TRIBUNAL SUPERIOR DO TRABALHO
Edital do Pregão Eletrônico n.º 058/2021

(Regido pela Lei Complementar 123/06, pela Lei 10.520/02, pelos Decretos 7.892/13, 10.024/19 e 8.538/15 e subsidiariamente pelas Leis 8.078/90, 8.666/93, 9.784/99 e alterações).

Objeto: **Registro de preços para aquisição de soluções de segurança, auditoria e prevenção de ameaças.**

Data de abertura da sessão pública:
16/12/2021 às 14h no sítio www.comprasgovernamentais.gov.br

Tipo:	**Modo de disputa:**	**Exclusiva ME/EPP?**	**Processo:**
Menor preço	Aberto	☐Sim ☒Não	6001640/2021-00

Valor total estimado: R$ 74.591.257,85	**Apresentação de amostra?** ☐Sim ☒Não	**Vistoria prévia?** ☐Obrigatória; ☐Facultativa; ☒Não se aplica.
Regime de execução: Empreitada por preço global.		

Pedidos de esclarecimento e impugnações:
Até às 19h de 13/12/2021.

Os pedidos de esclarecimento e as impugnações referentes a este procedimento devem ser encaminhados exclusivamente por meio eletrônico via internet, para o endereço cpl@tst.jus.br.

Documentos de habilitação: (veja seção 8)

Requisitos básicos:	**Requisitos específicos:**
1. SICAF* ou documentos equivalentes; 2. Comprovação de capital social não inferior a 10%, quando o índice de liquidez corrente for igual ou inferior a 1. *Será emitido pelo pregoeiro durante a sessão pública.	Apresentação de, pelo menos, um atestado de capacidade técnica compatível com o objeto desta licitação.

Endereço da Coordenadoria de Licitações e Contratos: SAFS quadra 8, conjunto A, bloco A, sala A3.41. Brasília – DF. CEP: 70070-943.
Retire o edital e acompanhe esta licitação e seus atos na internet pelos portais www.tst.jus.br e www.comprasgovernamentais.gov.br

MARCOS FRANCA SOARES:26517
Assinado de forma digital por MARCOS FRANCA SOARES:26517
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora da Justica - AC-JUS, ou=26221089000100, ou=Presencial, ou=Cert-JUS Institucional - A3, ou=Tribunal Superior do Trabalho - TST, ou=SERVIDOR, cn=MARCOS FRANCA SOARES:26517
Dados: 2021.12.03 14:14:34 -03'00'

Coordenador de Licitações e Contratos

Gustavo P de Miranda
Assinado de forma digital por Gustavo P de Miranda
DN: cn=Gustavo P de Miranda, o, ou, email=gustavo.miranda@tst.jus.br, c=BR
Dados: 2021.12.03 14:04:28 -03'00'

Supervisor SAACPL

1. Objeto da Licitação

1.1. O objeto deste certame é o registro de preços para 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 e nos termos e condições constantes neste edital, bem assim no Termo de Referência que constitui parte integrante deste instrumento convocatório.

Grupo 1 – Itens 1 a 4					
Item	**Especificação**	**Unidade**	**Quantidade total para registro**	**Pedido mínimo**	**Valor unitário estimado R$**
1	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*. **CATSER: 24333**	Usuários	20057	1	2.459,75
2	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados. **CATSER: 24333**	Usuários	19378	1	479,22
3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*. **CATSER: 26972**	Serviço	10	1	102.828,37
4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint.* **CATSER: 3840**	Turma	24	1	37.371,71
Grupo 2 – Itens 5 a 23					
Item	**Especificação**	**Unidade**	**Quantidade total para registro**	**Pedido mínimo para o TST**	**Valor unitário estimado R$**
5	*Cluster* para prover recursos para solução de acesso a usuários privilegiados **CATSER: 469726**	Cluster	9	1	265.577,29

6	Garantia do fabricante por período de 12 meses para *cluster* para prover recursos para solução de acesso a usuários privilegiados **CATSER: 26000**	Cluster	9	1	49.094,43
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk) **CATSER: 24333**	Usuários	461	1	1.427,36
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk) **CATSER: 26000**	Usuários	461	1	291,93
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages) **CATSER: 24333**	Servidores	4736	1	45,73
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages) **CATSER: 26000**	Servidores	4736	1	9,57
11	Licença para estações de trabalho Windows **CATSER: 24333**	Estações	17447	1	14,41
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows **CATSER: 26000**	Estações	17447	1	4,18
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP) **CATSER: 24333**	Equipamentos	2491	1	23,30
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP) **CATSER: 26000**	Equipamentos	2491	1	4,55
15	Licença para aplicações conteinerizadas com secrets **CATSER: 24333**	Aplicações	510	1	8.138,05

16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets **CATSER: 26000**	Aplicações	510	1	1.603,75
17	Licença para aplicações não-conteinerizadas com senha embutida (hard coded) **CATSER: 24333**	Aplicações	723	1	1.650,89
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded) **CATSER: 26000**	Aplicações	723	1	332,05
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL) **CATSER:24333**	Instâncias	609	1	1.056,93
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL) **CATSER: 26000**	Instâncias	609	1	223,24
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados. **CATSER: 26972**	Serviço	9	1	49.448,40
22	Treinamento para solução de controle de acesso de usuários privilegiados. **CATSER: 3840**	Turma	32	1	16.483,60
23	Serviço e suporte técnico especializado **CATSER: 26000**	Mês	133	12	12.106,40

1.2. As especificações técnicas do objeto constam do item 3.6 do Termo de Referência.

1.3. A Ata de Registro de Preços resultante da presente licitação tem como órgão gerenciador o Tribunal Superior do Trabalho e como órgãos participantes os Tribunais Regionais do Trabalho da 4ª, 10ª, 13ª, 16ª, 17ª, 18ª, 20ª, 21ª e 22ª Regiões.

1.3.1. O detalhamento do quantitativo a ser registrado e os endereços dos órgãos participantes constam do Anexo IV deste edital.

2. Condições para Participação

2.1. Poderão participar deste pregão os interessados que atenderem a todas as exigências constantes deste edital, que estiverem previamente credenciados perante a Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, provedor do sistema eletrônico, cuja comunicação se dá pela Internet.

2.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar do pregão deverão dispor de chave de identificação e senha que poderão ser utilizadas em qualquer pregão eletrônico, salvo quando cancelada por solicitação do credenciado ou em virtude de seu descadastramento perante o SICAF.

2.1.2. O uso da senha de acesso pelo licitante é de sua inteira responsabilidade bem assim quaisquer transações efetuadas diretamente ou por seu representante, e não caberá ao provedor do sistema ou ao TST a responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

2.1.3. A perda da senha ou a quebra do sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

2.1.4. O credenciamento perante o provedor do sistema implica a responsabilidade legal do licitante e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

2.2. Ficam impedidos de participar desta licitação:

2.2.1. Os interessados que se encontrem sob falência, concurso de credores, dissolução, liquidação ou em regime de consórcio, qualquer que seja sua forma de constituição e as empresas estrangeiras que não funcionem no país;

2.2.2. Aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública ou punidos com suspensão do direito de licitar e contratar pelo TST, com base na Lei n.º 8.666/1993; ou impedidos de licitar e contratar com a União, com base na Lei n.º 10.520/2002 (TCU Acórdãos 842/2013, 3439/2012, 3243/2012 e 2242/2013, todos do Plenário).

2.2.3. A pessoa jurídica cujo(s) sócio(s) que compõe(m) seu quadro societário incorra(m) na vedação constante do inciso VI do art. 2º da Resolução CNJ 7/2005, acrescentado pela Resolução CNJ 229/2016.

2.3. O pregoeiro realizará a Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União, que abrange o cadastro do CNJ, do CEIS, do próprio TCU e o CNEP, a fim de evitar a contratação de empresas que tenham sofrido penalidades que obstem a celebração do contrato pretendido.

3. Credenciamento dos Representantes

3.1. O credenciamento do licitante, bem assim a sua manutenção, dependerá de registro atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 10 do Decreto nº 10.024/2019.

3.1.1. Caberá ao licitante interessado em participar do pregão eletrônico credenciar-se no SICAF, conforme disposto no inciso I do art. 19 do Decreto 10.024/2019.

3.2. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico e assumirá como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou deste Tribunal por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4. Forma de Apresentação da Proposta

4.1. As propostas deverão ser formuladas e encaminhadas exclusivamente por meio do sistema eletrônico, concomitantemente com os documentos de habilitação exigidos neste edital, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

4.1.1. Para a solução do Grupo 01, itens 01 e 02, a proposta deverá conter, necessariamente, o descritivo detalhado de cada produto de softwares ofertado e as licenças a eles vinculados.

4.1.2. As propostas deverão consignar no(s) campo(s) apropriado(s) do sistema o preço unitário, expresso em reais, incluindo todos os impostos, taxas, fretes e demais encargos indispensáveis ao perfeito cumprimento das obrigações contratuais.

4.1.3. No campo apropriado do sistema, o licitante deverá informar a quantidade a ser registrada;

4.1.4. Não será aceito quantitativo inferior ao total previsto para registro;

4.1.5. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

4.1.6. Os documentos de habilitação abrangidos pelo SICAF serão verificados pelo pregoeiro durante a sessão pública, nos termos do *caput* do art. 43 do Decreto 10.024/19.

4.2. Os interessados deverão cotar **todos os itens do grupo**, sob pena de desclassificação.

4.3. No campo “Descrição Detalhada do Objeto Ofertado” devem ser incluídas todas as informações necessárias ao perfeito detalhamento do objeto e, ainda, prazo de validade da proposta de, no mínimo, noventa dias, cuja omissão e/ou contrariedade implica a aceitação do prazo indicado.

4.4. Serão desclassificadas as propostas que comprovadamente cotarem objeto diverso daquele requerido nesta licitação, **que deixarem de cotar todos os itens de cada grupo** ou as que desatendam às exigências deste edital.

4.5. Os licitantes, no ato de envio de suas propostas, devem encaminhar, de forma virtual, utilizando a funcionalidade existente no sistema de pregão eletrônico, as seguintes declarações:

4.5.1. Inexistência de fato superveniente que o impeça de participar do certame;

4.5.2. Cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal;

4.5.3. Concordância com as condições estabelecidas neste edital e que atende aos requisitos de habilitação;

4.5.4. Atendimento aos requisitos do art. 3º da Lei Complementar n.º 123/2006, no caso de microempresas e empresas de pequeno porte.

4.6. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará o licitante às sanções previstas neste edital.

4.7. O licitante melhor classificado, após a fase de lances, deverá encaminhar, ainda, atendendo convocação do pregoeiro, declaração, conforme modelo do Anexo II (disponível no seguinte link: http://bit.ly/decNEPlicit), a fim de resguardar este órgão quanto à prática de nepotismo vedada pela Resolução CNJ nº 7, de 18/10/2005, com as alterações introduzidas pela Resolução 229, de 22/06/2016.

4.7.1. A Declaração deverá ser reapresentada no momento da assinatura do contrato, firmada por todos os sócios que compõem o quadro societário do licitante, conforme modelo constante do Anexo III (http://bit.ly/decNEPcont).

5. Critério de Aceitabilidade dos Preços

5.1. Os preços deverão ser cotados em reais, com duas casas decimais, sob pena de serem truncados.

5.2. Não serão aceitas propostas cujos valores **de cada um dos itens ou do grupo sejam superiores aos valores estimados** ou com preços manifestamente inexequíveis.

5.2.1. Somente poderá ser considerado excessivo qualquer preço após o encerramento da etapa de lances e, quando formulada contraproposta pelo Pregoeiro, após sua recusa ou no caso de omissão por parte do respectivo proponente.

5.3. Considera-se inexequível a proposta que, comprovadamente, for insuficiente para a cobertura dos custos da contratação, apresente preços simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não

tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

5.3.1. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o grupo será obrigatória a realização de diligências para o exame da proposta.

5.3.2. O ônus da prova da exequibilidade dos preços cotados incumbe ao autor da proposta, no prazo de três dias úteis contados da notificação.

6. Sessão Pública do Pregão Eletrônico

6.1. A sessão pública deste pregão eletrônico, conduzida pelo pregoeiro designado, ocorrerá em data e hora indicadas exclusivamente no sistema eletrônico e obedecerá ao rito estabelecido nos Decretos 10.024/2019 e 8.538/15.

6.1.1. Por força do disposto no art. 19, inciso IV do Decreto 10.024/2019, os licitantes estão obrigados a acompanhar as operações no sistema eletrônico durante a licitação, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão.

6.2. Aberta a sessão pública, o pregoeiro verificará as propostas apresentadas e desclassificará aquelas que estejam em desconformidade com os requisitos estabelecidos neste edital.

6.2.1. O pregoeiro abrirá todos os itens e procederá a análise das propostas de cada um deles.

6.2.2. A desclassificação de um único item implicará a desclassificação da proposta global.

6.2.3. A desclassificação de proposta será sempre fundamentada e registrada no sistema, com acompanhamento, em tempo real, por todos os participantes.

6.2.4. O desatendimento de exigências formais não essenciais não importará no afastamento da Licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão de sua proposta, durante a realização da Sessão Pública.

6.3. O sistema ordenará automaticamente somente as propostas classificadas pelo pregoeiro, as quais participarão da fase de lances.

6.4. O pregoeiro dará início à fase competitiva, quando então os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico.

6.5. Os licitantes poderão oferecer lances sucessivos e inferiores aos últimos por eles ofertados e registrados pelo sistema, observado o intervalo mínimo de diferença de

valores entre os lances de R$ 0,10 (dez centavos), que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta, conforme disposto no parágrafo único do art. 31 do Decreto 10.024/2019.

6.5.1. Caso haja dois ou mais lances iguais, prevalecerá aquele que for recebido e registrado primeiro.

6.6. Na fase de lances, a disputa será por item e a classificação final será pelo valor global do grupo.

6.6.1. Não se recomenda concentrar o esforço de redução em apenas um dos itens que integram o grupo, pois a incompatibilidade de um deles com o respectivo valor estimado pode levar à desclassificação da respectiva empresa proponente, nos termos do item 7.7.1.

6.7. **MODO DE DISPUTA – ABERTO:** Será adotado para o envio de lances o modo de disputa aberto, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.7.1. A etapa de envio de lances durará dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos.

6.7.2. A prorrogação automática da etapa de envio de lances será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período, inclusive quando se tratar de lances intermediários.

6.7.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a etapa de envio de lances será encerrada automaticamente.

6.7.4. Encerrada a etapa de envio de lances sem prorrogação automática pelo sistema, o pregoeiro, mediante justificativa, poderá admitir o reinício dessa etapa, em prol da consecução do melhor preço disposto no parágrafo único do art. 7º do Decreto 10.024/2019.

6.8. A cada lance ofertado por item, o Sistema atualizará automaticamente o valor global do grupo.

6.8.1. A empresa que ofertar o menor valor global para o grupo será classificada em primeiro lugar pelo critério de Julgamento por Preço Global – Lote.

6.9. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, vedada a identificação do detentor do lance.

6.10. No caso de desconexão do pregoeiro durante a etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.11. **Se estiverem participando do certame microempresas e empresas de pequeno porte, será observada a disciplina estabelecida nos artigos 44 e 45 da Lei Complementar 123/06, regulamentados pelo art. 5º do Decreto 8.538/15.**

7. Julgamento das Propostas e Habilitação

7.1. Encerrada a etapa de lances, o pregoeiro irá verificar se os documentos de habilitação foram enviados concomitantemente com a proposta, conforme previsto no item 4.1. Em seguida, irá avaliar a necessidade de efetuar contraproposta ao licitante que tenha apresentado lance mais vantajoso pelo sistema eletrônico, para que seja obtida melhor proposta, observado o critério de julgamento, sendo inadmissível negociar condições diferentes daquelas previstas no edital.

7.1.1. A negociação será realizada exclusivamente pelo canal de comunicação (chat) existente no sistema e poderá ser acompanhada pelos demais licitantes.

7.2. Serão recusadas propostas com o quantitativo inferior ao total previsto para registro.

7.3. As propostas que resultarem preços manifestamente inexequíveis serão desclassificadas.

7.3.1. Consideram-se preços manifestamente inexequíveis aqueles que, comprovadamente, forem insuficientes para a cobertura dos custos decorrentes da contratação pretendida.

7.3.2. Se houver indícios de inexequibilidade da proposta de preço, ou em caso de necessidade de esclarecimentos complementares, poderão ser efetuadas outras diligências.

7.4. Em seguida, o pregoeiro, mediante notificação a ser efetuada por meio do canal de comunicação (chat), irá solicitar ao participante melhor classificado que, **no prazo de 24 (vinte e quatro) horas**, **envie a proposta adequada** ao último lance ofertado após a negociação realizada, acompanhada da declaração de nepotismo de que trata o item 4.7, e, se for o caso, dos documentos complementares necessários à confirmação daqueles exigidos neste edital e já apresentados.

7.5. Juntamente com a proposta de preços, e no mesmo prazo determinado no item anterior, o licitante deverá encaminhar, ainda, a proposta técnica**.**

7.5.1. PROPOSTA TÉCNICA – A proposta técnica deverá conter **a descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas.**

7.5.2. Em conjunto com a proposta técnica, deverá ser fornecida pela licitante uma tabela ponto a ponto, relacionando o número das páginas da proposta com a comprovação do atendimento dos requisitos exigidos.

7.5.2.1. A tabela de comprovação técnica é parte obrigatória da proposta técnica É necessária a especificação de todos os itens contidos neste edital e a apresentação da documentação comprobatória com indicação da página e com informações das funcionalidades e características exigidas no item 3.6 do Termo de Referência. Salienta-se que todos os itens da tabela devem ser devidamente preenchidos.

7.5.2.2. A tabela de comprovação técnica deverá possuir, no mínimo, as informações e estrutura conforme abaixo:

Nº Requisito no TR	Descrição da característica ou funcionalidade exigida	Documento do fabricante (nome)	Página(s)	Atende ao Requisito (sim/não)

7.5.3. A Licitante deverá apresentar na proposta a indicação detalhada da solução ofertada citando, quando houver, a marca, modelo, tipo e fabricante.

7.5.4. Serão considerados documentos oficiais para comprovação técnica: catálogos, folders, prospectos e manuais.

7.5.5. Para os documentos do fabricante, é mandatória a comprovação que se trata de documento oficial fornecido pelo fabricante ao mercado, sendo comprovação suficiente desse requisito o link para o acesso ao documento no site do fabricante.

7.5.6. Havendo divergência entre as características técnicas descritas na proposta da licitante e as disponibilizadas pelo fabricante, prevalecerão os informes do fabricante, salvo os casos específicos em que o licitante esclareça os motivos da divergência e que sejam aceitos pelo TST.

