4.2 Todas as funcionalidades referentes à detecção incidentes de segurança e vulnerabilidades visando a contenção de tais ameaças devem ser passíveis de automatização.

3.6.4.3 Realizar análise comportamental de softwares instalados nos *endpoints*.

3.6.4.4 Monitoramento on-line de todas as atividades de usuários, processos, arquivos e acessos à rede.

3.6.4.5 Os agentes a serem instalados nos *endpoints* deverão ser compatíveis, no mínimo, com os seguintes sistemas Operacionais:

3.6.4.5.1 Windows 10 32bits e 64 bits;

3.6.4.5.2 Windows 11 32bits e 64 bits;

3.6.4.5.3 Windows Server em suas versões 2012 R2, 2016 e 2019, 32 bits e 64 bits.

3.6.4.6 Os recursos de distribuição e instalação dos agentes deverão realizar:

3.6.4.6.1 Descoberta automática dos *endpoints* que não possuem o agente instalado;

3.6.4.6.2 Descoberta automática e evidenciação dos agentes que eventualmente tenham sido paralisados propositadamente;

3.6.4.6.3 Instalação remota via Group Policy (GPO), Web e console de gerenciamento.

3.6.4.7 A solução deverá possuir pacote único para cada sistema operacional suportado.

3.6.4.8 A instalação do agente em *endpoints* Windows deve ser realizada e gerenciada pela própria solução, por ferramenta da CONTRATANTE, ou manualmente, por usuário autorizado, de forma remota e autônoma, oculta, sem interferência do usuário final e sem a necessidade de reiniciar a máquina.

3.6.4.9 Os agentes não poderão consumir recursos substanciais do *endpoint* ou interferir em seus itens de configuração (memória, processamento e espaço em disco local e tráfego de rede), não podendo ultrapassar 2% (dois por cento) dos recursos totais de cada item, aferidos individualmente.

3.6.4.10 As atualizações ou comunicações que os agentes necessitarem deverão ser feitas pelo gerenciador da solução. Caso o *endpoint* esteja sendo utilizado fora do ambiente corporativo e o gerenciador da solução estiver

instalado na rede do Tribunal, este poderá acessar o gerenciador da solução via internet, mas através de VPN, apenas para coleta de atualizações e para envio de incidentes registrados. Esses acessos devem ser definidos através de políticas internas deste órgão e os dados devem trafegar por meio do protocolo TLS 1.1 ou superior.

3.6.4.11 Os agentes devem possuir proteção contra desinstalação ou interrupção do agente.

3.6.4.12 Os logs devem ser registrados no agente e no servidor, acessíveis por SSH, SCP ou TLS 1.1 ou superior, sempre com controle de acesso e trilha de auditoria.

3.6.4.13 A solução deverá contar com recursos de *Machine Learning* ou

Deep Learnig com as seguintes funcionalidades mínimas:

3.6.4.13.1 Capacidade de aprendizado de comportamento de usuários para aprimoramento das detecções de comportamentos suspeitos;

3.6.4.13.2 Deve possuir tecnologia de análise de arquivos binários para identificação de comportamento malicioso;

3.6.4.13.3 Deve permitir a utilização de Centro de Inteligência de reputação para análise granular de arquivos ou URL's maliciosas, de modo a prover, rápida detecção de novas ameaças.

3.6.4.14 A solução deverá monitorar e informar os recursos de segurança dos *endpoints* em dashboard e relatórios contendo, no mínimo, as seguintes informações:

3.6.4.14.1 Dados sobre existência e atualizações do antivírus;

3.6.4.14.2 Situação do firewall no *endpoint*;

3.6.4.14.3 Se há *antispyware* instalado e se está atualizado;

3.6.4.14.4 Qual é a versão do sistema operacional;

3.6.4.14.5 Métricas de uso de CPU, memória RAM e rede.

3.6.4.15 Deverá realizar análise comportamental e monitoração de softwares, tendo por finalidade identificar e subsidiar ação de contenção de malwares em *endpoints*.

3.6.4.16 Deverá realizar detecção proativa contra *botnets* (detectar tentativas de conexão com, no mínimo, Comando & Controle em WEB).

3.6.4.17 Deverá realizar detecção de ameaças com armazenamento e execução somente em memória (*fileless*).

3.6.4.18 Deverá realizar inspeção em memória para busca de ameaças cibernéticas.

3.6.4.19 Deverá realizar detecção de ameaças com propagação silenciosa, como *ransomware* e *exploits*;

3.6.4.20 Deverá realizar detecção de vulnerabilidades e ameaças de *zero- day*.

3.6.4.21 Deverá identificar a execução de softwares ou versões de softwares que possuam vulnerabilidades.

3.6.4.22 Deverá realizar verificação de unicidade dos arquivos por meio da análise de *hash*, evitando que o mesmo binário seja analisado diversas vezes.

3.6.4.23 Deverá prover identificação de tráfegos de entrada e saída, com base em endereços MAC, *frame types*, protocolos, endereçamento IP e portas (serviços).

3.6.4.24 Possui capacidade de parametrizada de coletar, registrar e armazenar todas as conexões (TCP) ou transmissões (UDP) de rede, incluindo informações sobre endereços IP, portas de origem e destino e domínios DNS.

3.6.4.25 Deverá informar programas e processos em execução em tempo real.

3.6.4.26 Possuir registro de softwares (instalados, executados e em execução), com possibilidade de mitigação de softwares vulneráveis em execução bem como a data de instalação de cada item.

3.6.4.27 Monitorar e alertar sobre arquivos e programas suspeitos e maliciosos na rede, bem como a utilização de recursos elevados do *endpoint* ou sistema operacional.

3.6.4.28 Possuir mitigação automatizada ou manual capaz de encerrar processos em execução.

3.6.4.29 Capaz de detectar e alertar sobre ataques de vírus, malwares, *worms*, trojans, *spyware*, *backdoors* e qualquer outra forma de código mal- intencionado.

3.6.4.30 Capaz de detectar malwares por comportamento utilizando assinaturas.

3.6.4.31 Capaz de detectar código malicioso por análise comportamental.

3.6.4.32 Capaz de identificar propagação de malwares tipo *ransomware* e atividades suspeitas de criptografia de arquivos.

3.6.4.33 Deverá possuir motor de análise e detecção de dados acessados pelo usuário, em trânsito, para fora ou dentro da rede e armazenados localmente ou em um compartilhamento de rede.

3.6.4.34 Deverá ser capaz de emitir alertas de alteração de hardware no console, indicando uma nova classe de dispositivo encontrada ao identificar um novo dispositivo conectado no *endpoint*, cujo hardware seja desconhecido.

3.6.4.35 Deverá monitorar e coletar de eventos de *logon* e *logoff* de usuários, bloqueio e desbloqueio de sessão e acessos a compartilhamentos de

rede.

3.6.4.36 Deverá monitorar páginas web acessadas e download de arquivos a partir de páginas web.

3.6.4.37 Deverá realizar monitoramento, registro e emissão de alertas sobre:

3.6.4.37.1 Tentativas de evitar a coleta de dados da solução;

3.6.4.37.2 Tentativas de desinstalar a solução;

3.6.4.37.3 Alterações nas chaves de registro e em arquivos de configuração do sistema operacional.

3.6.4.38 Deverá realizar monitoramento de acesso remoto aos *endpoints*, de acordo com configuração realizada, de forma centralizada, via gerenciador da solução.

3.6.4.39 Deverá realizar monitoramento de operações (acesso, cópia, modificação, duplicação e exclusão) com arquivos no disco local, dispositivos USB, dispositivos móveis conectados, drives CD/DVD, mídias removíveis, compartilhamento em rede ou em nuvem e acesso a drivers de rede, com a respectiva coleta de evidências da operação.