7.5.7. Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela Licitante, no canto inferior direito.

7.5.8. Além da indicação da página da documentação fornecida na qual se encontra a comprovação de cada funcionalidade ou característica técnica exigida para cada item, a correspondente comprovação deverá ser necessariamente grifada ou destacada com marca texto.

7.5.9. A não apresentação de tabela de comprovação técnica ou apresentação de tabela divergente do exigido acarretará a desclassificação da licitante.

7.5.10. **PROVA DE CONCEITO** - Caso haja dúvidas sobre a capacidade do produto ofertado atender ao exigido nas especificações técnicas, a equipe do Tribunal poderá exigir a comprovação da especificação em dúvida por meio de prova

de conceito, que deverá ser realizada na infraestrutura do Tribunal e nas seguintes condições:

7.5.10.1. A licitante deverá apresentar, em até 1 (um) dia útil, os requisitos para instalação da sua solução no ambiente do Tribunal;

7.5.10.2. A equipe do Tribunal disponibilizará, em até 1 (um) dia útil, a infraestrutura necessária para a instalação da solução;

7.5.10.3. Caso os requisitos apresentados pela licitante sejam exagerados e em desacordo com o exigido nas especificações técnicas, o item em dúvida será considerado como não atendido;

7.5.10.4. A licitante terá até 3 (três) dias úteis para proceder com a instalação ea comprovação do(s) requisito(s) técnico(s) que levantaram dúvidas sobre a capacidade de atendimento;

7.5.10.5. Todo o procedimento deverá ser realizado de forma remota e demonstrado através de sala do Google Meet a ser fornecida pelo Tribunal.

7.5.10.6. Caso o fabricante da solução possua laboratório próprio, será facultado à Licitante oferecer a comprovação do requisito através desse laboratório, cabendo à equipe técnica do Tribunal avaliar se a comprovação desta forma é adequadaou se é necessário realizar a instalação nas dependências do Tribunal.

7.5.11. A Licitante deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666/1993.

7.6. Examinada(s) e aprovadas(s) proposta(s) classificada(s) em primeiro lugar, quanto ao objeto (proposta técnica/prova de conceito) e valor, o pregoeiro irá proceder à aceitação da proposta.

7.7. **O pregoeiro realizará a aceitação da proposta para o grupo, sendo impossível aceitar parte dos itens.**

7.7.1. O preço ofertado final de cada item que integra o grupo não pode ser superior ao valor estimado para a respectiva contratação.

7.8. Em seguida, o pregoeiro verificará a habilitação do licitante conforme disposições do edital.

7.9. Constatado o atendimento pleno das exigências contidas no edital, o proponente será declarado vencedor.

7.10. Será desclassificada a proposta que:

7.10.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

7.10.2. contenha vício insanável ou ilegalidade;

7.10.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

7.10.4. apresente preço final superior ao estimado, ou que apresente preço manifestamente inexequível.

7.11. Se a proposta for desclassificada ou se o licitante não atender às exigências habilitadoras, o pregoeiro examinará as propostas subsequentes, na ordem de classificação, até a obtenção de uma que atenda ao edital.

7.12. Será desconsiderada qualquer oferta de vantagem não prevista neste edital.

7.13. O pregoeiro, em qualquer fase do procedimento, poderá promover diligências julgadas necessárias à análise das propostas e da documentação, e os licitantes deverão atender às solicitações no prazo por ele estipulado, contado do recebimento da notificação.

7.14. Se um dos licitantes estiver impedido de participar em licitações ou tiver sido declarado inidôneo para licitar e contratar com a Administração Pública, será afastado do certame sem prejuízo das sanções legais cabíveis.

7.15. No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos, nem sua validade jurídica, mediante despacho fundamentado registrado em ata e acessível a todos, e lhes atribuirá validade e eficácia para fins de habilitação e classificação.

7.16. **A(s) empresa(s) vencedora(s) do certame somente deverá(ão) encaminhar proposta(s), declarações ou quaisquer outros documentos se expressamente solicitado pelo pregoeiro, mediante notificação efetuada pelo canal de comunicação (*chat*), sob pena de serem descartados.**

7.17. O sistema eletrônico produzirá automaticamente ata circunstanciada da sessão pública imediatamente após seu encerramento, a qual ficará acessível no Portal de Compras do Governo Federal (www.comprasgovernamentais.gov.br) e nela serão registradas as ocorrências relevantes.

8. Requisitos de Habilitação dos Licitantes

8.1. A habilitação será verificada por meio do SICAF, nos documentos por ele abrangidos, podendo os licitantes deixar de apresentar os documentos de habilitação que já constem do referido Sistema de Cadastramento.

8.2. A habilitação no que tange à **regularidade fiscal** far-se-á com a verificação de que o licitante está em situação regular perante a Fazenda Nacional, a Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS, e as Fazendas Estaduais e Municipais, quando for o caso.

8.3. A **regularidade trabalhista** do licitante deverá ser comprovada mediante certidão negativa, provando a inexistência de débitos inadimplidos perante a Justiça do Trabalho, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n.º 5.452, de 1º de maio de 1943, a qual será emitida pelo Pregoeiro no sítio do TST durante a sessão pública.

8.4. Para comprovação da qualificação **econômico-financeira**, será exigido Índice de Liquidez Corrente (ILC) superior a um. Se o balanço patrimonial cadastrado no SICAF estiver vencido, o licitante deverá apresentar Balanço Patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, em que sejam nomeados os valores do ativo circulante (AC) e do passivo circulante (PC), de modo a extrair-se Índice de Liquidez Corrente (ILC) superior a um, vedada a substituição por balancetes ou balanços provisórios.

8.4.1. As empresas que apresentarem ILC igual ou menor do que um quando de sua habilitação, em vista dos riscos para a administração, deverão comprovar capital social no valor mínimo de dez por cento do valor global da ata resultante da licitação, admitida a atualização para a data de apresentação da proposta mediante índices oficiais.

8.4.2. Após 30 de abril, serão considerados válidos, para fins de habilitação, apenas os balanços patrimoniais do ano anterior, sendo que, se adotada a Escrituração Contábil Digital, as empresas vinculadas ao Sped só estarão obrigadas a apresentar o balanço do ano anterior após o último dia útil do mês de maio.

8.4.3. As empresas com menos de um exercício financeiro devem cumprir a exigência deste item mediante apresentação de Balanço de Abertura ou do último Balanço Patrimonial levantado, conforme o caso.

8.4.4. Não será exigido das microempresas ou das empresas de pequeno porte a apresentação do índice mencionado no item 8.4, ficando dispensadas de apresentar o balanço patrimonial do último exercício social, conforme previsto no artigo 3º, do Decreto nº 8.538/2015.

8.4.4.1. Neste caso, a qualificação econômico-financeira poderá ser comprovada por meio do contrato social, ou da certidão simplificada emitida pela junta comercial, demonstrando um capital social mínimo não inferior a 10% do valor total da proposta aceita.

8.5. A **qualificação técnica** será comprovada mediante apresentação de, pelo menos, um atestado de capacidade técnica compatível com o objeto desta licitação.

8.5.1. Para a solução do Grupo 01, serão considerados compatíveis com o objeto da licitação atestados de capacidade técnica que comprovem a entrega dos mesmos produtos ofertados pela licitante.

8.5.2. Para a solução do Grupo 02, serão considerados compatíveis com o objeto da licitação atestados de capacidade técnica que comprovem a entrega e serviço técnico especializado para soluções de PAM.

8.5.3. Caso entenda necessário, o pregoeiro, por meio de diligência, poderá solicitar ao licitante a comprovação da legitimidade dos atestados apresentados, devendo o licitante disponibilizar todas as informações pertinentes, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

8.6. Disposições gerais sobre habilitação:

8.6.1. **Os licitantes que estiverem em situação regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF poderão deixar de apresentar os documentos referentes à HABILITAÇÃO JURÍDICA, QUALIFICAÇÃO ECONÔMICO-FINANCEIRA, REGULARIDADE FISCAL e TRABALHISTA**.

8.6.2. Os documentos exigidos para habilitação que não estejam contemplados no SICAF serão enviados nos termos do disposto no item 4.1.

8.6.3. Na hipótese de necessidade de envio de documentos complementares após o julgamento da proposta, estes deverão ser apresentados em formato digital, via sistema, no **prazo de duas horas** contado da solicitação do Pregoeiro.

8.6.3.1. Comprovada a impossibilidade de envio por meio da referida ferramenta, a critério do Pregoeiro, poderá ser utilizada outra forma de envio.

8.6.3.2. O prazo para envio poderá ser prorrogado por mais uma hora, a critério do Pregoeiro, desde que solicitado e justificado pelo interessado no chat da sessão pública ou por e-mail antes de expirado o prazo inicial estabelecido.

8.6.4. Para fins de habilitação, a verificação pelo órgão promotor do certame nos portais oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

8.6.5. Se a documentação de habilitação não estiver completa e correta, ou contrariar qualquer dispositivo deste edital, poderá o pregoeiro considerar o proponente inabilitado.

8.6.6. Caso o licitante seja inabilitado por irregularidade constatada quando da consulta no SICAF, e comprovar, exclusivamente mediante apresentação do Recibo de Solicitação de Serviço – RSS, nos termos do art. 37 da IN SLTI/MPOG n.º 02, de 11/10/2010, ter entregado a documentação à sua Unidade Cadastradora no prazo regulamentar, o pregoeiro suspenderá os trabalhos para proceder diligência, na forma estabelecida no § 3º do art. 43 da Lei n.º 8.666/1993.

8.6.7. Os documentos deverão ter validade expressa ou estabelecida em lei, admitidos como válidos, no caso de omissão, os emitidos a menos de noventa dias.

8.6.8. Não serão aceitos **protocolos de entrega** ou **solicitação de documento** em substituição aos documentos requeridos no presente edital.

8.6.9. Os documentos apresentados com a validade expirada, se não for falta sanável, acarretarão a inabilitação do proponente.

8.6.10. **Para as microempresas e empresas de pequeno porte, a comprovação da regularidade fiscal e trabalhista observará a disciplina estabelecida nos artigos 42 e 43 da Lei Complementar 123, de 14/12/06, regulamentados pelo art. 4º do Decreto 8.538, de 06/10/15, com as alterações trazidas pelas Leis Complementares 147/2014 e 155/2016**.

8.6.11. No ato de assinatura da Ata de Registro de Preços, bem como na assinatura de cada contrato será exigida a comprovação das condições de habilitação consignadas neste edital, as quais deverão ser mantidas pela Contratada durante a vigência da ata e eventuais contratos.

9. Instruções e Normas para Impugnação do Edital e Interposição de Recursos

9.1. Em até **três dias úteis** antes da data fixada para abertura da sessão pública, qualquer pessoa poderá **impugnar** o ato convocatório do pregão eletrônico.

9.1.1. A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelo setor responsável pela elaboração do edital e seus anexos, decidir sobre a impugnação no prazo de dois dias úteis da data do seu recebimento.

9.1.2. Acolhida a impugnação contra o ato convocatório, será definida e publicada nova data para realização do certame.

9.2. Os **pedidos de esclarecimento** referentes ao processo licitatório deverão ser enviados ao pregoeiro até **três dias úteis** anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico via Internet (e-mail), para o endereço indicado na folha de rosto, em mensagens escritas que **não podem conter**

qualquer tipo de anexo, nem serem encaminhados após as 19 horas do último dia do prazo, sob pena de serem descartadas, **assim como as impugnações que não observarem as mesmas restrições de prazo, forma e conteúdo.**

9.2.1. Caberá ao pregoeiro, auxiliado pelo setor responsável pela elaboração do edital e seus anexos, decidir sobre os pedidos de esclarecimento no prazo de dois dias úteis da data do seu recebimento.

9.3. A formulação da proposta, sem impugnação tempestiva ao edital, implica a plena aceitação pelos interessados das condições nela estabelecidas.

9.4. Declarado o vencedor, qualquer licitante poderá manifestar sua intenção de recorrer ao final da sessão pública, imediata e motivadamente, em campo próprio do sistema, tendo três dias para apresentar as razões de recurso. Os demais licitantes ficam, desde logo, notificados a apresentar contrarrazões em igual prazo contado do término do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

9.5. O encaminhamento das razões de recurso, bem assim das contrarrazões, deverá ser efetuado somente por meio do sistema eletrônico.

9.6. O recurso contra decisão do Pregoeiro não terá efeito suspensivo.

9.7. A falta de manifestação imediata e motivada do licitante quanto à intenção de recorrer importará a decadência desse direito e o pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

9.8. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.9. Se não reconsiderar sua decisão, o pregoeiro submeterá o recurso devidamente informado à consideração da autoridade competente que proferirá decisão definitiva antes da homologação do procedimento.

9.10. Os autos do processo administrativo eletrônico permanecerão com vista franqueada aos interessados, que deverão solicitá-la pelo e-mail cpl@tst.jus.br.

10. Prazos e Condições para Assinatura da Ata de Registro de Preços e do Contrato

10.1. Após a homologação do resultado desta licitação, o TST convocará a empresa adjudicatária para assinar a Ata de Registro de Preços - ARP.

10.2. Após a assinatura da Ata de Registro de Preços, havendo necessidade de adquirir o objeto, a empresa cujo preço foi registrado será convocada para a assinatura do contrato e retirada da respectiva nota de empenho, quando será exigida a comprovação das condições de habilitação consignadas no edital e, no caso das Microempresas e Empresas de Pequeno Porte optantes pelo Simples Nacional,

deverá ser entregue declaração de que é regularmente inscrita neste sistema tributário, conforme 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.

10.2.1. Para fins de assinatura eletrônica do contrato/ata de registro de preço, a empresa adjudicatária deverá cadastrar representante ou procurador no Sistema Eletrônico de Informações do TST, no prazo de 2 dias úteis, contados da adjudicação.

10.2.2. O cadastro deverá ser realizado pelo link https://sei.tst.jus.br/sei/controlador_externo.php?acao=usuario_externo_avisar_cadastro&id_orgao_acesso_externo=0.

10.2.3. Será permitido o cadastramento de até 5 representantes ou procuradores.

10.2.4. Realizado o cadastro do representante ou procurador, a ata de registro de preços/instrumento contratual deverá ser assinado no prazo de 2 dias úteis, contados da liberação para assinatura externa.

10.2.5. O descumprimento injustificado dos prazos assinalados sujeitará à adjudicatária ou contratada às sanções previstas no item 20.3 deste edital e ainda à perda do direito à contratação.

10.2.6. O prazo tem início na data de envio do contrato, excluindo-se da contagem o dia do envio e incluindo-se o do vencimento.

10.2.7. As notificações ou convocações enviadas ao e-mail da licitante constante da proposta de preço ou de qualquer outro documento enviado na sessão pública do pregão eletrônico serão reputadas entregues, independente de confirmação de recebimento.

10.2.8. Aplicam-se às regras desse item nos casos de convocação para assinatura de aditamentos, termo de rescisão ou qualquer outro instrumento derivado da contratação.

10.3. Não serão admitidos recursos, protestos, representações, ressalvas ou outra forma de discordância ou inconformismo a quaisquer tópicos do contrato que guardem absoluta conformidade com sua minuta, em expressão e substância.

10.4. Ao assinar a Ata de Registro de Preços, e eventualmente o contrato, a empresa adjudicatária obriga-se a prestar os serviços necessários, conforme especificações e condições contidas neste edital e na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

10.5. Quando o proponente vencedor não assinar a ARP no prazo e condições estabelecidos, é facultado ao TST convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

10.6. Os pedidos de fornecimento obedecerão à conveniência e às necessidades do TST, o qual não está obrigado a firmar as contratações advindas do registro de preços, e fica facultada a realização de licitação específica para a aquisição pretendida e assegurada ao beneficiário do registro à preferência de fornecimento em igualdade de condições.

10.7. A Ata de Registro de Preços vigente poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Federal, mediante anuência do órgão gerenciador, Tribunal Superior do Trabalho, desde que devidamente comprovada a vantagem.

10.8. Os órgãos e entidades, quando desejarem fazer uso da Ata de Registro de Preços, deverão consultar este Tribunal, por meio do e-mail contratos@tst.jus.br, para manifestação sobre a possibilidade de adesão.

10.9. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com este Tribunal.

10.10. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos do item deste instrumento convocatório e registrados na ata de registro de preços.

10.11. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços, independente do número de órgãos não participantes que aderirem.

11. Vigência da Ata de Registro de Preços e do Contrato

11.1. O prazo de vigência da Ata de Registro de Preços será de um ano.

11.1.1. Durante a vigência da ARP serão realizadas pesquisas de mercado periódicas para comprovação da vantajosidade dos preços registrados.

11.2. O prazo de vigência do contrato será 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.

11.2.1. Para o Grupo 01, a prorrogação é referente apenas aos itens 01 e 02.

11.2.2. Para o Grupo 02, a prorrogação contratual é referente apenas aos itens 06, 08, 10, 12, 14, 16, 18, 20 e 23.

12. Fiscalização da Execução Contratual

12.1. Na hipótese de aquisição do objeto do Registro de Preços, após a assinatura do contrato, a Administração designará um servidor, ou comissão de servidores, doravante denominado Fiscalização, com autoridade para exercer toda e qualquer ação de orientação geral durante a execução contratual.

12.2. São atribuições da Fiscalização, entre outras:

12.2.1. Acompanhar, fiscalizar e atestar a execução contratual, bem assim indicar as ocorrências verificadas;

12.2.2. 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;

12.2.3. Manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;

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

12.2.5. Propor a aplicação de penalidades à Contratada e encaminhar à Coordenadoria de Material e Logística - CMLOG os documentos necessários à instrução de procedimentos para possível aplicação de sanções administrativas.

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

13. Condições de Recebimento do Objeto da Licitação

13.1. O objeto de cada contrato será recebido das seguintes formas:

13.1.1. **Grupo 01, 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;

13.1.2. **Grupo 01, item 03** – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do serviço. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

13.1.3. **Grupo 01, item 04** – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do treinamento. Definitivamente,

mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

13.1.4. **Grupo 02, itens 05 a 20** – Provisoriamente, mediante termo circunstanciado, imediatamente depois de efetuada a entrega dos equipamentos e licenças, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a conclusão da instalação;

13.1.5. **Grupo 02, item 21** – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do serviço. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

13.1.6. **Grupo 02, item 22** – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do treinamento. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

13.1.7. **Grupo 02, item 23** - Provisoriamente, mediante termo circunstanciado, imediatamente após a entrega da nota fiscal referente aos serviços prestados no mês anterior, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo Circunstanciado, em até 10 (dez) dias úteis, após a verificação da perfeita execução das obrigações contratuais.

13.2. Os objetos entregues ou os serviços prestados em desconformidade com o especificado 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.

13.2.1. Essa notificação suspende os prazos de recebimento e de pagamento até que a irregularidade seja sanada.

13.3. 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 determinado pelo Contratante.

13.4. 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.

14. Condições de Pagamento

14.1. Os pagamentos serão efetuados da seguinte forma:

14.1.1. **Para todos os itens do Grupo 1** – 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.

14.1.2. **Para os itens 5 a 22 do Grupo 2** – 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.

14.1.3. **Para o item 23 do Grupo 2 –** mensalmente, em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo de cada mês, mediante atesto da nota fiscal e verificação da perfeita execução contratual pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

14.1.4. Para o TST, as notas fiscais e os documentos exigidos no edital para fins de liquidação e pagamento das despesas deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística do TST, situada no SAFS, quadra 8, conjunto A, bloco A, térreo, sala AT.152, CEP 70070-943, Brasília-DF, (61) 3043-4095.

14.1.5. Para os órgãos participantes, as notas fiscais e os documentos exigidos no edital para fins de liquidação e pagamento das despesas deverão ser entregues, a expensas da(s) Contratada(s), nos endereços constantes no Anexo IV.

14.1.6. Durante o período da pandemia do Coronavírus, os documentos indicados no item 14.1.4 deverão ser encaminhados exclusivamente ao e-mail sgcon@tst.jus.br.

14.1.7. A Nota Fiscal deverá corresponder ao objeto recebido 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.

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

14.2. 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.

14.3. A retenção dos tributos não será efetuada caso a Contratada apresente, no ato de assinatura do contrato ou entrega da nota de empenho, 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.

14.4. 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 edital, 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.

15. Reajustamento dos Preços

15.1. Os valores constantes da Ata de Registro de Preços admitem revisão na forma disciplinada no Decreto 7.892/2013.

15.2. 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:

$R = \frac{I - Io}{Io} \times P$, 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.

15.3. 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.

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

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

16. Obrigações da Contratada

16.1. Executar os serviços e entregar os produtos objeto desta licitação na forma e em prazo não superior ao máximo estipulado neste edital.

16.1.1. Os objetos deverão ser entregues na Coordenadoria de Infraestrutura Tecnológica, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, Sala A2.32, Brasília-DF, CEP 70.070-943, fones: (061) 3043-3035. E-mail de contato: citec@tst.jus.br.

16.1.2. 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.).

16.2. Reparar, corrigir, remover e substituir, a suas expensas, as partes do objeto deste edital em que se verifiquem vícios, defeitos ou incorreções resultantes da execução dos serviços.

16.3. 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.

16.4. Cumprir, para início da execução do objeto deste edital, os seguintes prazos:

16.4.1. **Grupo 01, itens 01 e 02** – em até 5 (cinco) dias úteis após a assinatura do contrato;

16.4.2. **Grupo 01, item 03** – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação;

16.4.3. **Grupo 01, item 04** – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento;

16.4.4. **Grupo 02, itens 05 a 20 e item 23** – em até 45 (quarenta e cinco) dias após a assinatura do contrato;

16.4.5. **Grupo 02, item 21** – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação;

16.4.6. **Grupo 02, item 22** – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento;

16.4.7. As reuniões de planejamento da instalação e de treinamento previstas para os itens 03 e 04 do Grupo 01 e itens 21 e 22 do Grupo 02, deverão ser realizadas em até 10 dias após a assinatura do contrato, a critério do Contratante.

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

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

16.4.10. A Contratada deverá se atentar, ainda, ao cumprimento dos prazos constantes do item 3.6 do Termo de Referência.

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

16.6. 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.

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

16.8. Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

16.9. 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.

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

16.11. Utilizar padrões definidos pela Contratante (nomenclaturas, metodologias etc.).

16.12. Substituir imediatamente aquele profissional que seja consideradoinconveniente à boa ordem ou que venha a transgredir as normas disciplinaresdo TST.

16.12.1. 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 do TST, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.

16.12.2. 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.

16.12.3. Divulgar aos seus profissionais a Política de Segurança da Informação do TST, PSI-TST, e assegurar-se de sua observação e cumprimento no curso da prestação de serviços no Tribunal. A PSI-TST está formalizada no ATO

GDGSET.GP. N° 183, DE 27 DE MAIO DE 2019 e pode ser consultada no endereço eletrônico: https://juslaboris.tst.jus.br/handle/20.500.12178/156111

16.13. 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.

16.14. Manter, durante toda a validade da Ata de Registro de Preços, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas.

16.15. 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 o TST.

16.16. Responder, integralmente, por perdas e danos que vier a causar diretamente ao TST 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.

16.17. A Contratada não será responsável:

16.17.1. Por qualquer perda ou dano resultante de caso fortuito ou força maior;

16.17.2. Por quaisquer obrigações, responsabilidades, trabalhos ou serviços não previstos neste edital.

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

17. Obrigações do TST

17.1. O TST, após a assinatura de cada contrato, compromete-se a:

17.1.1. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitir o acesso dos funcionários da Contratada às dependências do TST, relacionadas à execução do objeto deste edital;

17.1.2. Promover os pagamentos nas condições e dentro do prazo estipulado; e

17.1.3. Fornecer atestados de capacidade técnica, desde que atendidas às obrigações contratuais. Os requerimentos deverão ser protocolizados ou enviados por correspondência para o Protocolo Geral do TST, localizado no SAFS, quadra 08, conjunto A, bloco A, térreo, Brasília-DF, CEP 70.070-943.

18. Alterações na Ata de Registro de Preços

18.1. A Ata de Registro de Preços poderá sofrer alterações, obedecidas às disposições contidas nos artigos 17 e 18 do Decreto n.º 7.892/2013.

19. Cancelamento do Registro de Preços

19.1. O Fornecedor terá seu registro cancelado quando:

19.1.1. Descumprir as condições da Ata de Registro de Preços;

19.1.2. Deixar de retirar a respectiva ordem de fornecimento, nota de empenho ou instrumento equivalente, no prazo estabelecido pela Administração, sem justificativa aceitável;

19.1.3. Recusar-se a reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; e

19.1.4. Sofrer sanção prevista nos incisos III e IV do caput do art. 87 da Lei n.º 8.666 de 1993, ou no art. 7º da Lei 10.520 de 2002.

19.2. O cancelamento de registro nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do órgão gerenciador.

19.3. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

19.3.1. Por razão de interesse público; ou

19.3.2. A pedido do fornecedor.

20. Sanções para o Caso de Inadimplemento

20.1. 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 neste edital e no contrato e das demais cominações legais, aquele que:

20.1.1. Não assinar a ata de registro de preços ou o contrato;

20.1.2. Não entregar documentação exigida neste edital;

20.1.3. Apresentar documentação falsa;

20.1.4. Causar o atraso na execução do objeto;

20.1.5. Não mantiver a proposta;

20.1.6. Falhar ou fraudar na execução contratual;

20.1.7. Comportar-se de modo inidôneo;

20.1.8. Declarar informações falsas;

20.1.9. Cometer fraude fiscal.

20.2. 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.

20.2.1. Nessa hipótese, o atraso injustificado por período superior a 30 (trinta) dias caracterizará o descumprimento total da obrigação, punível com a sanção prevista no item 20.1 deste edital, como também a inexecução total contratual.

20.3. No caso de atraso no cumprimento do prazo de assinatura da ata de registro de preços ou do contrato, assinalado no item 10.2.5 deste edital, será aplicada multa de 0,5% (cinco décimos por cento) ao dia sobre o valor total contratado, até o limite de 15% (quinze por cento).

20.4. Para os itens do Grupo 01, 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.

20.5. Para os itens do Grupo 02, 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.

20.6. 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.

20.7. 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.

20.8. 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.

20.9. 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.

20.10. A não manutenção de todas as condições de habilitação e qualificação exigidas na licitação poderá resultar na rescisão do contrato, além das penalidades já previstas em lei, caso a Contratada não regularize a situação no prazo de 30 dias.

20.11. As multas porventura aplicadas serão descontadas dos pagamentos devidos pelo TST ou cobradas diretamente da empresa, amigável ou judicialmente, e poderão ser aplicadas cumulativamente com as demais sanções previstas neste tópico.

20.12. As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

20.13. 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.

20.13.1. Eventual pedido de prorrogação para os materiais/serviços adquiridos pelo TST deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, quadra 08, conjunto A, bloco A, térreo, sala T-18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4096 e-mail: sgcon@tst.jus.br.

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

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

21. Da Proteção de Dados

21.1. As partes envolvidas deverão observar as disposições da Lei 13.709, de 14/8/2018, 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 edital.

21.2. O Tribunal Superior do Trabalho 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.

21.3. A Contratada está obrigada 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.

21.4. Em caso de necessidade de coleta de dados pessoais indispensáveis à própria prestação do serviço, esta será realizada mediante prévia aprovação do TST, 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 edital, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins.

21.4.1. Eventualmente, as partes podem ajustar que o TST será responsável por obter o consentimento dos titulares, observadas as demais condicionantes do item 19.4.

21.5. A Contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas neste item, inclusive no tocante à Política de Privacidade do TST, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata este item.

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

21.6.1. Cumprimento de obrigação legal ou regulatória pelo controlador;

21.6.2. Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

21.6.3. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados;

21.7. O Encarregado indicado pela Contratada manterá contato formal com o Encarregado pelo contrato indicado pelo TST, 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.

21.8. 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.

22. Generalidades

22.1. O CNPJ do TST é 00.509.968/0001-48 e a UASG é 080001.

22.2. Esta licitação poderá ser revogada total ou parcialmente, sem que caiba indenização aos licitantes em consequência do ato, nos termos do art. 50 do Decreto 10.024/2019.

22.3. No curso da contratação, 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 contratual, cabendo à Administração decidir pelo prosseguimento ou rescisão contratual.

22.4. Em consonância com a Resolução 7, de 18 de outubro de 2005, do Conselho Nacional da Justiça, constante do Anexo I, 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.

22.4.1. A vedação constante no item anterior 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.

22.5. É de responsabilidade do Proponente o conhecimento das características dos serviços e produtos relacionados no objeto desta licitação.

22.6. Em caso de discrepância entre o Edital, seus anexos e os dados incluídos no sistema Comprasnet, prevalecerá a redação do instrumento convocatório.

22.7. **FORMAÇÃO DE CADASTRO RESERVA** - Em atendimento ao disposto no Decreto n.º 7.892/13, por ocasião da homologação do pregão no Sistema Comprasnet, havendo fornecedores com proposta(s) NÃO RECUSADA(S), estes serão convocados, a partir de e-mail enviado pelo Sistema, para aderirem ao Cadastro de Reserva pelo preço do licitante vencedor.

22.7.1. O registro da intenção de participar do cadastro será feito em funcionalidade disponibilizada pelo Sistema;

22.7.2. A data/hora final para o cadastro de reserva não será inferior a 24 horas, contadas da convocação;

22.7.3. O cadastro de reserva envolverá somente itens com propostas adjudicadas;

22.7.4. Findo o prazo para manifestação dos interessados, será gerada a correspondente Ata pelo Sistema;

22.7.5. **As sanções previstas no *caput* da cláusula vinte também se aplicam aos integrantes do cadastro de reserva que, convocados, não honrarem o**

compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

22.8. Quaisquer outros elementos necessários ao perfeito entendimento deste edital poderão ser obtidos na Coordenadoria de Licitações e Contratos, exclusivamente pelo endereço eletrônico cpl@tst.jus.br.

22.9. Esta licitação poderá ser acompanhada pelos portais www.tst.jus.br e www.comprasgovernamentais.gov.br, onde são divulgados os prazos, consultas e demais informações do certame.

ANEXO I

RESOLUÇÃO CNJ Nº 7, DE 18 DE OUTUBRO DE 2005

Art. 1° É vedada a prática de nepotismo no âmbito de todos os órgãos do Poder Judiciário, sendo nulos os atos assim caracterizados.

Art. 2° Constituem práticas de nepotismo, dentre outras:

I - o exercício de cargo de provimento em comissão ou de função gratificada, no âmbito da jurisdição de cada Tribunal ou Juízo, por cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados;

II - o exercício, em Tribunais ou Juízos diversos, de cargos de provimento em comissão, ou de funções gratificadas, por cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dois ou mais magistrados, ou de servidores investidos em cargos de direção ou de assessoramento, em circunstâncias que caracterizem ajuste para burlar a regra do inciso anterior mediante reciprocidade nas nomeações ou designações;

III - o exercício de cargo de provimento em comissão ou de função gratificada, no âmbito da jurisdição de cada Tribunal ou Juízo, por cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de qualquer servidor investido em cargo de direção ou de assessoramento;

IV - a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, de cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados, bem como de qualquer servidor investido em cargo de direção ou de assessoramento;

V - a contratação, em casos excepcionais de dispensa ou inexigibilidade de licitação, de pessoa jurídica da qual sejam sócios cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados, ou servidor investido em cargo de direção e de assessoramento; (Redação dada pela Resolução nº 229, de 22.06.16)

VI - a contratação, independentemente da modalidade de licitação, de pessoa jurídica 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. (Incluído pela Resolução nº 229, de 22.06.16)

§ 1º Ficam excepcionadas, nas hipóteses dos incisos I, II e III deste artigo, as nomeações ou designações de servidores ocupantes de cargo de provimento efetivo das carreiras judiciárias, admitidos por concurso público, observada a compatibilidade do grau de escolaridade do cargo de origem, a qualificação profissional do servidor e a complexidade inerente ao cargo em comissão a ser exercido, e que o outro servidor também seja titular de cargo de provimento efetivo das carreiras judiciárias, vedada, em qualquer caso a nomeação ou designação para servir subordinado ao magistrado ou servidor determinante da incompatibilidade. (Redação dada pela Resolução nº 181, de 17.10.13)

§ 2° A vedação constante do inciso IV deste artigo não se aplica quando a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público houver sido precedida de regular processo seletivo, em cumprimento de preceito legal.

§ 3º A vedação constante do inciso VI deste artigo 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. (Incluído pela Resolução nº 229, de 22.06.16)

§ 4º A contratação de empresa pertencente a parente de magistrado ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo tribunal, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório. (Incluído pela Resolução nº 229, de 22.06.16)

Art. 3º É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal contratante, devendo tal condição constar expressamente dos editais de licitação. (Redação dada pela Resolução n° 9, de 06.12.05)

Art. 4° O nomeado ou designado, antes da posse, declarará por escrito não ter relação familiar ou de parentesco que importe prática vedada na forma do artigo 2°.

Art. 5° Os Presidentes dos Tribunais, dentro do prazo de noventa dias, contado da publicação deste ato, promoverão a exoneração dos atuais ocupantes de cargos de provimento em comissão e de funções gratificadas, nas situações previstas no art. 2°, comunicando a este Conselho.

Parágrafo único Os atos de exoneração produzirão efeitos a contar de suas respectivas publicações.

Art. 6° O Conselho Nacional de Justiça, em cento e oitenta dias, com base nas informações colhidas pela Comissão de Estatística, analisará a relação entre cargos de provimento efetivo e cargos de provimento em comissão, em todos os Tribunais, visando à elaboração de políticas que privilegiem mecanismos de acesso ao serviço público baseados em processos objetivos de aferição de mérito.

Art. 7° Esta Resolução entra em vigor na data de sua publicação.

Relação familiar		
I - Cônjuge ou companheiro.		
II - Relação de parentesco até o 3º grau, inclusive.		
II.1 - Parentesco natural e civil.		
Linha reta	Ascendente	a) pais - 1º grau b) avós - 2º grau c) bisavós - 3º grau
	Descendente	a) filhos - 1º grau b) netos - 2º grau c) bisnetos - 3º grau
Linha colateral		a) irmãos - 2º grau b) tios e sobrinhos – 3º grau
II.2 - Parentesco por afinidade		
Linha reta	Ascendente	a) sogros (pais do cônjuge ou companheiro) - 1º grau b) padrasto ou madrasta - 1º grau c) padrasto ou madrasta do cônjuge ou companheiro - 1º grau d) avós do cônjuge ou companheiro - 2º grau e) bisavós do cônjuge ou companheiro - 3º grau
	Descendente	a) genro ou nora (cônjuge ou companheiro dos filhos) - 1º grau b) enteados (filhos do cônjuge ou companheiro) - 1º grau c) filhos dos enteados (netos do cônjuge ou companheiro) - 2º grau d) netos dos enteados (bisnetos do cônjuge ou companheiro) - 3º grau
Linha colateral		a) cunhados - 2º grau b) tios e sobrinhos do cônjuge ou companheiro - 3º grau

ANEXO II

DECLARAÇÃO

Identificação da Empresa:

Razão Social:
CNPJ:
Endereço:
Telefone:

Declaro, para fins de participação no Pregão Eletrônico n.º 058/2021, não haver no quadro societário da empresa identificada acima 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 do Tribunal Superior do Trabalho situadas na linha hierárquica da área encarregada da licitação.

A presente Declaração abrange um período de seis meses anteriores a esta data.

Local e data

_____

Representante da empresa

ANEXO III

DECLARAÇÃO

Identificação da Empresa:

Razão Social:
CNPJ:
Endereço:
Telefone:

Na condição de sócio(s) da empresa identificada acima, para fins de contratação decorrente do Pregão Eletrônico n.º 058/2021, declaro(amos) não incorrer na vedação do inciso VI do art. 2º da Resolução CNJ 7/2005, acrescentado pela Resolução CNJ 229/2016.

A presente Declaração abrange um período de seis meses anteriores a esta data.