3.6.4.40 Deverá realizar monitoramento, emissão de alertas e bloqueio automático ou manual de softwares não autorizados.

3.6.4.41 Deverá identificar patches não aplicados em sistemas operacionais e softwares instalados em *endpoints*.

3.6.4.42 Todos os registros de eventos classificados como incidentes deverão ser passíveis de envio ao gerenciador da solução.

3.6.4.43 Deverá realizar monitoramento e detecção dos seguintes atributos mínimos de hardware e software:

3.6.4.43.1 Versões;

3.6.4.43.2 Número de série;

3.6.4.43.3 Fabricante;

3.6.4.43.4 Data de instalação;

3.6.4.43.5 Identificação de novas instalações de software;

3.6.4.43.6 Localização imediata do primeiro software instalado na rede.

3.6.4.44 Deverá realizar monitoramento e detecção do desempenho dos *endpoints*, contemplando, no mínimo, os seguintes atributos:

3.6.4.44.1 CPU;

3.6.4.44.2 I/O;

3.6.4.44.3 Memória RAM;

3.6.4.44.4 Memória virtual;

3.6.4.44.5 Unidade de armazenamento.

3.6.4.45 Deverá realizar monitoramento e detecção de processos, drivers e serviços com, no mínimo, as seguintes informações:

3.6.4.45.1 Identificação de novo processo e localização da primeira ocorrência;

3.6.4.45.2 Identificar processos suspeitos através de análise comportamental;

3.6.4.45.3 Identificação de alteração de comportamento de processo, através de mudança de registro de versão, *hash*, assinatura, nome original e *checksum*.

3.6.4.46 O agente deve monitorar dados classificados contra vazamento nos seguintes vetores:

3.6.4.46.1 Software de cópia (clipboard);

3.6.4.46.2 Print de tela, independente de ferramenta;

3.6.4.46.3 Aplicações em Nuvem;

3.6.4.46.4 E-mail;

3.6.4.46.5 Compartilhamento de Rede;

3.6.4.46.6 Comportamento de usuário;

3.6.4.46.7 Monitorar uso de dados por P2P;

3.6.4.46.8 Monitoramento de arquivos sensíveis acessados na rede;

3.6.4.46.9 Rastreamento do uso de mídias removíveis.

3.6.4.47 Deverá detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade:

3.6.4.47.1 Heap spray;

3.6.4.47.2 Rootkit;

3.6.4.47.3 Falha em aplicação causada por exploit;

3.6.4.47.4 Identificação de processos vulneráveis, capazes de fazer sniffer, tokenização, encriptação, keylogger e ramsomware.

3.6.4.48 Deverá permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não:

3.6.4.48.1 Arquivos escritos;

3.6.4.48.2 Arquivos copiados para dispositivos de armazenamento externo e vice-versa;

3.6.4.48.3 Falhas de *logon* e *logoff*, local ou no domínio;

3.6.4.48.4 Logins paralelos;

3.6.4.48.5 Tentativa de resolução de *hostname*;

3.6.4.48.6 Tentativa de acesso a URL;

3.6.4.48.7 Logs do Windows com eventos de aplicação, segurança e sistema para usuários locais ou do domínio;

3.6.4.48.8 Identificação de acesso remoto via processos, IP e conexões internas ou externas;

3.6.4.48.9 Histórico de usuários que realizaram *logon* no equipamento;

3.6.4.48.10 Portas de rede ativas;

3.6.4.48.11 Hash MD5, SHA1, SHA2 e SHA3;

3.6.4.48.12 Processos na memória;

3.6.4.48.13 Processos usando a API do Sistema Operacional;

3.6.4.48.14 Contas de usuários;

3.6.4.48.15 Listagem de volumes;

3.6.4.48.16 Tarefas do Sistema Operacional.

3.6.4.49 Deverá permitir administração de *endpoints off-site* (conexão VPN, nuvem).

3.6.4.50 Deverá permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos.

3.6.4.51 Deverá permitir visualização por meio de aplicação web dos eventos contextualizados e ocorridos no passado (base histórica), permitindo investigação dos incidentes até suas causas raízes, detalhando as ações do artefato como: comunicações, gestão de arquivos e acesso a recursos de rede.