Local e data

_____

Sócio 1

_____

Sócio 2

_____

Sócio 3

ANEXO IV

QUANTITATIVO REGISTRADO POR ÓRGÃO E ENDEREÇO DOS ÓRGÃOS PARTICIPANTES

Item	Quantitativo por órgão										Total
	TST	TRT 4ª	TRT 10ª	TRT 13ª	TRT 16ª	TRT 17ª	TRT 18ª	TRT 20ª	TRT 21ª	TRT 22ª	
1	3755	4300	2000	1204	880	1418	2400	1000	1100	2000	**20057**
2	4000	4250	2000	1330	880	1418	2400	1000	1100	1000	**19378**
3	1	1	1	1	1	1	1	1	1	1	**10**
4	4	1	1	2	4	2	4	2	2	2	**24**
5	1	0	1	1	1	1	1	1	1	1	**9**
6	1	0	1	1	1	1	1	1	1	1	**9**
7	60	0	10	60	45	56	100	30	70	30	**461**
8	60	0	10	60	45	56	100	30	70	30	**461**
9	1059	0	400	300	100	377	900	400	800	400	**4736**
10	1059	0	400	300	100	377	900	400	800	400	**4736**
11	3645	0	2500	1500	750	1352	2500	1200	2000	2000	**17447**
12	3645	0	2500	1500	750	1352	2500	1200	2000	2000	**17447**
13	323	0	300	230	614	274	350	100	150	150	**2491**
14	323	0	300	230	614	274	350	100	150	150	**2491**
15	5	0	50	30	43	30	300	10	30	12	**510**
16	5	0	50	30	43	30	300	10	30	12	**510**
17	77	0	200	50	26	70	50	80	20	150	**723**
18	77	0	200	50	26	70	50	80	20	150	**723**
19	60	0	100	35	43	41	70	35	200	25	**609**
20	60	0	100	35	43	41	70	35	200	25	**609**
21	1	0	1	1	1	1	1	1	1	1	**9**
22	6	0	1	6	3	6	4	2	2	2	**32**
23	12	0	1	12	12	12	12	12	48	12	**133**

Orgão	Endereço
TST	SAFS, quadra 8, conjunto A, bloco A, térreo, sala T18, CEP 70070-943, Brasília-DF, (61) 3043-4080.
Tribunal Regional do Trabalho da 4ª Região - UASG: 80014	Av. Praia de Belas, 1100 Porto Alegre/RS CEP: 90110-903 (51) 3255-2000
Tribunal Regional do Trabalho da 10ª Região - UASG: 80016	SAS Quadra 1, Bloco "D" Praça dos Tribunais Superiores - Brasília/DF CEP: 70097-900 (61) 3348-1100
Tribunal Regional do Trabalho da 13ª Região - UASG: 80005	Av. Corálio Soares de Oliveira, S/N, Centro João Pessoa/PB CEP: 58013-260 (83) 3222-8229
Tribunal Regional do Trabalho da 16ª Região - UASG: 80018	Av. Senador Vitorino Freire, Nº 2001, Areinha CEP: 65010-650 (98) 2109 – 9378 São Luís/MA
Tribunal Regional do Trabalho da 17ª Região - UASG: 80019	Rua Pietrângelo de Biase, 33, Centro, Vitória-ES CEP 29010-922 (27) 3321-2400
Tribunal Regional do Trabalho da 18ª Região - UASG: 80020	Rua T-29, esquina com rua T-51, n.1403, Lotes 7 a 22, Quadra T 22, S. Bueno Goiânia, GO CEP: 74215-901 (62) 3901-3610
Tribunal Regional do Trabalho da 20ª Região - UASG: 80023	Av. Carlos Rodrigues da Cruz, s/nº Centro Administrativo Gov. Augusto Franco - Capucho - Aracaju/SE CEP: 49081-015 (79) 2105-8870 / (79) 2105-8864
Tribunal Regional do Trabalho da 21ª Região - UASG: 80021	Av. Capitão-Mor Gouveia, 3104 - Lagoa Nova - Natal/RN CEP: 59063-900 (84) 4006-3001 / 4006-3002
Tribunal Regional do Trabalho da 22ª Região - UASG: 80024	Av. João XXIII, 1460, bairro dos Noivos Teresina-PI, Cep: 64000-931 (86) 2106-9574

ATA DE REGISTRO DE PREÇOS PE – 058/2021

No dia __ de _____ de 2021, no Tribunal Superior do Trabalho, órgão gerenciador desta Ata, registra-se o preço da empresa abaixo identificada para 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), abrangendo garantia, serviço de instalação e treinamento, conforme descrito no quadro abaixo, resultante do Pregão Eletrônico n.º 058/2021, tendo como órgãos participantes os TRT's da 4ª, 10ª, 13ª, 16ª, 17ª, 18ª, 20ª, 21ª e 22ª Regiões. As especificações técnicas constantes do processo administrativo TST 6001640/2021-00, bem assim os termos da proposta, integram esta Ata de Registro de Preços, independentemente de transcrição.

Este registro de preços tem a vigência de um ano, até __ de _____de 2022.

Item	Especificação	Unidade	Quantidade total para registro	Pedido mínimo	Preço unitário registrado
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 estruturados, abrangendo centro de dados e *endpoint*.	Usuários	20057	1	
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	19378	1	
3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.	Serviço	10	1	
4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint.*	Turma	24	1	
5	*Cluster* para prover recursos para solução de acesso a usuários privilegiados	Cluster	9	1	
6	Garantia do fabricante por período de 12 meses para *cluster* para prover recursos para solução de acesso a usuários privilegiados	Cluster	9	1	
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)	Usuários	461	1	

Item	Especificação	Unidade	Quantidade total para registro	Pedido mínimo	Preço unitário registrado
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk)	Usuários	461	1	
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	4736	1	
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	4736	1	
11	Licença para estações de trabalho Windows	Estações	17447	1	
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações	17447	1	
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	2491	1	
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	2491	1	
15	Licença para aplicações conteinerizadas com secrets	Aplicações	510	1	
16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets	Aplicações	510	1	
17	Licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações	723	1	
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações	723	1	
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	609	1	
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	609	1	
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	Serviço	9	1	
22	Treinamento para solução de controle de acesso de usuários privilegiados.	Turma	32	1	
23	Serviço e suporte técnico especializado	Mês	133	12	

Item	Especificação	Unidade	Quantidade total para registro	Pedido mínimo	Preço unitário registrado
Empresa vencedora: ... CNPJ: Endereço: CEP: Telefone: (..) Fax: (..) E-mail:					

Dirley Sérgio de Melo
Secretário de Administração
Tribunal Superior do Trabalho

Nome
Cargo
Empresa

Marcos França Soares
Coordenador de Licitações e Contratos
Tribunal Superior do Trabalho

1. Definição do Objeto

1.1 Registro de preços para 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), abrangendo garantia, serviço de instalação e treinamento.

Grupo 01 - Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.					
Grupo	**Item**	**Especificação**	**Unidade**	**Quantidade a Registrar**	**Pedido Mínimo**
01	01	Licença de uso de *software* e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.	Usuários	3755	1
	Código CATMAT/CATSER: **111490**				
	02	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	4000	1
	Código CATMAT/CATSER: **002299-3**				
	03	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.	Serviço	1	1
	Código CATMAT/CATSER: **26972**				
	04	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.	Turma	4	1
	Código CATMAT/CATSER: **3840**				
Classificação do Objeto:		**3.33.90.40.07 (Manutenção corretiva/adaptativa e sustentação de *softwares*)**			
Código do SIGEO:		**151012021000169**			

Tabela 1 – Objetos a registrar, Grupo 01.

Grupo 02 - Solução de controle de acesso de usuários privilegiados					
Grupo	**Item**	**Especificação**	**Unidade**	**Quantida de a Registrar**	**Pedido Mínimo**
02	05	*Cluster* para prover recursos para solução de acesso a usuários privilegiados	*Cluster*	1	1
	Código CATMAT/CATSER: **469726**				
	06	Garantia do fabricante por período de 12 meses para *cluster* para prover recursos para solução de acesso a usuários privilegiados	*Cluster*	1	1
	Código CATMAT/CATSER: **002299-3**				
	07	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk)	Usuários	60	1
	Código CATMAT/CATSER: **111490**				
	08	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk)	Usuários	60	1
	Código CATMAT/CATSER: **002299-3**				
	09	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	1.059	1
	Código CATMAT/CATSER: **111490**				
	10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	1.059	1
	Código CATMAT/CATSER: **002299-3**				
	11	Licença para estações de trabalho Windows	Estações	3.645	1
	Código CATMAT/CATSER: **111490**				
	12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações	3.645	1
	Código CATMAT/CATSER: **002299-3**				
	13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e	Equipamentos	323	1

Grupo 02 - Solução de controle de acesso de usuários privilegiados					
Grupo	**Item**	**Especificação**	**Unidade**	**Quantida de a Registrar**	**Pedido Mínimo**
		Controladoras WIFI, VOIP)			
	Código CATMAT/CATSER: **111490**				
	14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	323	1
	Código CATMAT/CATSER: **002299-3**				
	15	Licença para aplicações conteinerizadas com secrets	Aplicações	5	1
	Código CATMAT/CATSER: **111490**				
	16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets	Aplicações	5	1
	Código CATMAT/CATSER: **002299-3**				
	17	Licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações	77	1
	Código CATMAT/CATSER: **111490**				
	18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações	77	1
	Código CATMAT/CATSER: **002299-3**				
	19	Licença para instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL)	Instâncias	60	1
	Código CATMAT/CATSER: **111490**				
	20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL)	Instâncias	60	1
	Código CATMAT/CATSER: **002299-3**				
	21	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	Serviço	1	1
	Código CATMAT/CATSER: **26972**				
	22	Treinamento para solução de controle de acesso de usuários	Turma	6	1

Grupo 02 - Solução de controle de acesso de usuários privilegiados					
Grupo	**Item**	**Especificação**	**Unidade**	**Quantida de a Registrar**	**Pedido Mínimo**
		privilegiados.			
	Código CATMAT/CATSER: **3840**				
	23	Serviço e suporte técnico especializado	Meses	12	12
	Código CATMAT/CATSER: **26972**				
Classificação do Objeto:	**3.33.90.40.07 (Manutenção corretiva/adaptativa e sustentação de *softwares*)**				
Código do SIGEO:	**151012021000169**				

Tabela 2 – Objetos a registrar, Grupo 02.

1.2 O preço final deverá incluir todas as despesas referentes ao frete, às embalagens, aos tributos e aos demais encargos indispensáveis ao perfeito cumprimento das obrigações decorrentes do contrato.

1.3 A proposta deverá especificar, quando cabíveis: marca, modelo, data de fabricação, data de validade, fabricante, custos unitários e totais e, se possível, outras referências que bem identifiquem o objeto cotado.

1.4 Para a solução do Grupo 01, itens 01 e 02, a proposta deverá conter, necessariamente, o descritivo detalhado de cada produto de softwares ofertado e as licenças a eles vinculados.

1.5 A proposta deverá ser enviada em conjunto com a proposta técnica.

1.6 No que se referir a hardware, os materiais deverão ser acondicionados em embalagens lacradas, com a devida identificação do produto.

2. Fundamentação da Contratação

2.1 Motivação da Contratação

Em novembro de novembro de 2020 o Superior Tribunal de Justiça foi alvo do maior ataque cibernético já realizado ao um órgão do Governo Brasileiro. Foram mais de 7 dias com todos os sistemas indisponíveis. O foco do ataque foi a infraestrutura do Datacenter do STJ. Ataque com consequência semelhante foi realizado no Tribunal de Justiça do Rio Grande do Sul, TJ/RS, no final de abril de 2021, mas o foco, dessa vez, foram as mais de 12.000 estações de trabalho do TJ/RS, conhecidos como *endpoints*. Focos diferentes, estragos semelhantes, modo de operação similar: ataques do tipo *ransomware* que exploram vulnerabilidades existentes.

Durante a ataque ocorrido ao STJ, o TST criou uma sala de guerra para buscar ações que reduzissem as eventuais vulnerabilidades do seu ambiente computacional, no entanto, a pergunta mais crítica que não pode ser respondida foi: “há algum usuário comprometido no nosso ambiente?”.

Diante desse cenário em que vários órgãos da Administração Pública Federal e instituições privadas sofreram ataques, propomos a aquisição da solução proposta com o objetivo de mitigar e até eliminar potenciais vulnerabilidades que porventura poderiam vir a ser exploradas no TST e CSJT.

2.2 Objetivos a serem alcançados

O principal objetivo é da pretensa contratação é:

- Aprimorar a segurança da informação, através da aquisição, implantação e uso de ferramentas avançadas de segurança da informação.

Com a contratação de tais ferramentas, pretende-se colocar o Tribunal em acordo com às recomendações constates no Manual de Referência de Proteção de Infraestruturas Críticas de TIC, aprovado através da PORTARIA CNJ No 162, DE 10 DE JUNHO DE 2021, e às recomendações constantes na norma ABNT NBR ISO/IEC 27001:2013, item 10.10.

A necessidade apresentada não se limita ao TST, sendo comum a todos os tribunais da Justiça do Trabalho. Nesse sentido, outros tribunais da JT podem se beneficiar da contratação de soluções de TIC advindas do presente estudo. Assim, esse estudo deverá ser compartilhado com os demais tribunais da JT que poderão participar do pregão eletrônico em momento oportuno.

2.3 Benefícios diretos e indiretos resultantes da contratação

Ao atingir o objetivo principal, é esperado que os seguintes benefícios, diretos e indiretos, sejam alcançados:

- Permitir a automação de controle de privilégios aos curadores dos dados e informações;
- Aprimorar a governança de TI quanto aos dados não estruturados;
- Aprimorar a gestão de segurança da informação e comunicações.
- Aproveitamento eficiente do espaço de armazenamento dos eventos de auditoria;

Mitigar o risco de ataques de *ransomware* e, caso ele ocorra, limitar seu efeito e consequente impacto.

2.4 Alinhamento entre a contratação e os planos estratégicos do TST e planos estratégicos de Tecnologia da Informação

A contratação em questão está alinhada ao Plano Estratégico 2021-2026, Perspectiva “Sociedade” Objetivo Estratégico “Fortalecer imagem institucional” e ao Plano Diretor de TIC do TST 2021 Objetivo Estratégico “OE-1 Buscar uma excelente experiência do usuário”.

2.5 Referência aos Estudos Preliminares de STIC realizados

Os Estudos Técnicos Preliminares (ETP) constam dos autos.

2.6 Relação entre a demanda prevista e a quantidade de cada item

A relação entre demanda prevista e quantitativo de cada item consta no item 2.7 dos ETP.

2.7 Soluções similares disponíveis em outros órgãos e no Portal do Software Público Brasileiro

Em consulta ao portal do software público brasileiro (https://softwarepublico.gov.br/social/), realizada em 30/07/2021, não foram

identificadas soluções de auditoria para ambientes de datacenter, *endpoint* e gestão de usuários privilegiados que atendam a demanda em tela.

2.8 Análise do mercado de Tecnologia da Informação e Comunicação

O levantamento de mercado consta do item 2.9 Levantamento de mercado dos ETP.

2.9 Natureza do objeto a ser contratado

Trata-se de aquisição de serviço comum, cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

2.10 Justificativas para o parcelamento ou não da solução

A justificativa para o não parcelamento consta do item 4.2 do ETP.

2.11 Forma de adjudicação do objeto

Conforme item 4.3 Adjudicação do objeto, do ETP, a adjudicação do objeto será global para cada Grupo, de forma que os produtos formem um conjunto único, compatíveis em marca e modelo e projeto.

2.12 Modalidade e tipo de licitação

O regime de contratação proposto é de Licitação por Pregão Eletrônico para registro de preços, com amparo na Lei nº 10.520/2002, regulamentada pelo Decreto nº 10.024/2019, combinados com o Decreto nº 3.555/2000 e com a Lei nº 8.666/93.

2.13 Impacto ambiental decorrente da contratação

Não haverá impacto ambiental decorrente da contratação.

3. Modelo de execução e gestão do contrato

3.1 Deveres e responsabilidades do CONTRATANTE

3.1.1 Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir o livre acesso dos técnicos da CONTRATADA às dependências do CONTRATANTE relacionadas à execução da garantia.

3.1.2 Promover os pagamentos em moeda corrente nacional, mediante depósito na conta bancária indicada pela CONTRATADA, após o ateste da Nota Fiscal.

3.1.3 Fornecer atestados de capacidade técnica quando solicitado, desde que atendidas às obrigações contratuais.

3.1.4 Após a assinatura do contrato, o CONTRATANTE designará, formalmente, servidor ou comissão de servidores para exercerem o acompanhamento e fiscalização da execução contratual.

3.2 Deveres e responsabilidades da CONTRATADA

3.2.1 Entregar o objeto e executar os serviços descritos no contrato nos prazos máximos nele determinados.

3.2.2 Atender prontamente as solicitações da fiscalização do contrato e da garantia, inerentes ao objeto, sem qualquer ônus adicional ao órgão CONTRATANTE.

3.2.3 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.

3.2.4 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços.

3.2.5 Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez inexistir, no caso, vínculo empregatício deles com o CONTRATANTE.

3.2.6 Responder integralmente por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão dolosa ou culposa, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

3.2.7 Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações por ele solicitadas, relativas ao cumprimento do objeto.

3.2.8 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

3.2.9 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.

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

3.2.11 Utilizar padrões definidos pela CONTRATANTE (nomenclaturas, metodologias etc.).

3.2.12 Substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares do TST.

3.2.13 Os profissionais disponibilizados pela CONTRATADA para a prestação dos serviços deverão estar identificados com crachá de identificação dela,1 estando sujeitos às normas internas de segurança do TST, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.

3.2.14 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.

3.2.15 Divulgar aos seus profissionais a Política de Segurança da Informação do TST, PSI-TST, e assegurar-se de sua observação e cumprimento no curso da prestação de serviços no Tribunal. A PSI-TST está formalizada no ATO GDGSET.GP. N° 183, DE 27 DE MAIO DE 2019 e pode ser consultada no endereço eletrônico: https://juslaboris.tst.jus.br/handle/20.500.12178/156111

3.2.16 Comprovar a quitação dos tributos de importação referentes aos produtos, conforme disposto no Decreto nº 7.174/2010, art. 3º, inc. III, da seguinte forma:

3.2.16.1 Caso os produtos entregues sejam importados e a CONTRATADA for a importadora, a comprovação poderá ser feita por meio da apresentação dos seguintes documentos, sob pena de rescisão contratual e multa:

a) Comprovante de Importação emitido no Siscomex quando a Declaração de Importação – DI, é desembaraçada;

b) Última versão do extrato da Declaração de Importação.

3.2.16.1.1 Os bens fornecidos devem estar descritos na DI de forma a permitir a identificação precisa, constando marca, modelo e, se possível, nº de série.

3.2.16.2 Caso o produto entregue não seja importado deverá ser apresentada, no momento da entrega, uma declaração da CONTRATADA atestando essa situação.

3.2.16.2.1 A declaração deverá ser apresentada mesmo para as empresas que participaram da licitação utilizando-se da preferência de que trata o art. 3º da Lei 8.248/91.

3.2.16.3 Caso o produto entregue seja importado, mas se a CONTRATADA não for a titular da obrigação tributária correspondente, a CONTRATADA deverá comprovar, no momento da entrega, a aquisição do produto importado pelo contratado não importador, junto ao seu fornecedor, de modo a afastar sua responsabilidade pelos tributos de importação, considerando não ser sujeito passivo tributário.

3.3 Proposta Técnica

3.3.1 A licitante deverá apresentar Proposta Técnica, contendo a descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas.

3.3.2 Deverá ser fornecida pela licitante uma tabela com o número das páginas de sua proposta na qual contenha a comprovação do atendimento dos requisitos

exigidos.

3.3.3 Apresentar na proposta a indicação detalhada da solução ofertada citando, quando houver, a marca, modelo, tipo e fabricante.

3.3.4 A tabela de comprovação técnica é parte obrigatória da proposta comercial e deve ser apresentada conforme modelo abaixo. É necessária a especificação de **todos** os itens contidos neste Termo de Referência e no Edital e a apresentação da documentação comprobatória com indicação da página e com informações das funcionalidades e características exigidas grifadas. Salienta-se que todos os itens da tabela devem ser devidamente preenchidos.

3.3.5 A tabela de comprovação técnica deverá possuir, no mínimo, as informações e estrutura conforme:

Nº Requisito no TR	Descrição da característica ou funcionalidade exigida	Documento do fabricante (nome)	Página(s)	Atende ao Requisito (sim/não)

3.3.6 Serão considerados documentos oficiais para comprovação técnica: catálogos, folders, prospectos e manuais.

3.3.7 Para os documentos do fabricante, é mandatório a comprovação que se trata de documento oficial fornecido pelo fabricante ao mercado, sendo comprovação suficiente desse requisito o link para o acesso ao documento no site do fabricante.

3.3.8 Havendo divergência entra as características técnicas descritas na proposta da licitante e as disponibilizadas pelo fabricante, prevalecerão os informes do fabricante, salvo os casos específicos em que o licitante esclareça os motivos da divergência e que sejam aceitos pela CONTRATANTE.

3.3.9 Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela Licitante, no canto inferior direito.

3.3.10 Além da indicação da página da documentação fornecida na qual se encontra a comprovação de cada funcionalidade ou característica técnica exigida para cada item, a correspondente comprovação deverá ser necessariamente grifada ou destacada com marca texto.

3.3.11 A não apresentação de tabela de comprovação técnica ou apresentação de tabela divergente do exigido acarretará a desclassificação da licitante.

3.3.12 Caso haja dúvidas sobre a capacidade do produto ofertado atender ao exigido nas especificações técnicas, a equipe do Tribunal poderá exigir a comprovação da especificação em dúvida por meio de prova de conceito, que deverá ser realizada na infraestrutura do Tribunal e nas seguintes condições:

I. A licitante deverá apresentar, em até 1(um) dia útil, os requisitos para instalação da sua solução no ambiente do Tribunal;

II. A equipe do Tribunal disponibilizará, em até 1(um) dia útil, a infraestrutura necessária para a instalação da solução;

III. Caso os requisitos apresentados pela licitante sejam exagerados e em

desacordo com o exigido nas especificações técnicas, o item em dúvida será considerado como não atendido;

IV. A licitante terá até 3 (três) dias úteis para proceder com a instalação e a comprovação do(s) requisito(s) técnico(s) que levantaram dúvidas sobre a capacidade de atendimento;

V. Todo o procedimento deverá ser realizado de forma remota e demonstrado através de sala do Google Meet a ser fornecida pelo Tribunal.

3.3.13 Caso o fabricante da solução possua laboratório próprio, será facultado à Licitante oferecer a comprovação do requisito através desse laboratório, cabendo a equipe técnica do Tribunal avaliar se a comprovação desta forma é adequada ou se é necessário realizar a instalação nas dependências do Tribunal.

3.3.14 A CONTRATADA deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666/1993.

3.4 Da Qualificação Técnica

3.4.1 A qualificação técnica será comprovada mediante apresentação de, pelo menos, um atestado de capacidade técnica compatível com o objeto desta licitação, expedido por pessoa jurídica de direito público ou privado, em nome da licitante.

3.4.2 Para a solução do Grupo 01, serão considerados compatíveis com ao objeto da licitação atestados de capacidade técnica que comprovem a entrega dos mesmos produtos ofertados pela licitante.

3.4.3 Para a solução do Grupo 02, serão considerados compatíveis com ao objeto da licitação atestados de capacidade técnica que comprovem a entrega e serviço técnico especializado para soluções de PAM.

3.4.4 Poderá ser realizada DILIGÊNCIA para comprovar a autenticidade do(s) Atestado(s) de Capacidade Técnica.

3.6 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;

3.6.2.5.3 Deverá 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 passiveis 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. Operação prossegue 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.

3.6.7 **Grupo 01, Item 03 - Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.**

3.6.7.1 A instalação deverá ser realizada, preferencialmente, em ambiente virtual a ser fornecido pela CONTRATANTE.

3.6.7.2 A instalação deverá ser precedida de reunião de planejamento com a equipe da CONTRATADA e terá como resultado o plano de instalação, que deverá conter, no mínimo:

3.6.7.2.1 Detalhamento do Escopo;

3.6.7.2.2 Descrição de atividades em cada etapa do projeto;

3.6.7.2.3 Cronograma de atividades;

3.6.7.2.4 Definição de responsabilidades;

3.6.7.2.5 Pontos de controle;

3.6.7.2.6 Descrição detalhada dos componentes;

3.6.7.2.7 Requisitos necessários.

3.6.7.3 O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

3.6.7.4 O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

3.6.7.5 A instalação deverá estar em acordo com o especificado para a solução e não poderá acarretar acréscimos de custos de licenciamento para a CONTRATANTE.

3.6.7.6 Cabe a CONTRATADA entregar a equipe da CONTRATANTE o dimensionamento dos recursos computacionais para os servidores que irão suportar a solução.

3.6.7.7 O dimensionamento dos recursos computacionais deverá possuir respaldo na documentação oficial do fabricante da solução.

3.6.7.8 Deverão ser criados, a critério da CONTRATANTE, até 10 dashboards em acordo com o exigido nas especificações técnicas.

3.6.8 **Grupo 01, Item 04 - Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.**

3.6.8.1 O treinamento contemplará todos os *softwares* que compõem a solução.

3.6.8.2 O treinamento deverá ser realizado remotamente.

3.6.8.3 Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

3.6.8.4 O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

3.6.8.5 O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

3.6.8.6 A carga horária mínima exigida para este treinamento é de 30 horas.

3.6.8.7 A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.

3.6.8.8 Deverá ser ministrada uma turma de treinamento que terá até 10 participantes.

3.6.8.9 Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

3.6.8.10 Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o período de realização e o nome completo do participante.

3.6.8.11 O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

3.6.8.12 As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

3.6.8.13 O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

3.6.8.14 A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a CONTRATANTE.

3.6.8.15 Para ser considerado adequado, o treinamento deverá ser aprovado por pelo menos 70% dos participantes das turmas.

3.6.8.16 A avaliação dos treinamentos levará em consideração as questões listadas a seguir:

3.6.8.16.1 Avaliação do conteúdo:

3.6.8.16.1.1 Adequação dos conteúdos aos objetivos propostos;

3.6.8.16.1.2 Adequação das atividades desenvolvidas para alcance dos objetivos propostos;

3.6.8.16.1.3 Adequação do tempo para o alcance dos objetivos propostos;

3.6.8.16.1.4 Profundidade com que o conteúdo foi abordado, considerando os objetivos propostos;

3.6.8.16.1.5 Integração entre teoria, pesquisa, prática e/ou aspectos da realidade;

3.6.8.16.1.6 Qualidade dos exemplos utilizados;

3.6.8.16.1.7 Aplicabilidade dos conhecimentos adquiridos no trabalho;

3.6.8.16.1.8 Contribuição para melhoria do desempenho no trabalho;

3.6.8.16.1.9 Qualidade do material instrucional (apostilas, gráficos etc.).

3.6.8.16.2 Avaliação do instrutor:

3.6.8.16.2.1 Formas/métodos de apresentação dos conteúdos;

3.6.8.16.2.2 Conhecimento dos temas tratados;

3.6.8.16.2.3 Visão prática dos conteúdos tratados;

3.6.8.16.2.4 Uso de estratégias para motivar os alunos em relação ao conteúdo;

3.6.8.16.2.5 Incentivo à participação dos alunos em sala de aula;

3.6.8.16.2.6 Incentivo à realização de atividades adicionais de aprofundamento do aprendizado.

3.6.8.16.3 Avaliação de ambiente e recursos

3.6.8.16.3.1 Qualidade dos recursos tecnológicos utilizados pelo instrutor (áudio, vídeo, recursos para demonstração etc.);

3.6.8.16.3.2 Qualidade do ambiente virtual disponibilizado para o curso;

3.6.8.16.3.3 Qualidade da conexão disponibilizada pela CONTRATADA.

3.6.8.17 Cada participante deverá indicar uma nota de 1 a 10 para cada item e letra da avaliação.

3.6.8.18 A nota do treinamento será calculada pela média das respostas de todos os itens e letras, e de todos os participantes indicados.

3.6.8.19 O treinamento será considerado com qualidade suficiente, caso atinja uma nota igual ou superior a 7,5.

3.6.8.20 Para comprovação da nota do treinamento, deverá ser encaminhado o detalhamento do cálculo realizado pela CONTRATADA, juntamente com uma cópia dos formulários preenchidos pelos participantes.

3.6.8.21 Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da CONTRATADA, ela estará sujeita às sanções previstas neste termo de referência.

3.6.9 **Grupo 02, item 05 - Cluster para prover recursos para solução de acesso a usuários privilegiados**

3.6.9.1 Deverá ser composto por, no mínimo, dois servidores dedicados e físicos.

3.6.9.2 Deverá atender, sem perde de desempenho, a solução em sua capacidade máxima, considerando o licenciamento na maior quantidade suportada pela solução, ou seja, se a solução suportar 10.000 usuário privilegiados como sua capacidade máxima, o cluster deverá ser dimensionado para suportar essa capacidade. Essa regra é aplicável a todos os recursos que são licenciados.

3.6.9.3 Os equipamentos entregues deverão ser novos e de primeiro uso.

3.6.9.4 Deverá ser possível distribuir os nós do cluster entre *datacenters* distintos, ou seja, um nó em cada *datacenter*, sem que isso acarrete perda de funcionalidade ou desempenho. Para esse requisito ser atendido, as características mínimas de interconexão entre os dois *datacenters* deverão ser:

3.6.9.4.1 Interconectados por fibras apagadas, através de LAN estendida;

3.6.9.4.2 20Gbps de taxa de transferência na interconexão de LAN;

3.6.9.4.3 Distância máxima entre os dois sites de 1,8km.

3.6.9.5 Deverá ser específico para rack de 19 (dezenove) polegadas.

3.6.9.6 Deverá dispor de chaveamento automático de tensão (sem a necessidade e intervenção humana em chaves de troca de voltagem), considerando as faixas de 115 V a 230 V, com frequência de 50/60 Hertz.

3.6.9.7 Deverá possuir plena redundância, ou seja, funcionar em sem que haja qualquer ponto único de falha, seja na camada lógica (software) ou na camada física (hardware).

3.6.9.8 A solução deve poder ser configurada em cluster de contingência, alta disponibilidade (HA) e recuperação de desastres (DR).

3.6.9.9 A solução deverá continuar funcionando localmente mesmo com a falha de um nó de cada elemento.

3.6.9.10 O modelo mínimo de funcionamento e tolerância a falhas a ser implantado é:

3.6.9.10.1 Componentes principais: ativo/ativo ou ativo/passivo com *failover* automático;

3.6.9.10.2 Componentes secundários: ativo/ativo ou ativo/passivo com *failover* automático.

3.6.9.11 No caso de falha em um dos nós do cluster, o nó restante deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades.

3.6.10 **Grupo 02, Itens 07, 09, 11, 13, 15 ,17 e 19 – Licenças para contas para acesso privilegiados e licenças para ativos protegidos**

3.6.10.1 As licenças deverão ser totalmente compatíveis entre si.

3.6.10.2 Licenças deverão ser perpétuas com garantia e direito de atualização por, no mínimo, 12 meses.

3.6.10.3 Suportar, no mínimo, 8.000 sessões simultâneas;

3.6.10.4 Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências.

3.6.10.5 Suportar, no mínimo, a gravação de 8h horas por dia, 5 dias por semana, de vídeo com retenção de 90 dias para cada usuário privilegiado.

3.6.10.6 Armazenar os logs de acesso por, pelo menos, 90 dias.

3.6.10.7 Permitir o backup externo, criptografado, dos vídeos e logs de acesso dos usuários privilegiados.

3.6.10.8 Caso o quantitativo de ativos licenciados seja esgotado, a tentativa de acréscimo de mais ativos do mesmo tipo deverá gerar um alerta para o administrador, mas não poderá, em hipótese alguma, impedir o acréscimo e limitar o uso da solução.

3.6.10.9 A solução não deve limitar a quantidade de dispositivos controlados e deve ser capaz de lidar com, no mínimo, 15.000 dispositivos, sem perda de desempenho.

3.6.10.10 Prover autenticação transparente nas aplicações e sistemas-alvos. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso.

3.6.10.11 Eliminar credenciais inseridas em códigos-fonte, scripts e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e invisíveis aos desenvolvedores e equipe de suporte de TI.

3.6.10.12 Possuir banco de dados de uso exclusivo para evitar que informações sejam armazenadas em bancos de dados compartilhados.

3.6.10.13 Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos e aplicações.

3.6.10.14 Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa.

3.6.10.15 Integração com ferramentas de Service Desk e de Gestão Mudança com possibilidade de validação de critérios pré-definidos para liberação de acesso.

3.6.10.16 Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.

3.6.10.17 Oferecer interface com visão personalizada exclusiva para auditorias contendo os dispositivos e credenciais gerenciadas pela solução.

3.6.10.18 Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo.

3.6.10.19 Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata.

3.6.10.20 Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais.

3.6.10.21 Permitir o monitoramento on-line do uso das contas e desligamento da sessão.

3.6.10.22 Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade.

3.6.10.23 Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos.

3.6.10.24 Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão ou gerar alerta caso o usuário execute um comando indevido.

3.6.10.25 Permitir Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.

3.6.10.26 Possui configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado

3.6.10.27 Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato "csv".

3.6.10.28 Deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH, API REST HTTP/HTTPS.

3.6.10.29 Caso seja necessária alguma integração com aplicações legadas e/ou integrações com o ambiente interno, o mesmo deverá ser customizado pela CONTRATANTE em acordo com as possibilidades da solução contratada e sem que haja necessidade de desenvolvimento.

3.6.10.30 Extrair informações do servidor localizado nos Data Centers remotos caso seja necessário restaurar todas as configurações e os dados da solução de cofre de senhas.

3.6.10.31 A solução deve possuir ferramenta de monitoração para que seja possível especificar limiares (*threasholds*) referente ao uso de memória, CPU, disco e banco de dados, por exemplo.

3.6.10.32 Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperação de senhas no caso de falha total da solução.

3.6.10.33 Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local deve ser automaticamente replicada para os outros servidores de redundância.

3.6.10.34 Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (*Hash*) ou endereço IP do host ou conjunto de hosts a serem acessados pela solução.

3.6.10.35 Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS;

3.6.10.36 Implementar a especificação IETF RFC 2460, referente ao protocolo IPv6.

3.6.10.37 Implementar a MIB II conforme RFC 1213.

3.6.10.38 Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local.

3.6.10.39 Caso a solução seja separada em componentes, nenhum deles deve conter senhas em texto claro para autenticação.

3.6.10.40 Gerenciar chaves SSH e fazer Scan de servidores Linux e identificação e publicação de chaves SSH.

3.6.10.41 Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA.

3.6.10.42 Permitir a liberação de acesso para execução de tarefas específicas em plataforma SSH.

3.6.10.43 Toda a solução deverá ter seus componentes de hardware e sistema operacional “hardenizados” e protegidos com firewall interno e detecção de intrusão.

3.6.11 **Para as licenças de usuários privilegiados protegidos:**

3.6.11.1 A licença deve permitir a proteção de, no mínimo, os seguintes tipos de usuários privilegiados:

3.6.11.1.1 Administradores de sistemas Windows;

3.6.11.1.2 Usuário root de sistemas Linux;

3.6.11.1.3 Usuários de segurança de rede;

3.6.11.1.4 Usuários Domain Admin;

3.6.11.1.5 Usuários DBadmin;

3.6.11.1.6 Usuários SysDBA;

3.6.11.1.7 Usuários VMadmin;

3.6.11.1.8 Usuários de helpdesk;

3.6.11.1.9 Usuários com privilégio de administrador em qualquer tipo de ativo suportado.

3.6.11.2 O acesso dos usuários deve ser simultâneo.

3.6.12 **Para as licenças de ativos protegidos**

3.6.12.1 A licença deve permitir a proteção de, no mínimo, os seguintes tipos de ativos:

3.6.12.1.1 Estações de trabalho, seja desktop ou notebook, com os sistemas operacionais Windows;

3.6.12.1.2 Servidores físicos com sistema sistemas operacionais Linux, Windows Server e VMware ESXi;

3.6.12.1.3 Servidores virtuais com sistema sistemas operacionais Linux e Windows Server;

3.6.12.1.4 Storage com administração realizada aatrvés de protocolo SSH e http/https.

3.6.12.1.5 Equipamentos de rede como switches LAN;

3.6.12.1.6 Equipamentos de rede como AP Wi-Fi;

3.6.12.1.7 Controlador Wi-Fi com acesso via protocolos http/https e SSH;

3.6.12.1.8 Firewall de rede com acesso via protocolos http/https e SSH;

3.6.12.1.9 Aplicação que utiliza infraestrutura de container (aplicação conteineirizada) com *secrets;*

3.6.12.1.9.1 Cada licença de aplicação em container dever também ser licenciado, ao menos, duas licenças de *secrets.*

3.6.12.1.10 Aplicação não conteineirizadas com senha embutida no código (hard coded);

3.6.12.1.11 Instância de bancos de dados Oracle;

3.6.12.1.12 Instância de bancos de dados Microsoft SQL Server (MS SQL);

3.6.12.1.13 Instância de bancos de dados PostgreSQL;

3.6.12.1.14 Instância de bancos de dados MySql e MariaDB;

3.6.12.1.15 Instância de Elastic Search.

3.6.12.2 Caso o número de ativos protegidos pela solução ofertada seja ilimitado, a proponente deverá preencher os respectivos itens de licenças na tabela de precificação com o valor zero.

3.6.13 **Sobre a gestão de usuários e perfis.**

3.6.13.1 Cadastro de usuários com informações de nome e e-mail.

3.6.13.2 Cadastro de perfis de usuários.

3.6.13.3 Segregação de funções por perfis de acesso.

3.6.13.4 Flexibilidade para criação de quaisquer perfis novos, com diversas combinações de telas e funcionalidades de acordo com a necessidade do negócio sem intervenção do fornecedor.

3.6.13.5 Importação automática de contas de usuários do diretório Microsoft Active Directory (AD) ou outra diretório que utilize o protocolo LDAP.