3.6.4.52 Disponibilizar todo o ciclo de execução de processos nos *endpoints* monitorados mostrando, no mínimo, recursos do *endpoint*, comunicações, edição e criação de arquivos. As informações do clico de execução deverão permitir a visualização dos eventos relevantes à análise dos incidentes, a partir dos campos usados nas pesquisas.

3.6.4.53 Deve ter a capacidade de identificar as seguintes informações nos dados armazenados no servidor central:

3.6.4.53.1 Como um ataque começou, por meio da visualização do encadeamento de processos executados até a causa raiz de um ataque;

3.6.4.53.2 O que o atacante fez, por meio do detalhamento dos processos e comandos executados, inclusive com parâmetros utilizados e alterações em sistema de arquivos;

3.6.4.53.3 Quantos e quais *endpoints* foram impactados;

3.6.4.53.4 Quais arquivos foram criados, modificados, acessados e removidos, por meio da visualização de alterações feitas no sistema de arquivos;

3.6.4.53.5 As comunicações efetuadas pelos processos analisados, por meio da listagem de conexões TCP/IP que foram efetuadas pelos sistemas e em que portas.

3.6.4.54 Deverá permitir, a qualquer momento, a listagem e pesquisa de valores históricos de registros dos artefatos monitorados.

3.6.4.55 Deverá permitir visualização dos parâmetros passados para os arquivos executáveis, quando houver a execução de binários em modo console (prompt de comando).

3.6.4.56 Deverá permitir o acesso, por meio do histórico armazenado no próprio gerenciador da solução, às alterações feitas nos sistemas de arquivo, leituras e alterações de registro, leituras, criações, remoções e modificações de arquivos, comunicações TCP/IP e todos os processos executados no sistema operacional de todos os computadores monitorados.

3.6.4.57 Possuir a capacidade de realizar inventário dos *endpoints* (software e hardware) onde estão instalados os agentes.

3.6.4.58 Deverá registrar a execução de aplicativos de terceiros, incluindo a capacidade de registrar o usuário responsável pela execução; como composição do sistema de segurança ativa.

3.6.4.59 Deverá identificar os *endpoints* com agentes desatualizados.

3.6.4.60 Deverá possuir mecanismo para identificar e eliminar a propagação lateral de ameaças sempre que identificar um *endpoint* infectado.

3.6.4.61 Ser compatível protocolo Network Time Protocol (NTP) e permitir alteração de fuso horário.

3.6.4.62 Possuir alimentação automática ou manual de fontes externas de inteligência para detecção e combate a novas ameaças e ataques (*threat intelligence*).

3.6.4.63 Possuir mecanismo automático de priorização de ameaças, fornecendo insumos para que infecções mais graves sejam investigadas prioritariamente.

3.6.4.64 Ter funcionalidade de identificar ameaças através de correlação de eventos e comportamentos dos *endpoints* gerenciados.

3.6.4.65 A solução deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes, de forma normalizada.

3.6.4.66 Os registros de logs devem conter, no mínimo: data e hora do evento, origem de acesso, usuário, *hostname* do equipamento, ameaças detectadas, excluídas e ações executadas.

3.6.4.67 O Gerenciador deve ter capacidade de armazenamento de logs de funcionamento da solução, para serem armazenados por, no mínimo, 12 (doze) meses e devem estar disponíveis para acesso por intermédio de filtros de pesquisa.

3.6.4.68 Possibilitar o envio dos logs a outros sistemas de armazenamento, seguindo padrão CSV ou XML.

3.6.4.69 Sobre geração de relatórios para *endpoint*, a solução:

3.6.4.69.1 Deve gerar relatórios a partir de todos os dados monitorados;

3.6.4.69.2 Deve permitir filtros personalizados para facilitar a visualização e gerenciamento;

3.6.4.69.3 Deve gerar relatórios automatizados em períodos, por hora, por dia, por semana, por mês e por ano, configuráveis pelo administrador.

3.6.4.70 Relatórios para *endpoints* devem conter, no mínimo:

3.6.4.70.1 Informações por domínio;

3.6.4.70.2 Informações por grupo de *endpoints*;

3.6.4.70.3 Informações por usuário (atividade web, uso de aplicativos e produtividade);

3.6.4.70.4 Informações por estação ou grupo de estações;

3.6.4.70.5 Informações de ataques identificados;

3.6.4.70.6 Informações de *logon* e *logoff* de usuários nos *endpoints*, inclusive *logons* secundários e em cache, além de bloqueios e desbloqueios de sessão;

3.6.4.70.7 Informações de arquivos (modificados, excluídos, copiados, acessados e duplicados);

3.6.4.70.8 Informações de programas (instalados, executados e em execução);

3.6.4.70.9 Informações de arquivos copiados dos discos locais dos *endpoints* para dispositivos de armazenamento externo e vice-versa;

3.6.4.70.10 Informações de histórico de ocorrências quanto ao uso simultâneo de redes WIFI e cabeadas por máquina ou por usuário;

3.6.4.70.11 Inventário de hardware, software e dispositivos;

3.6.4.70.12 Atividade de impressora quanto ao uso, ordem de impressão e arquivos enviados para impressão;

3.6.4.70.13 Performance das máquinas;

3.6.4.70.14 Estatística da rede;

3.6.4.70.15 Informações sobre ocorrência e irregularidade de processos.

3.6.4.71 Deverá fornecer resumo geral sobre status de segurança dos *endpoints* tais como: antivírus, Firewall do Windows, falta de atualização de segurança do Windows e computadores desprotegidos.

3.6.4.72 Deverá possuir sistema de notificações e alertas personalizável pelo administrador que poderá configurar os itens constantes no alerta, como ataques identificados, vulnerabilidades conhecidas, infecções detectadas, arquivos acessados, copiados, apagados, alterados, atividades de mídias removíveis (USB), alteração de hardware, utilização simultânea de redes sem fio e cabeada, avisos sobre eventos críticos no sistema (falha de hardware, falta de espaço de armazenamento em disco, notificação de ataque, etc.), instalação de novos aplicativos e demais itens que sejam monitorados.

3.6.4.73 Deverá possibilitar alertas por e-mail, para um destino definido pelo administrador.

3.6.4.74 Deverá possuir capacidade de apresentar os alertas em interface web.

3.6.4.75 Deverá ser capaz de emitir alertas baseados na comparação de *hashes* criptográficos de executáveis com *blacklists*, fornecidas pela própria solução, caso um executável considerado malicioso seja executado em um ou mais computadores.

3.6.4.76 Deverá possuir sistema de alertas personalizável pelo administrador que poderá configurar, no mínimo, os seguintes itens constantes em um alerta:

3.6.4.76.1 Ataques identificados;

3.6.4.76.2 Vulnerabilidades conhecidas;

3.6.4.76.3 Infecções detectadas;

3.6.4.76.4 Arquivos acessados;

3.6.4.76.5 Arquivos copiados;

3.6.4.76.6 Arquivos apagados;

3.6.4.76.7 Arquivos alterados;

3.6.4.76.8 *Logon* de determinados usuários;

3.6.4.76.9 Execução de determinados executáveis;

3.6.4.76.10 Aviso sobre eventos críticos no sistema (mínimo de falha de hardware, falta de espaço de armazenamento em disco e notificação de ataque);

3.6.4.76.11 Instalação de novos aplicativos.

3.6.5 Grupo 01, Item 02 - Licença de uso de software e garantia para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.

3.6.5.1 Os produtos de softwares que irão compor a solução poderão ser licenciados no modelo de direito de uso, desde que:

3.6.5.1.1 não perca suas funcionalidades quando da expiração da licença;

3.6.5.1.2 o direito de uso da licença e a garantia deverão ser de, no mínimo, 12 meses.