3.6.13.6 Gerenciamento de Grupos e Perfis de acesso integrados aos grupos do AD e LDAP.

3.6.13.7 Autenticação de usuários deve realizar, no mínimo:

3.6.13.7.1 Autenticação local através de usuários e senha;

3.6.13.7.2 Autenticação centralizada integrada com LDAP, LDAPS e MS AD com múltiplos DCS;

3.6.13.7.3 Autenticação centralizada integrada com RADIUS;

3.6.13.7.4 Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores;

3.6.13.7.5 Duplo fator de autenticação nativo para acesso web ou através de cliente;

3.6.13.7.6 Gestão de autenticação com múltiplos autenticadores simultaneamente.

3.6.14 **Sobre o cadastro de ativos.**

3.6.14.1 Deve realizar descoberta (*scan*) automática de servidores Linux e identificação de chaves SSH.

3.6.14.2 Deve permitir cadastro de equipamentos parametrizado manualmente.

3.6.14.3 Deve possui, no mínimo, atributos de ativos tais como marca, modelo, fabricante, localidade e informações que podem ser parametrizados pelo administrador da ferramenta.

3.6.14.4 Possuir *discovery* automatizado de credencias em servidores e bancos de dados.

3.6.15 **Sobre cofre de credenciais.**

3.6.15.1 As senhas armazenadas devem ser criptografadas com padrões de criptografias fortes como AES 256 ou superior.

3.6.15.2 Deve realizar consolidação periódica de senhas para identificar senhas que foram alteradas em sistemas gerenciados. A consolidação deverá ser feita de forma automática ou por meio de relatórios.

3.6.15.3 Deve envio de alerta por SIEM de senhas que não estejam iguais ao cofre.

3.6.16 **Sobre cofre de informações privilegiadas.**

3.6.16.1 Deve realizar o armazenamento de senhas pessoais.

3.6.16.2 Deve permitir alertas de vencimento das informações armazenadas.

3.6.16.3 Possuir *logs* de alteração de informações privilegiadas.

3.6.17 **Sobre o compartilhamento de vídeo sem download com fluxo dentro da ferramenta.**

3.6.17.1 Permissão para compartilhamento de informações com outros usuários.

3.6.17.2 Gravação de logs (vídeos e comandos).

3.6.17.3 Gravação de vídeo das sessões realizadas através de *web proxy* ou *proxy* transparente em formato otimizado.

3.6.17.4 Gravação de comandos digitados em ambientes RDP e SSH.

3.6.17.5 Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download.

3.6.17.6 Possuir proxy transparente com gravação de logs e vídeos ao sistema alvo sem revelar aos usuários as credenciais utilizadas através cliente local utilizado pelo usuário como Putty, ou RDP Client, sem necessidade de abrir interface web ou baixar nenhum cliente adicional na máquina do usuário.

3.6.17.7 Permitir exportação de sessão em formato vídeo.

3.6.17.8 Busca de registro de sessão por usuário, sistema alvo, ip alvo, data e hora.

3.6.17.9 Busca por comandos e entradas de teclado digitados em plataforma Linux e Windows.

3.6.17.10 Gravação de Logs de Input e Output de comandos sem necessidade de agentes locais para gravação de sessão;

3.6.17.11 Deve realizar o armazenamento e consulta de logs que forneçam ao menos, as seguintes informações:

3.6.17.11.1 Identificação do usuário que realizou determinado acesso a um dispositivo;

3.6.17.11.2 Identificação de quem aprovou o acesso do usuário;

3.6.17.11.3 Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto;

3.6.17.11.4 Prover, ao menos, os seguintes filtros para a recuperação de logs: Usuário; Sistema-alvo acessado, Tipo de atividade, Intervalo de tempo (data/hora/minuto inicial e final);

3.6.17.11.5 Permitir o acompanhamento on-line de sessões remotas pelo administrador e desligamento da sessão remotamente.

3.6.18 **Sobre o bloqueio de comandos e controle de privilégios.**

3.6.18.1 Permitir bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução.

3.6.18.2 Possibilidade de bloqueio e auditoria de comandos específicos.

3.6.18.3 Interface para acesso via RDP a aplicações locais com gravação de sessão.

3.6.18.4 No caso de acesso a aplicação remota (*Remote App*) ao fechar a aplicação a sessão do usuário deve ser encerrada.

3.6.18.5 Permitir a busca por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.

3.6.18.6 Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado.

3.6.19 **Sobre rotação de senhas**

3.6.19.1 Troca automática de senhas para os tipos de ativos protegidos.

3.6.19.2 Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da instituição.

3.6.19.3 Flexibilidade para configuração de força de senha gerada.

3.6.19.4 Permitir a liberação de acesso para execução de tarefas específicas em plataforma SSH.

3.6.19.5 Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.

3.6.19.6 Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado.

3.6.19.7 Armazenamento de histórico de senhas por equipamento.

3.6.19.8 Registro de troca executadas.

3.6.19.9 Relatório de acompanhamento de trocas.

3.6.19.10 Relatório de erros de trocas.

3.6.19.11 Alertas de falha ou sucesso de trocas.

3.6.19.12 *Templates* abertos e configuráveis para criação de *booking* para execução de comandos específicos, conforme perfil do usuário ou grupo de usuários.

3.6.19.13 Cadastrar automaticamente chaves públicas das chaves SSH em servidores autorizados.

3.6.19.14 Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca.

3.6.19.15 Disponibilizar os *Templates* de troca de senha de forma que possam ser abertos, editáveis e auditáveis.

3.6.19.16 Possuir fluxo de aprovação de alteração de *Template* para evitar fraudes.

3.6.19.17 Rastreabilidade de Alteração de *Template*.

3.6.19.18 Troca de senhas em aplicações HTTP/HTTPS através de *Templates*.

3.6.20 **Sobre análise de comportamento.**

3.6.20.1 Realizar análise de sessão de usuário baseado em histórico de comportamento. Análise mínima das variáveis de estações origem, estações destino, credenciais, horários e duração de sessão.

3.6.20.2 Identificação de comportamento diferenciados com alertas de anormalidade em relatórios em tela ou alertas para SIEM/SYSLOG.

3.6.20.3 Análise de sessão de usuários a fim de apresentar comando críticos com alertas de anormalidade em relatórios em tela ou alertas para SIEM/SYSLOG.

3.6.20.4 Possuir dashboards gráficos com informações sobre riscos e ameaças.

3.6.21 **Sobre *dashboards* e relatórios a solução deve possuir:**

3.6.21.1 Relatórios de operação com lista e usuários cadastrados, equipamentos cadastros, credenciais cadastradas;

3.6.21.2 Relatórios PCI;

3.6.21.3 Relatórios de Gestão de Evidências;

3.6.21.4 Relatórios de Auditoria;

3.6.21.5 Relatórios de Alertas;

3.6.21.6 Exportação para Excel (.csv);

3.6.21.7 Dashboard de utilização;

3.6.21.8 Dashboard de conexões;

3.6.21.9 Dashboard de utilização de sessões;

3.6.21.10 Dashboard de sessão;

3.6.21.11 Dashboard de usuário;

3.6.21.12 Dashboard de servidor.

3.6.22 **Sobre a central gerenciamento.**

3.6.22.1 Console central de gerenciamento de aplicação com capacidade para:

3.6.22.1.1 Suporte à utilização de certificados digitais válidos pela ICP-Brasil, certificados digitais internacionais e certificados auto assinados gerados pela própria solução;

3.6.22.1.2 Criação de usuários;

3.6.22.1.3 Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download;

3.6.22.1.4 Busca de sessões gravadas;

3.6.22.1.5 Possibilidade de sessão remota através dos protocolos SSH e RDP ou programa cliente instalado na estação de trabalho do usuário sem a necessidade de passar por aplicação web ou baixar nenhum cliente adicional na máquina do usuário;

3.6.22.1.6 Permitir a busca por senhas que foram trocadas em momento anterior;

3.6.22.1.7 Gestão de políticas de acesso centralizadas;

3.6.22.1.8 Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores;

3.6.22.1.9 Cadastro de dispositivos centralizados.

3.6.23 **Grupo 02, itens 06, 08, 10, 12, 14, 16, 18 e 20 – Garantia do fabricante.**

3.6.23.1 As garantias fornecidas pelo fabricante deverão ser por todo período mínimo de 12 meses.

3.6.23.2 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.

3.6.23.3 Define-se garantia do fabricante como sendo serviço efetuado mediante abertura de chamado junto ao 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 sobre configuração, uso e atualização dos produtos. Também faz parte da garantia o fornecimento de qualquer atualização de versão das licenças, sejam elas corretivas, evolutivas ou de outra natureza, durante a vigência da garantia.

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

3.6.23.5 O fabricante 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.

3.6.23.6 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. Operação prossegue 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

3.6.23.7 O nível de severidade dos chamados deverá ser comunicado ao Fabricante pela CONTRATANTE no momento de sua abertura.

3.6.23.8 O início do atendimento dos chamados técnicos de nível de severidade 1 deverá ser iniciado em até 1 (uma) hora; os de nível de severidade 2, em até 2 (duas) horas, os de nível de severidade 3 em até 8 (oito) horas e o de nível de severidade 4 em até 12 (doze) horas.

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

3.6.24 **Grupo 02, item 21 - Serviço de instalação para solução de controle de acesso de usuários privilegiados.**

3.6.24.1 A instalação deverá ser precedida de reunião de planejamento com a equipe da CONTRATADA e terá como resultado o plano de instalação, que deverá conter, no mínimo:

3.6.24.1.1 Detalhamento do Escopo;

3.6.24.1.2 Descrição de atividades em cada etapa do projeto;

3.6.24.1.3 Cronograma de atividades;

3.6.24.1.4 Definição de responsabilidades;

3.6.24.1.5 Pontos de controle;

3.6.24.1.6 Descrição detalhada dos componentes;

3.6.24.1.7 Documentação a ser entregue, incluindo todos os detalhes das instalações a serem realizadas onde deverá apresentar informações para procedimentos, incluindo comandos e testes aplicáveis, procedimentos de inicialização e procedimentos de configuração;

3.6.24.1.8 Requisitos necessários.

3.6.24.2 O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

3.6.24.3 O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

3.6.24.4 Eventuais ajustes no cabeamento elétrico, como troca do tipo de tomada, é de responsabilidade da CONTRATADA e não poderá gerar custos a CONTRATANTE.

3.6.24.5 A instalação deverá estar em acordo com o especificado para a solução e não poderá acarretar acréscimos de custos de licenciamento para a CONTRATANTE.

3.6.24.6 Caso seja necessário efetuar ajustes no equipamento para compatibilizar com a infraestrutura da CONTRATANTE, esses ajustes deverão ser feitos pela CONTRATADA sem ônus para a CONTRATANTE.

3.6.24.7 Caberá a CONTRATADA, na fase de instalação, realizar as devidas configurações para que os ativos licenciados sejam protegidos conforme o quantitativo de licenças contratadas, sendo eles do tipo:

3.6.24.7.1 Servidores físicos e virtuais (Linux, Windows e Storages);

3.6.24.7.2 Estações de trabalho Windows;

3.6.24.7.3 Equipamentos de conectividade de Rede, VOIP e Segurança-LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP);

3.6.24.7.4 Instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL).

3.6.25 **Grupo 02, item 22 - Treinamento para solução de controle de acesso de usuários privilegiados.**

3.6.25.1 O treinamento deverá ser precedido de reunião de planejamento com a equipe da CONTRATANTE.

3.6.25.2 O treinamento contemplará todos os softwares e hardwares que compõem a solução.

3.6.25.3 O treinamento deverá ser realizado remotamente.

3.6.25.4 Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

3.6.25.5 O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

3.6.25.6 O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

3.6.25.7 A carga horária mínima exigida para este treinamento é de 30 horas.

3.6.25.8 A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.

3.6.25.9 Deverá ser ministrada uma turma de treinamento que terá até 10 participantes.

3.6.25.10 Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

3.6.25.11 Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o período de realização e o nome completo do participante.

3.6.25.12 O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

3.6.25.13 As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

3.6.25.14 O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

3.6.25.15 A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a CONTRATANTE.

3.6.25.16 Para ser considerado adequado, o treinamento deverá ser aprovado por pelo menos 70% dos participantes das turmas.

3.6.25.17 A avaliação dos treinamentos levará em consideração as questões listadas a seguir:

3.6.25.17.1 Avaliação do conteúdo:

3.6.25.17.1.1 Adequação dos conteúdos aos objetivos propostos;

3.6.25.17.1.2 Adequação das atividades desenvolvidas para alcance dos objetivos propostos;

3.6.25.17.1.3 Adequação do tempo para o alcance dos objetivos propostos;

3.6.25.17.1.4 Profundidade com que o conteúdo foi abordado, considerando os objetivos propostos;

3.6.25.17.1.5 Integração entre teoria, pesquisa, prática e/ou aspectos da realidade;

3.6.25.17.1.6 Qualidade dos exemplos utilizados;

3.6.25.17.1.7 Aplicabilidade dos conhecimentos adquiridos no trabalho;

3.6.25.17.1.8 Contribuição para melhoria do desempenho no trabalho;

3.6.25.17.1.9 Qualidade do material instrucional (apostilas, gráficos etc.).

3.6.25.17.2 Avaliação do instrutor:

3.6.25.17.2.1 Formas/métodos de apresentação dos conteúdos;

3.6.25.17.2.2 Conhecimento dos temas tratados;

3.6.25.17.2.3 Visão prática dos conteúdos tratados;

3.6.25.17.2.4 Uso de estratégias para motivar os alunos em relação ao conteúdo;

3.6.25.17.2.5 Incentivo à participação dos alunos em sala de aula;

3.6.25.17.2.6 Incentivo à realização de atividades adicionais de aprofundamento do aprendizado.

3.6.25.17.3 Avaliação de ambiente e recursos:

3.6.25.17.3.1 Qualidade dos recursos tecnológicos utilizados pelo instrutor (áudio, vídeo, recursos para demonstração etc.);

3.6.25.17.3.2 Qualidade do ambiente virtual disponibilizado para o curso;

3.6.25.17.3.3 Qualidade da conexão disponibilizada pela CONTRATADA.

3.6.25.18 Cada participante deverá indicar uma nota de 1 a 10 para cada item e letra da avaliação.

3.6.25.19 A nota do treinamento será calculada pela média das respostas de todos os itens e letras, e de todos os participantes indicados.

3.6.25.20 O treinamento será considerado com qualidade suficiente, caso atinja uma nota igual ou superior a 7,5.

3.6.25.21 Para comprovação da nota do treinamento, deverá ser encaminhado o detalhamento do cálculo realizado pela CONTRATADA, juntamente com uma cópia dos formulários preenchidos pelos participantes.

3.6.25.22 Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da CONTRATADA, ela estará sujeita às sanções previstas neste termo de referência.

3.6.26 **Grupo 02, item 23 – Serviço e suporte técnico especializado.**

3.6.26.1 Deverá ser prestado suporte técnico e manutenção pela CONTRATADA por todo período mínimo de 12 meses.

3.6.26.2 Define-se serviço de suporte técnico sendo aquele efetuado mediante abertura de chamado junto à CONTRATADA, 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.

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

3.6.26.4 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.

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

3.6.26.6 Caberá a CONTRATADA realizar a manutenção evolutiva dos *softwares* da solução, fornecendo, instalando e configurando as novas versões e/ou releases e atualizações lançadas durante a vigência da garantia, mantendo-os funcionais e compatíveis com o ambiente utilizado pela CONTRATANTE.

3.6.26.7 A CONTRATADA deverá garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços, configurações e fornecimento "fixes" e "releases", durante toda a vigência da garantia.

3.6.26.8 Executar, durante o período de vigência da garantia, suporte preventivo e corretivo da solução objeto do contrato, para as seguintes atividades:

3.6.26.8.1 Parametrização e auditoria técnica de disponibilidade e funcionamento da solução;

3.6.26.8.2 Manutenção e suporte a todo o ambiente de software básico da solução, atuando em casos de incidentes escalonados pela equipe técnica do CONTRATANTE, mediante identificação da causa raiz do problema, definição e implantação da solução de contorno para garantir o nível de disponibilidade do ambiente, aplicação da solução definitiva;

3.6.26.8.3 Promover o escalonamento dos incidentes e problemas graves ou de solução que demore mais tempo que o previsto contratualmente ao suporte especializado do fabricante, para rápida normalização do ambiente;

3.6.26.8.4 Relatar e implementar melhorias, atualizações e ajustes finos para aprimorar a solução de proteção de dados.

3.6.26.8.4.1 As implementações deverão ser fruto de análise das atualizações e correções disponibilizadas pelo fabricante, da análise do ambiente e do conjunto de melhores práticas para o ambiente;

3.6.26.8.4.2 As implementações deverão ser planejadas, detalhadas em atividades, com análise dos riscos e impacto no ambiente e de indicação de benefícios para sua execução.

3.6.26.8.5 Ações de aperfeiçoamento de funcionalidade, disponibilidade e configuração dos produtos da solução;

3.6.26.8.6 Execução de procedimentos de instalação em conformidade com as recomendações do fabricante, documentações existentes e as boas práticas de mercado;

3.6.26.8.7 Execução dos procedimentos descritos na documentação e proposições para a melhoria contínua desses procedimentos;

3.6.26.8.8 Suporte, configuração, customização, parametrização e implantação de sistemas auxiliares, visando manter a disponibilidade e o desempenho da solução;

3.6.26.8.9 Análise e proposição de soluções adequadas para o ambiente contratado, sob orientação da equipe técnica do CONTRATANTE;

3.6.26.8.10 Detecção, análise e resolução dos problemas de funcionalidade, configuração e parametrização, atuando preventivamente para evitar ocorrência de incidentes, identificação de pontos de falhas,

análise de potenciais de riscos da infraestrutura de backup e identificação de tendências de capacidade e disponibilidade do ambiente de backup;

3.6.26.8.11 Análise de "logs" e registros dos equipamentos, ferramentas e softwares envolvidos na solução, com anotações e geração de relatórios estatísticos;

3.6.26.8.12 Geração de relatórios de ocorrências para todas as falhas de serviços classificados pelo CONTRATANTE como críticos, com informações de causa e efeito, providências e correções aplicadas e recomendações sobre as lições aprendidas;

3.6.26.9 A CONTRATADA deverá realizar manutenção preventiva programada, que se destina a prevenir indisponibilidades e/ou falhas dos componentes da solução contratada, em suas instalações, subsistemas e componentes envolvidos, mantendo-as em perfeito estado de funcionamento e conservação, conforme especificado em projeto, manuais e normas técnicas específicas.

3.6.26.9.1 A manutenção preventiva programada deverá ser realizada mediante visita mensal da CONTRATADA, visando analisar desempenho e funcionalidade da solução, emitindo relatório mensal de serviços e resultados, com as sugestões de melhoria possíveis, visando garantir melhor performance da solução e segurança cibernética das credenciais.

3.6.26.9.2 A manutenção preventiva programada deverá ser realizada, preferencialmente, de forma remota, salvo quando houver impossibilidade técnica de acesso ao ambiente da CONTRATANTE.