3.6.5.2 Caso a licença ofertada seja perpétua, a garantia deverá ser de, no mínimo, 12 meses.

3.6.5.3 As licenças desse item deverão ser compatíveis com as licenças do item 1.

3.6.5.4 A solução deverá suportar o monitoramento dos repositórios de dados não estruturados do Google G-Drive e Microsoft OneDrive. **No momento da contratação será optado por qual dos repositórios será licenciado.**

3.6.5.5 A solução deverá apresentar todos os usuários e grupos de segurança do repositório da nuvem monitorado.

3.6.5.6 A solução deverá apresentar todos os diretórios do repositório da nuvem monitorado.

3.6.5.7 A solução deverá permitir a busca por uma credencial, pasta ou arquivo sem a necessidade de navegação pelo diretório de usuários ou pastas.

3.6.5.8 A solução deverá mapear todas as permissões dos usuários nos arquivos e pastas e mostrar, graficamente para um usuário selecionado, todas as pastas que este tem acesso.

3.6.5.9 A solução deverá apresentar todas as contas, os usuários ou grupos de segurança com permissões em determinada pasta ou arquivo.

3.6.5.10 A solução deverá reter os eventos de auditoria nos arquivos e pastas com informações sobre o evento: data e hora, o usuário que realizou e que tipo de ação ocorreu e permitir a exportação destas informações da auditoria.

3.6.5.11 A solução deverá apresentar, em dashboard e em relatório, dados expostos na nuvem.

3.6.5.12 A solução deverá identificar e apresentar dados sensíveis compartilhados externamente.

3.6.5.13 A solução deverá possuir regras de comportamentos suspeitos, tal como excesso de uso, excesso de compartilhamento, recomendação de limpeza de permissões e usuários inativos.

3.6.5.14 A solução deverá permitir a criação manual de regras de comportamentos suspeitos.

3.6.5.15 A solução deverá apresentar em dashboard os alertas de comportamentos suspeitos gerados com informações do objeto impactado, usuário que realizou a ação e data e hora do evento;

3.6.5.16 A solução deverá permitir, a partir da seleção do alerta, a visualização dos eventos envolvidos no alerta.

3.6.5.17 A solução deverá demonstrar graficamente as permissões externas (através de contas externas ou *share links*) nos arquivos ou pastas dos recursos de nuvem monitorados.

3.6.5.18 A solução deverá permitir a busca e filtragem gráfica dos eventos de auditoria de acessos aos dados armazenados na solução.

3.6.5.19 A solução deverá possuir uma base de relatórios pré-definidos;

3.6.5.20 A solução deverá permitir a customização dos relatórios ou a criação de novos relatórios.

3.6.6 Serviços de suporte técnico e garantia dos itens 01 e 02 do Grupo 01.

3.6.6.1 Deverá ser prestado suporte técnico e manutenção pelo fabricante e CONTRATADA por todo período de vigência da garantia.

3.6.6.2 A CONTRATADA deverá fornecer credencial de acesso à CONTRATANTE para os sistemas do fabricante que estejam relacionados a procedimentos de suporte e perguntas mais frequentes.

3.6.6.3 Define-se serviço de suporte técnico e garantia como sendo aquele efetuado mediante abertura de chamado junto à CONTRATADA ou fabricante, via chamada telefônica 0800, e-mail ou internet, devendo o recebimento dos chamados ocorrerem em período integral (24 horas por dia e 7 dias por semana), com objetivo de solucionar problemas de funcionamento, disponibilidade da solução e de esclarecer dúvidas relacionadas à instalação, configuração, uso e atualização dos produtos.

3.6.6.4 Não haverá limite de quantidade de chamados remotos durante a vigência da garantia.

3.6.6.5 A CONTRATADA deverá disponibilizar canal de atendimento para abertura de chamados técnicos 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, mediante sistema *Web*, *e-mail* ou de um telefone 0800.

3.6.6.6 Concomitante ao suporte oferecido pela CONTRATADA, a solução ofertada deverá contemplar suporte direto com os fabricantes com nível de SLA equivalente ao exigido à CONTRATDADA.

3.6.6.7 Os mecanismos de acesso ao suporte da CONTRATADA e dos fabricantes deverão ser entregues pela CONTRATADA juntamente com as licenças de uso dos softwares.