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

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

3.6.26.12 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. Operação prossegue 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

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

3.6.26.14 O início do atendimento dos chamados técnicos de nível de severidade 1 deverá ser iniciado em até 1 (uma) hora; os de nível de

severidade 2, em até 2 (duas) horas, os de nível de severidade 3 em até 8 (oito) horas e o de nível de severidade 4 em até 12 (doze) horas.

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

Nível de severidade	Período máximo para solução
1	24 horas
2	36 horas
3	48 horas úteis
4	72 horas úteis

3.6.26.16 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.

3.6.26.17 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.

3.6.26.18 A CONTRATANTE poderá CONTRATADA deverá ser realizado suporte proativo, a critério da CONTRATANTE,

3.6.26.19 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.

3.6.26.20 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.

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

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

3.7 Vigência

3.7.1 O contrato terá vigência de 12 (doze) meses a partir do recebimento definitivo do produto, podendo ser prorrogado por iguais e sucessivos períodos até o máximo de 60 (sessenta) meses, conforme dispões o inciso II do art. 57 da Lei 8.666/1993.

3.7.2 Para o Grupo 01, a prorrogação é referente apenas aos itens 01 e 02.

3.7.3 Para o Grupo 02, a prorrogação contratual é referente apenas aos itens 06, 08, 10, 12, 14, 16, 18, 20 e 23.

3.7.4 A vigência das garantias dos objetos descritos nos itens 01 e 02 do Grupo 1 e dos itens 06, 08, 10, 12, 14, 16, 18 e 20 do Grupo 02 terão prazo de início a contar do termo de aceite definitivo, conforme regras de cada item.

3.8 Prazos de execução

3.8.1 O prazo para a entrega dos objetos será, conforme:

3.8.1.1 **Grupo 01, itens 01 e 02** – em até 5 (cinco) dias úteis após a assinatura do contrato;

3.8.1.2 **Grupo 01, item 03** – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação;

3.8.1.3 **Grupo 01, item 04** – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento;

3.8.1.4 **Grupo 02, itens 05 a 20 e item 23** – em até 45 (quarenta e cinco) dias após a assinatura do contrato;

3.8.1.5 **Grupo 02, item 21** – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação;

3.8.1.6 **Grupo 02, item 22** – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento;

3.8.2 As reuniões de planejamento da instalação e de treinamento previstas para os itens 03 e 04 do Grupo 01 e itens 21 e 22 do Grupo 02, deverão ser realizadas em até 10 dias após a assinatura do contrato, a critério da CONTRATANTE.

3.8.3 Após a reunião de planejamento da instalação, deverá ser apresentado o plano de instalação em até 15 dias corridos após a reunião de planejamento.

3.8.4 Os objetos deverão ser entregues na Coordenadoria de Infraestrutura Tecnológica, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, Sala A2.32, Brasília-DF, CEP 70.070-943, fones: (061) 3043-3035. E-mail de contato: citec@tst.jus.br.

3.8.5 A seu critério, a CONTRATANTE poderá suspender a execução de prazos associados a instalação e ao treinamento e restabelecê-los em momento oportuno.

3.8.6 Na contagem dos prazos previstos neste documento, excluir-se-á o dia de início e incluir-se-á o dia do vencimento. Só se iniciam e vencem os prazos em dias úteis e de expediente no Tribunal Superior do Trabalho.

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

3.8.8 Havendo pedido de prorrogação do prazo de entrega, este somente será concedido nas hipóteses previstas no Art. 57, §1°, da Lei nº 8.666/93, em caráter excepcional e sem efeito suspensivo, e deverá ser encaminhado por

escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela CONTRATADA.

3.8.9 O eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, Sala 18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4165, (061) 3043-4096, e-mail: sgcon@tst.jus.br.

3.8.10 Em casos excepcionais, autorizados pelo CONTRATANTE, o documento comprobatório do alegado poderá acompanhar a entrega do produto.

3.9 Fiscalização

3.9.1 Os produtos e serviços objetos desta contratação serão fiscalizados por servidor ou comissão de servidores do CONTRATANTE, doravante denominados Fiscalização, que terá autoridade para exercer toda e qualquer ação de orientação geral, controle e fiscalização da execução contratual.

3.9.2 À Fiscalização compete, entre outras atribuições:

3.9.2.1 Solicitar à CONTRATADA e seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento da garantia e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências;

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

3.9.2.3 Acompanhar e atestar a prestação dos serviços contratados e indicar a ocorrência de inconformidade desses serviços ou não cumprimento da garantia;

3.9.2.4 Encaminhar à Secretaria de Administração os documentos para exame e deliberação sobre a possível aplicação de sanções administrativas;

3.9.2.5 A ação da Fiscalização não exonera a CONTRATADA de suas responsabilidades contratuais.

3.10 Recebimento do objeto

3.10.1 Em conformidade com os artigos 73 a 76 da Lei n.º 8.666/93, cada item do objeto deste contrato será aceito conforme:

3.10.1.1 **Grupo 01, itens 01 e 02** - Provisoriamente 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;

3.10.1.2 **Grupo 01, item 03** - Provisoriamente imediatamente depois da conclusão do serviço. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

3.10.1.3 **Grupo 01, item 04** - Provisoriamente imediatamente depois da conclusão do treinamento. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

3.10.1.4 **Grupo 02, itens 05 a 20** - Provisoriamente imediatamente depois de efetuada a entrega dos equipamentos e licenças, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a conclusão da instalação;

3.10.1.5 **Grupo 02, item 21** - Provisoriamente imediatamente depois da conclusão do serviço. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

3.10.1.6 **Grupo 02, item 22** - Provisoriamente imediatamente depois da conclusão do treinamento. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

3.10.1.7 **Grupo 02, item 23** - Provisoriamente, mediante Termo Circunstanciado, imediatamente após cada serviço, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo Circunstanciado, em até 10 (dez) dias úteis, condicionado a apresentação da nota fiscal e a verificação da perfeita execução das obrigações contratuais.

3.10.2 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.).

3.10.3 Após o recebimento provisório, a fiscalização avaliará as características do objeto, identificando eventuais problemas. Estando em conformidade, será efetuado o Recebimento Definitivo.

3.10.4 Se, após o aceite provisório, constatar-se que o objeto foi entregue em desacordo com este contrato ou com a proposta, com incorreção, ou incompleto, serão interrompidos os prazos de recebimento e suspenso o pagamento, após a notificação por escrito à CONTRATADA e até que seja sanada a situação.

3.10.5 Os objetos entregues em desacordo com o especificado neste Termo de Referência, no Instrumento Convocatório, no Contrato ou com defeito serão rejeitados parcial ou totalmente, conforme o caso, e a CONTRATADA será obrigada a substituí-los dentro do prazo da garantia, sob pena de se considerar atraso na entrega.

3.10.6 A CONTRATADA ficará obrigada a trocar, a suas expensas, o material que vier a ser recusado.

3.10.7 A CONTRATADA deverá retirar o material recusado no momento da entrega do material correto. A CONTRATANTE não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo.

3.10.8 Será considerado abandonado o material que não for recolhido pela CONTRATADA em até 30 dias após a comunicação da equipe da CONTRATANTE à CONTRATADA.

3.10.9 A Administração poderá dar a destinação que julgar conveniente ao material abandonado em suas dependências.

3.10.10 A CONTRATADA deverá entregar todo o material discriminado na nota de empenho, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento da obrigação.

3.10.11 Independentemente da aceitação, a CONTRATADA garantirá a qualidade de cada unidade do produto fornecido pelo prazo estabelecido nas especificações, obrigando-se a reparar aquela que apresentar defeito no prazo estabelecido pelo CONTRATANTE.

3.10.12 O aceite provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato e da garantia, dentro dos limites estabelecidos pela lei ou por este instrumento.

3.11 Pagamento

3.11.1 O pagamento será efetuado, conforme:

3.11.1.1 **Para todos os itens do Grupo 1** – em parcela única e 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.

3.11.1.2 **Para os itens 5 a 22 do Grupo 2** – em parcela única e 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.

3.11.1.3 **Para o item 23 do Grupo 2 –** mensalmente e em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo através do Termo Circunstanciado, mediante atesto da nota fiscal e verificação perfeita das execuções contratuais pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

3.11.2 A nota fiscal deverá corresponder ao objeto fornecido e aos respectivos valores consignados na nota de empenho, e o CONTRATANTE, no caso de divergência, especialmente quando houver entrega parcial, notificará a CONTRATADA a substituí-la em até três dias úteis, com suspensão do prazo de pagamento.

3.11.3 As notas fiscais e os documentos exigidos no edital e no contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística, situada no SAFS, Quadra 8, Conjunto A, Bloco A, Subsolo, Brasília-DF, telefone (61) 3043-4095, ou encaminhado ao e-mail sgcon@tst.jus.br.

3.11.4 Durante o período da pandemia, enquanto perdurarem as medidas adotadas pelo Tribunal Superior do Trabalho quanto ao isolamento social devido à pandemia de COVID-19:

3.11.4.1 Os documentos indicados no subitem **3.11.3** deverão ser encaminhados exclusivamente ao e-mail sgcon@tst.jus.br;

3.11.4.2 As entregas onde hardware deverão necessariamente ser agendadas pelo e-mail scmat@tst.jus.br.

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

3.12 Sanções

3.12.1 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 neste edital e das demais cominações legais, aquele que:

3.12.1.1 não assinar o contrato ou ata de registro de preços;

3.12.1.2 não entregar a documentação exigida no edital;

3.12.1.3 apresentar documentação falsa;

3.12.1.4 causar o atraso na execução do objeto;

3.12.1.5 não mantiver a proposta;

3.12.1.6 falhar ou fraudar na execução contratual;

3.12.1.7 comportar-se de modo inidôneo;

3.12.1.8 declarar informações falsas; e

3.12.1.9 cometer fraude fiscal.

3.12.2 No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com a CONTRATANTE, as sanções administrativas aplicadas à CONTRATADA serão:

3.12.2.1 Advertência;

3.12.2.2 Multa;

3.12.2.3 Suspensão temporária de participar de licitações e impedimento de contratar com o Tribunal Superior do Trabalho;

3.12.2.4 Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

3.12.3 O atraso injustificado na entrega do objeto ou na execução da garantia sujeitará a aplicação de multa correspondente a 1% (um por cento) por dia de atraso a partir do 1º (primeiro) dia útil após a data fixada, até o percentual máximo de 30% (trinta por cento) do valor do contrato, caracterizando, neste caso, a inexecução total da obrigação, punível com as sanções previstas nos itens **3.12.2.3** e **3.12.2.4.**

3.12.4 No caso de atraso no cumprimento do prazo de assinatura da ata de registro de preços ou da retirada da nota de empenho, será aplicada multa de 0,5% (cinco décimos por cento) ao dia sobre o valor total adjudicado, até o limite de 15% (quinze por cento).

3.12.5 Para os itens do Grupo 01, 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.

3.12.6 Para os itens do Grupo 02, 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.

3.12.7 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).

3.12.8 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).

3.12.9 A CONTRATADA deverá justificar fundamentada, prévia e formalmente qualquer ocorrência que a leve a descumprir os deveres estabelecidos neste Termo. A aceitação da justificativa ficará a critério do CONTRATANTE.

3.12.10 As multas porventura aplicadas serão descontadas da garantia ofertada ou cobradas diretamente da CONTRATADA, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

3.12.11 As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

3.12.12 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.

3.12.13 O eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, térreo, sala T-18, Brasília-DF, CEP 70.070-943, fones: (61) 3043-4165, (61) 3043-7570 e-mail: sgcon@tst.jus.br.

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

3.13 Demais disposições

3.13.1 É de responsabilidade da CONTRATADA o conhecimento das características do material relacionado no objeto desta licitação.

3.13.2 A CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para terceiros, sejam fabricantes, representantes ou quaisquer outros.

Brasília, 20 de outubro de 2021.

Integrante Demandante	Integrante Técnico	Integrante Administrativo
Leonardo Lobo Pulcineli **Matrícula: c042780**	**Adriano Bontempo da Silva Martinho** **Matrícula: 39337**	**Aluísio Ferreira Leite** **Matrícula: 45503**

Equipe de Planejamento e Apoio à Contratação

Poder Judiciário
Justiça do Trabalho
Tribunal Superior do Trabalho

CONTRATO PE-058/2021 – AQUISIÇÃO DE SOLUÇÕES DE SEGURANÇA, AUDITORIA E PREVENÇÃO DE AMEAÇAS. (Processo TST N.º 6001640/2021-00).

O **TRIBUNAL SUPERIOR DO TRABALHO**, inscrito no CNPJ/MF sob o n.º 00.509.968/0001-48, sediado no Setor de Administração Federal Sul, quadra 8, conjunto A, Brasília, DF, CEP 70070-943, telefone geral (61) 3043-4300, doravante denominado simplesmente **CONTRATANTE**, neste ato representado pelo ....., ..., e a empresa **XXXXXXXXX**, inscrita no CNPJ/MF sob o n.º ....., com sede na ....., Brasília, DF, CEP ....., telefone (xx) ....., e-mail ....., doravante denominada simplesmente **CONTRATADA**, neste ato representada pelo ....., ..., considerando o julgamento do Pregão Eletrônico n.º 058/2021, publicado no Diário Oficial da União do dia xx de xxxxxxx de xxxx, e a respectiva homologação, que consta no Processo Administrativo TST n.º 6001640/2021-00, celebram o presente contrato, observando-se as normas constantes na 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, e ainda, mediante as cláusulas a seguir enumeradas.

CLÁUSULA PRIMEIRA - DO OBJETO

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 estruturados, abrangendo centro de dados e *endpoint*.	Usuários			
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	Usuários			

MINUTA

	estruturados.				
3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.	Serviço			
4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint.*	Turma			
5	*Cluster* para prover recursos para solução de acesso a usuários privilegiados	Cluster			
6	Garantia do fabricante por período de 12 meses para *cluster* para prover recursos para solução de acesso a usuários privilegiados	Cluster			
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)	Usuários			
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)	Usuários			
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores			
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores			
11	Licença para estações de trabalho Windows	Estações			
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações			
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos			
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos			
15	Licença para aplicações conteinerizadas com secrets	Aplicações			

MINUTA

16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets	Aplicações			
17	Licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações			
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações			
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias			
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias			
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	Serviço			
22	Treinamento para solução de controle de acesso de usuários privilegiados.	Turma			
23	Serviço e suporte técnico especializado	Mês			

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

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

CLÁUSULA SEGUNDA - DA VIGÊNCIA

O prazo de vigência deste contrato é de 12 (doze) meses, contados da data da sua assinatura, e, para os itens 01, 02, 06, 08, 10, 12, 14, 16, 18, 20 e 23, 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.

Subcláusula primeira. 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.

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

Subcláusula terceira. 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.

MINUTA

Subcláusula quarta. 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.

Subcláusula quinta. 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.

CLÁUSULA TERCEIRA - DO VALOR

O valor total deste contrato é de R$ ..... (.....).

Subcláusula única. 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.

CLÁUSULA QUARTA - DO REAJUSTE

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:

$R = \frac{I - Io}{Io} * P$, 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.

Subcláusula primeira. 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.

MINUTA

Subcláusula segunda. Na hipótese de sobrevirem fatos imprevisíveis ou impeditivos da execução do ajustado, poderá ser admitida a revisão do valor pactuado, objetivando manter o equilíbrio econômico-financeiro inicial do contrato.

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

CLÁUSULA QUINTA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas oriundas deste contrato correrão à conta dos recursos orçamentários consignados ao Contratante, programa de trabalho ....., elemento de despesa ....., nota de empenho ....., emitida em ...../...../.....

CLÁUSULA SEXTA – DOS PRAZOS

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. item 03 – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação;

III. item 04 – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento;

IV. itens 05 a 20 e item 23 – em até 45 (quarenta e cinco) dias após a assinatura do contrato;

V. item 21 – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação;

VI. item 22 – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento;

VII. As reuniões de planejamento da instalação e de treinamento previstas para os itens 03, 04, 21 e 22, deverão ser realizadas em até 10 dias após a assinatura do contrato, a critério do Contratante.

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

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

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

Subcláusula primeira. 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

MINUTA

antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

Subcláusula segunda. Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, quadra 08, conjunto A, Bloco A, sala T-18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4096, e-mail: sgcon@tst.jus.br.

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

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

CLÁUSULA SÉTIMA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

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.

Subcláusula primeira. 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 Coordenadoria de Material e Logística - CMLOG os documentos necessários à instrução de procedimentos para possível aplicação de sanções administrativas.

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

CLÁUSULA OITAVA - DO RECEBIMENTO E DA ACEITAÇÃO DO OBJETO

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

MINUTA

de posterior verificação de sua conformidade. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após o termo de aceite provisório;

II. item 03 – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do serviço. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

III. item 04 – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do treinamento. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

IV. itens 05 a 20 – Provisoriamente, mediante termo circunstanciado, imediatamente depois de efetuada a entrega dos equipamentos e licenças, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a conclusão da instalação;

V. item 21 – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do serviço. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

VI. item 22 – Provisoriamente, mediante termo circunstanciado, imediatamente depois da conclusão do treinamento. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias após a entrega provisória;

VII. item 23 - Provisoriamente, mediante termo circunstanciado, imediatamente após a entrega da nota fiscal referente aos serviços prestados no mês anterior, para efeito de posterior verificação de sua conformidade. Definitivamente, mediante Termo Circunstanciado, em até 10 (dez) dias úteis, após a verificação da perfeita execução das obrigações contratuais.

Subcláusula primeira. 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.

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

Subcláusula terceira. 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.

Subcláusula quarta. 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.

MINUTA

CLÁUSULA NONA - DO PAGAMENTO

O pagamento será efetuado da seguinte forma:

I. Para os itens 1 a 4 – 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.

II. Para os itens 5 a 22 – 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.

III. Para o item 23 – mensalmente, em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo de cada mês, mediante atesto da nota fiscal e verificação da perfeita execução contratual pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

Subcláusula primeira. As notas fiscais e os documentos exigidos no edital para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística do TST, situada no SAFS, quadra 8, conjunto A, bloco A, térreo, sala AT.152, CEP 70070-943, Brasília-DF, (61) 3043-4095.

Subcláusula segunda. Durante o período da pandemia do Coronavírus, os documentos indicados na subcláusula anterior deverão ser encaminhados exclusivamente ao e-mail sgcon@tst.jus.br.

Subcláusula terceira. 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.

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

Subcláusula quinta. 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.

Subcláusula sexta. 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.

Subcláusula sétima. O Contratante pagará à Contratada a atualização monetária sobre o valor devido entre a data do adimplemento das obrigações contratuais e a do efetivo

MINUTA

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.