3.6.6.8 A CONTRATDADA deverá realizado o suporte técnico, preferencialmente, de forma remota.

3.6.6.9 O modelo de acesso remoto ao ambiente da CONTRATANTE será acordado com a CONTRATADA durante a vigência da garantia.

3.6.6.10 Na impossibilidade do suporte remoto por alguma questão técnica, a CONTRATADA deverá realizar o suporte presencialmente nas dependências da CONTRATANTE.

3.6.6.11 Os chamados técnicos serão categorizados nos seguintes níveis de severidade:

Nível	Descrição
1	Serviço fora de operação e sem qualquer solução de contorno para emprego imediato.
2	Funcionalidades principais severamente prejudicadas. Operaçãoprossegue com restrições significativas. Solução de contorno temporária disponível.
3	Perda de funcionalidades não críticas. Operações deficientes de alguns componentes, mas o usuário continua a utilizar os serviços.
4	Questões de caráter geral

3.6.6.12 O nível de severidade dos chamados deverá ser comunicado à CONTRATADA pela CONTRATANTE no momento de sua abertura.

3.6.6.13 O início do atendimento dos chamados técnicos de nível de severidade 1 deverá ser iniciado em até 45 (quarenta e cinco) minutos; os de nível de severidade 2, em até 4 (quatro) horas, os de nível de severidade 3 em até 12 (doze) horas e o de nível de severidade 4 em até 24 (doze) horas.

3.6.6.14 Iniciado o atendimento, a CONTRATADA deverá solucionar o problema nos tempos máximos conforme:

Nível de severidade	Período máximo para solução
1	24 horas corridas
2	48 horas corridas
3	48 horas úteis
4	72 horas úteis

3.6.6.15 Caso a solução do problema dependa de ação do fabricante do *software,* a CONTRATADA deverá informar à CONTRATANTE essa situação e, com a anuência da CONTRATANTE, o tempo para a solução do problema poderá ser suspenso, retomando do ponto em que parou após o fabricante apresentar a solução.

3.6.6.16 A CONTRATADA deverá apresentar, mensalmente, ou através de sistema WEB, relatório contendo as informações de data e hora de abertura e fechamento do chamado,

nome do responsável pela abertura, nome do responsável pelo atendimento, número de controle (protocolo), nível de severidade e descrição sucinta do chamado.

3.6.6.17 Para cada chamado técnico, a CONTRATADA deverá informar um número de controle (protocolo) para registro, disponibilizar um meio de acompanhamento de seu estado, bem como manter histórico de ações e atividades realizadas.

3.6.6.18 Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações: número do chamado, categoria de prioridade, descrição do problema, descrição da solução, procedimentos realizados, data e hora da abertura do chamado, data e hora do fechamento do chamado, data e hora do início do atendimento, data e hora do término da execução dos serviços e identificação do técnico da empresa responsável pelo atendimento.

3.6.6.19 O Suporte técnico deverá ser efetuado em português por técnicos certificados nas soluções ofertadas.

3.6.6.20 O chamado técnico só será considerado concluído após confirmação do CONTRATANTE.

ANEXO II

MODELO DE TERMO DE CONFIDENCIALIDADE

A **Coordenação de Aperfeiçoamento de Pessoal de Nível Superior**, sediada em Brasília, Setor Bancário Norte, Quadra 2, Bloco L, CNPJ n.º 00889834/0001-08, doravante denominada **CONTRATANTE**, e, de outro lado, a JAMC Consultoria e Representação de Software LTDA, sediada em SRTVN Quadra 701, conjunto C, Ala B, Parte V, Nº 124, Asa Norte, CEP nº 70.719-903, em Brasília-DF, CNPJ n.º 24.425.034/0001-96, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º 45/2022,** doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações confidenciais do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações confidenciais, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE CONFIDENCIALIDADE, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e confidenciais, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informações classificadas em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados, processados ou não, que podem ser utilizados para a produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação Pública ou Ostensiva: é aquela cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informação Confidencial: informação sensível ou sigilosa objeto de proteção por meio deste Termo de Confidencialidade.

Informação Sensível: é o conhecimento estratégico que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possa beneficiar a sociedade e o Estado brasileiros.

Informação Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES CONFIDENCIAIS

Será considerada informação confidencial toda e qualquer informação sensível ou sigilosa, nos termos das definições previstas na cláusula segunda do presente Termo de Confidencialidade, classificada ou não nos termos da Lei de Acesso à Informação, Lei nº 12.527, de 2011. As disposições deste Termo de Confidencialidade incidem sobre toda informação que se enquadre nos conceitos definidos acima, seja escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES CONFIDENCIAIS, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES CONFIDENCIAIS que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III - sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso das INFORMAÇÕES CONFIDENCIAIS, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – As partes deverão cuidar para que as informações confidenciais fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Segundo – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia de informação confidencial a que tiver acesso sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Terceiro – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza confidencial das informações a que tiver acesso.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Quarto – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação confidencial da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quinto – Cada parte permanecerá como fiel depositária das informações confidenciais reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES CONFIDENCIAIS deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Sexto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações confidenciais disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sétimo - A CONTRATADA, na forma disposta no parágrafo segundo, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES CONFIDENCIAIS, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES CONFIDENCIAIS por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES CONFIDENCIAIS, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações confidenciais.

Parágrafo Oitavo – A CONTRATADA reconhece que é dever exclusivo da CONTRATANTE responder a quaisquer pedidos de acesso à informação formulados com fundamento na Lei nº 12.527, de 2011, bem como obriga-se a encaminhar formalmente à CONTRATANTE qualquer pedido de acesso à informação que lhe for formulado;

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, e obriga as partes desde a data de sua assinatura até expirar o prazo de classificação da informação confidencial a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL, ou até completar-se 5 anos do fim da vigência do CONTRATO PRINCIPAL, no caso das informações confidenciais não classificadas ou no caso de a classificação expirar antes.

Cláusula Sétima – DAS PENALIDADES

O descumprimento deste Termo de Confidencialidade, devidamente comprovado, possibilitará:

I – Imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular

processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666, de 1993.

II – Ao controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigatório a repará-lo, conforme previsto na Lei nº 13.709, de 2018.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Esse Termo de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste Termo de Confidencialidade, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações confidenciais disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações confidenciais inicialmente disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar informações confidenciais para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro de Brasília-DF, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CONFIDENCIALIDADE é assinado pelas partes em 2 vias de igual teor e um só efeito.

Brasília/DF.

CONTRATANTE

Representante Legal

Cargo

CONTRATADA

Representante Legal

Cargo

TESTEMUNHAS:

1 - *(Assinatura)*

2 - *(Assinatura)*

Documento assinado eletronicamente por **José André Mendes Coimbra**, **Usuário Externo**, em 20/12/2022, às 16:46, conforme horário oficial de Brasília, com fundamento no art. 54, inciso II, da Portaria nº 06/2021 da Capes.

Documento assinado eletronicamente por **Cláudia Mansani Queda de Toledo**, **Presidente**, em 21/12/2022, às 18:14, conforme horário oficial de Brasília, com fundamento no art. 54, inciso II, da Portaria nº 06/2021 da Capes.

Documento assinado eletronicamente por **Welandro Damasceno Ramalho**, **Testemunha**, em 21/12/2022, às 18:40, conforme horário oficial de Brasília, com fundamento no art. 54, inciso II, da Portaria nº 06/2021 da Capes.

Documento assinado eletronicamente por **Jaqueline de Souza Cardoso Alecrim**, **Testemunha**, em 21/12/2022, às 18:46, conforme horário oficial de Brasília, com fundamento no art. 54, inciso II, da Portaria nº 06/2021 da Capes.

[redacted] A autenticidade deste documento pode ser conferida no site http://sei.capes.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador [redacted] e o código CRC [redacted]