CLÁUSULA DEZ - DAS OBRIGAÇÕES DA CONTRATADA

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 Coordenadoria de Infraestrutura Tecnológica, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, Sala A2.32, Brasília-DF, CEP 70.070-943, fones: (061) 3043-3035. E-mail de contato: citec@tst.jus.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.

MINUTA

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 do TST e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do TST 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 do TST.

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 do TST, 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 do TST, PSI-TST, e assegurar-se de sua observação e cumprimento no curso da prestação de serviços no Tribunal. A PSI-TST está formalizada no ATO GDGSET.GP. N° 183, DE 27 DE MAIO DE 2019 e pode ser consultada no endereço eletrônico: https://juslaboris.tst.jus.br/handle/20.500.12178/156111.

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 o TST;

MINUTA

XVI. responder, integralmente, por perdas e danos que vier a causar diretamente ao TST 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.

Subcláusula primeira. 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.

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

CLÁUSULA ONZE - DAS OBRIGAÇÕES DO CONTRATANTE

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 do TST, 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 o Protocolo Geral do TST, localizado no SAFS, quadra 08, conjunto A, bloco A, térreo, Brasília-DF, CEP 70.070-943.

CLÁUSULA DOZE - DAS PENALIDADES SOBRE A CONTRATADA

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.

MINUTA

Subcláusula primeira. 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.

Subcláusula segunda. 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.

Subcláusula terceira. 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.

Subcláusula quarta. 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.

Subcláusula quinta. 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.

Subcláusula sexta. 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.

Subcláusula sétima. 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.

Subcláusula oitava. 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.

Subcláusula nona. A não manutenção de todas as condições de habilitação e qualificação exigidas na licitação poderá resultar na rescisão deste contrato, além das penalidades já previstas em lei, caso a Contratada não regularize a situação no prazo de 30 dias.

Subcláusula dez. As multas porventura aplicadas serão descontadas dos pagamentos devidos pelo Contratante, da garantia contratual ou cobradas diretamente da Contratada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

Subcláusula onze. As penalidades serão obrigatoriamente registradas no SICAF, e a sua aplicação será precedida da concessão da oportunidade de ampla defesa para a Contratada, na forma da lei.

MINUTA

CLÁUSULA TREZE - DAS CONDIÇÕES DE HABILITAÇÃO DA CONTRATADA

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.

CLÁUSULA QUATORZE - DA PUBLICAÇÃO

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.

CLÁUSULA QUINZE - DAS ALTERAÇÕES DO CONTRATO

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.

CLÁUSULA DEZESSEIS - DA RESCISÃO

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.

CLÁUSULA DEZESSETE - DA UTILIZAÇÃO DO NOME DO CONTRATANTE

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.

CLÁUSULA DEZOITO - DA PROTEÇÃO DE DADOS

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.

Subcláusula primeira. 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.

MINUTA

Subcláusula segunda. A Contratada está obrigada 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.

Subcláusula terceira. 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.

Subcláusula quarta. A Contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula contratual, inclusive no tocante à Política de Privacidade do TST, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata a presente cláusula.

Subcláusula quinta. 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.

Subcláusula sexta. 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.

Subcláusula sétima. 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.

MINUTA

CLÁUSULA DEZENOVE - DOS CASOS FORTUITOS, DE FORÇA MAIOR OU OMISSOS

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.

CLÁUSULA VINTE - DAS DISPOSIÇÕES FINAIS

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.

Subcláusula primeira. 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.

Subcláusula segunda. 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.

Subcláusula terceira. 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.

Subcláusula quarta. 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.

Subcláusula quinta. 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.

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

Subcláusula sétima. 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

MINUTA

respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

CLÁUSULA VINTE E UM - DO FORO

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.

E, por estarem ajustadas e acordadas, as partes assinam este termo em duas vias de igual teor e forma para um só efeito legal.

Brasília, de de 201 .

CONTRATANTE **CONTRATADA**

MINUTA

ANEXO I

DOS REQUISITOS TÉCNICOS E FUNCIONAIS

MINUTA

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;

3.6.2.5.3 Deverá 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 passiveis 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. Operação prossegue 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.

3.6.7 Grupo 01, Item 03 - Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.

3.6.7.1 A instalação deverá ser realizada, preferencialmente, em ambiente virtual a ser fornecido pela CONTRATANTE.

3.6.7.2 A instalação deverá ser precedida de reunião de planejamento com a equipe da CONTRATADA e terá como resultado o plano de instalação, que deverá conter, no mínimo:

3.6.7.2.1 Detalhamento do Escopo;

3.6.7.2.2 Descrição de atividades em cada etapa do projeto;

3.6.7.2.3 Cronograma de atividades;

3.6.7.2.4 Definição de responsabilidades;

3.6.7.2.5 Pontos de controle;

3.6.7.2.6 Descrição detalhada dos componentes;

3.6.7.2.7 Requisitos necessários.

3.6.7.3 O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

3.6.7.4 O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

3.6.7.5 A instalação deverá estar em acordo com o especificado para a solução e não poderá acarretar acréscimos de custos de licenciamento para a CONTRATANTE.

3.6.7.6 Cabe a CONTRATADA entregar a equipe da CONTRATANTE o dimensionamento dos recursos computacionais para os servidores que irão suportar a solução.

3.6.7.7 O dimensionamento dos recursos computacionais deverá possuir respaldo na documentação oficial do fabricante da solução.

3.6.7.8 Deverão ser criados, a critério da CONTRATANTE, até 10 dashboards em acordo com o exigido nas especificações técnicas.

3.6.8 Grupo 01, Item 04 - Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.

3.6.8.1 O treinamento contemplará todos os *softwares* que compõem a solução.

3.6.8.2 O treinamento deverá ser realizado remotamente.

3.6.8.3 Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

3.6.8.4 O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

3.6.8.5 O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

3.6.8.6 A carga horária mínima exigida para este treinamento é de 30 horas.

3.6.8.7 A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.

3.6.8.8 Deverá ser ministrada uma turma de treinamento que terá até 10 participantes.

3.6.8.9 Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

3.6.8.10 Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o período de realização e o nome completo do participante.

3.6.8.11 O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

3.6.8.12 As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

3.6.8.13 O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

3.6.8.14 A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a CONTRATANTE.

3.6.8.15 Para ser considerado adequado, o treinamento deverá ser aprovadopor pelo menos 70% dos participantes das turmas.

3.6.8.16 A avaliação dos treinamentos levará em consideração as questõeslistadas a seguir:

3.6.8.16.1 Avaliação do conteúdo:

3.6.8.16.1.1 Adequação dos conteúdos aos objetivos propostos;

3.6.8.16.1.2 Adequação das atividades desenvolvidas para alcancedos objetivos propostos;

3.6.8.16.1.3 Adequação do tempo para o alcance dos objetivospropostos;

3.6.8.16.1.4 Profundidade com que o conteúdo foi abordado,considerando os objetivos propostos;

3.6.8.16.1.5 Integração entre teoria, pesquisa, prática e/ou aspectosda realidade;

3.6.8.16.1.6 Qualidade dos exemplos utilizados;

3.6.8.16.1.7 Aplicabilidade dos conhecimentos adquiridos notrabalho;

3.6.8.16.1.8 Contribuição para melhoria do desempenho notrabalho;

3.6.8.16.1.9 Qualidade do material instrucional (apostilas, gráficosetc.).

3.6.8.16.2 Avaliação do instrutor:

3.6.8.16.2.1 Formas/métodos de apresentação dos conteúdos;

3.6.8.16.2.2 Conhecimento dos temas tratados;

3.6.8.16.2.3 Visão prática dos conteúdos tratados;

3.6.8.16.2.4 Uso de estratégias para motivar os alunos em relação aoconteúdo;

3.6.8.16.2.5 Incentivo à participação dos alunos em sala de aula;

3.6.8.16.2.6 Incentivo à realização de atividades adicionais deaprofundamento do aprendizado.

3.6.8.16.3 Avaliação de ambiente e recursos

3.6.8.16.3.1 Qualidade dos recursos tecnológicos utilizados peloinstrutor (áudio, vídeo, recursos para demonstração etc.);

3.6.8.16.3.2 Qualidade do ambiente virtual disponibilizado para ocurso;

3.6.8.16.3.3 Qualidade da conexão disponibilizada pela CONTRATADA.

3.6.8.17 Cada participante deverá indicar uma nota de 1 a 10 para cada item e letra da avaliação.

3.6.8.18 A nota do treinamento será calculada pela média das respostas de todos os itens e letras, e de todos os participantes indicados.

3.6.8.19 O treinamento será considerado com qualidade suficiente, casoatinja uma nota igual ou superior a 7,5.

3.6.8.20 Para comprovação da nota do treinamento, deverá ser encaminhado o detalhamento do cálculo realizado pela CONTRATADA, juntamente com uma cópia dos formulários preenchidos pelos participantes.

3.6.8.21 Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da CONTRATADA, ela estará sujeita às sanções previstas neste termo de referência.

3.6.9 Grupo 02, item 05 - Cluster para prover recursos para solução de acesso a usuários privilegiados

3.6.9.1 Deverá ser composto por, no mínimo, dois servidores dedicados e físicos.

3.6.9.2 Deverá atender, sem perde de desempenho, a solução em sua capacidade máxima, considerando o licenciamento na maior quantidade suportada pela solução, ou seja, se a solução suportar 10.000 usuário privilegiados como sua capacidade máxima, o cluster deverá ser dimensionado para suportar essa capacidade. Essa regra é aplicável a todos osrecursos que são licenciados.

3.6.9.3 Os equipamentos entregues deverão ser novos e de primeiro uso.

3.6.9.4 Deverá ser possível distribuir os nós do cluster entre *datacenters* distintos, ou seja, um nó em cada *datacenter*, sem que isso acarrete perda de funcionalidade ou desempenho. Para esse requisito ser atendido, as características mínimas de interconexão entre os dois *datacenters* deverão ser:

3.6.9.4.1 Interconectados por fibras apagadas, através de LANestendida;

3.6.9.4.2 20Gbps de taxa de transferência na interconexão de LAN;

3.6.9.4.3 Distância máxima entre os dois sites de 1,8km.

3.6.9.5 Deverá ser específico para rack de 19 (dezenove) polegadas.

3.6.9.6 Deverá dispor de chaveamento automático de tensão (sem a necessidade e intervenção humana em chaves de troca de voltagem), considerando as faixas de 115 V a 230 V, com frequência de 50/60 Hertz.

3.6.9.7 Deverá possuir plena redundância, ou seja, funcionar em sem que haja qualquer ponto único de falha, seja na camada lógica (software) ou na camada física (hardware).

3.6.9.8 A solução deve poder ser configurada em cluster de contingência, alta disponibilidade (HA) e recuperação de desastres (DR).

3.6.9.9 A solução deverá continuar funcionando localmente mesmo com a falha de um nó de cada elemento.

3.6.9.10 O modelo mínimo de funcionamento e tolerância a falhas a ser implantado é:

3.6.9.10.1 Componentes principais: ativo/ativo ou ativo/passivo com *failover* automático;

3.6.9.10.2 Componentes secundários: ativo/ativo ou ativo/passivo com

failover automático.

3.6.9.11 No caso de falha em um dos nós do cluster, o nó restante deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ounas funcionalidades.

3.6.10 Grupo 02, Itens 07, 09, 11, 13, 15 ,17 e 19 – Licenças para contas para acesso privilegiados e licenças para ativos protegidos

3.6.10.1 As licenças deverão ser totalmente compatíveis entre si.

3.6.10.2 Licenças deverão ser perpétuas com garantia e direito de atualização por, no mínimo, 12 meses.

3.6.10.3 Suportar, no mínimo, 8.000 sessões simultâneas;

3.6.10.4 Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contraqualquer alteração que comprometa a integridade dessas evidências.

3.6.10.5 Suportar, no mínimo, a gravação de 8h horas por dia, 5 dias por semana, de vídeo com retenção de 90 dias para cada usuário privilegiado.

3.6.10.6 Armazenar os logs de acesso por, pelo menos, 90 dias.

3.6.10.7 Permitir o backup externo, criptografado, dos vídeos e logs deacesso dos usuários privilegiados.

3.6.10.8 Caso o quantitativo de ativos licenciados seja esgotado, a tentativa de acréscimo de mais ativos do mesmo tipo deverá gerar um alerta para o administrador, mas não poderá, em hipótese alguma, impedir o acréscimo e limitar o uso da solução.

3.6.10.9 A solução não deve limitar a quantidade de dispositivos controlados e deve ser capaz de lidar com, no mínimo, 15.000 dispositivos, sem perda de desempenho.

3.6.10.10 Prover autenticação transparente nas aplicações e sistemas-alvos. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema- alvo, de forma que a senha não seja exposta ao solicitante do acesso.

3.6.10.11 Eliminar credenciais inseridas em códigos-fonte, scripts e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e invisíveis aos desenvolvedores e equipe de suporte de TI.

3.6.10.12 Possuir banco de dados de uso exclusivo para evitar que informações sejam armazenadas em bancos de dados compartilhados.

3.6.10.13 Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos e aplicações.

3.6.10.14 Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa.

3.6.10.15 Integração com ferramentas de Service Desk e de Gestão Mudança com possibilidade de validação de critérios pré-definidos para liberação de acesso.

3.6.10.16 Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.

3.6.10.17 Oferecer interface com visão personalizada exclusiva para auditorias contendo os dispositivos e credenciais gerenciadas pela solução.

3.6.10.18 Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo.

3.6.10.19 Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata.

3.6.10.20 Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais.

3.6.10.21 Permitir o monitoramento on-line do uso das contas e desligamentoda sessão.

3.6.10.22 Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade.

3.6.10.23 Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos.

3.6.10.24 Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão ou gerar alerta caso o usuário execute um comando indevido.

3.6.10.25 Permitir Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.

3.6.10.26 Possui configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado

3.6.10.27 Possibilidade de geração de relatórios baseados nos logs e exportá- los para arquivos em formato "csv".

3.6.10.28 Deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação

diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH, API REST HTTP/HTTPS.

3.6.10.29 Caso seja necessária alguma integração com aplicações legadas e/ou integrações com o ambiente interno, o mesmo deverá ser customizado pela CONTRATANTE em acordo com as possibilidades da solução contratada e sem que haja necessidade de desenvolvimento.

3.6.10.30 Extrair informações do servidor localizado nos Data Centers remotos caso seja necessário restaurar todas as configurações e os dados da solução de cofre de senhas.

3.6.10.31 A solução deve possuir ferramenta de monitoração para que seja possível especificar limiares (*threasholds*) referente ao uso de memória, CPU,disco e banco de dados, por exemplo.

3.6.10.32 Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperação de senhas no caso de falha total da solução.

3.6.10.33 Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local deve ser automaticamente replicada para os outros servidores de redundância.

3.6.10.34 Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (*Hash*) ou endereço IP do host ou conjunto de hosts a serem acessados pela solução.

3.6.10.35 Possibilidade de comunicação com os serviços de diretório viaprotocolo LDAPS;

3.6.10.36 Implementar a especificação IETF RFC 2460, referente aoprotocolo IPv6.

3.6.10.37 Implementar a MIB II conforme RFC 1213.

3.6.10.38 Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local.

3.6.10.39 Caso a solução seja separada em componentes, nenhum deles deve conter senhas em texto claro para autenticação.

3.6.10.40 Gerenciar chaves SSH e fazer Scan de servidores Linux e identificação e publicação de chaves SSH.

3.6.10.41 Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA.

3.6.10.42 Permitir a liberação de acesso para execução de tarefas específicas em plataforma SSH.

3.6.10.43 Toda a solução deverá ter seus componentes de hardware e sistema operacional “hardenizados” e protegidos

com firewall interno e detecção de intrusão.

3.6.11 Para as licenças de usuários privilegiados protegidos:

3.6.11.1 A licença deve permitir a proteção de, no mínimo, os seguintes tipos de usuários privilegiados:

3.6.11.1.1 Administradores de sistemas Windows;

3.6.11.1.2 Usuário root de sistemas Linux;

3.6.11.1.3 Usuários de segurança de rede;

3.6.11.1.4 Usuários Domain Admin;

3.6.11.1.5 Usuários DBadmin;

3.6.11.1.6 Usuários SysDBA;

3.6.11.1.7 Usuários VMadmin;

3.6.11.1.8 Usuários de helpdesk;

3.6.11.1.9 Usuários com privilégio de administrador em qualquer tipode ativo suportado.

3.6.11.2 O acesso dos usuários deve ser simultâneo.

3.6.12 Para as licenças de ativos protegidos

3.6.12.1 A licença deve permitir a proteção de, no mínimo, os seguintestipos de ativos:

3.6.12.1.1 Estações de trabalho, seja desktop ou notebook, com ossistemas operacionais Windows;

3.6.12.1.2 Servidores físicos com sistema sistemas operacionais Linux,Windows Server e VMware ESXi;

3.6.12.1.3 Servidores virtuais com sistema sistemas operacionais Linuxe Windows Server;

3.6.12.1.4 Storage com administração realizada aatrvés de protocoloSSH e http/https.

3.6.12.1.5 Equipamentos de rede como switches LAN;

3.6.12.1.6 Equipamentos de rede como AP Wi-Fi;

3.6.12.1.7 Controlador Wi-Fi com acesso via protocolos http/https eSSH;

3.6.12.1.8 Firewall de rede com acesso via protocolos http/https e SSH;

3.6.12.1.9 Aplicação que utiliza infraestrutura de container (aplicaçãoconteineirizada) com *secrets;*

3.6.12.1.9.1 Cada licença de aplicação em container dever tambémser licenciado, ao menos, duas licenças de *secrets.*

3.6.12.1.10 Aplicação não conteineirizadas com senha embutida nocódigo (hard coded);

3.6.12.1.11 Instância de bancos de dados Oracle;

3.6.12.1.12 Instância de bancos de dados Microsoft SQL Server (MSSQL);

3.6.12.1.13 Instância de bancos de dados

PostgreSQL; 3.6.12.1.14 Instância de bancos

de dados MySql e MariaDB;3.6.12.1.15

Instância de Elastic Search.

3.6.12.2 Caso o número de ativos protegidos pela solução ofertada seja ilimitado, a proponente deverá preencher os respectivos itens de licenças na tabela de precificação com o valor zero.

3.6.13 Sobre a gestão de usuários e perfis.

3.6.13.1 Cadastro de usuários com informações de nome e e-mail.

3.6.13.2 Cadastro de perfis de usuários.

3.6.13.3 Segregação de funções por perfis de acesso.

3.6.13.4 Flexibilidade para criação de quaisquer perfis novos, com diversas combinações de telas e funcionalidades de acordo com a necessidade do negócio sem intervenção do fornecedor.

3.6.13.5 Importação automática de contas de usuários do diretório MicrosoftActive Directory (AD) ou outra diretório que utilize o protocolo LDAP.

3.6.13.6 Gerenciamento de Grupos e Perfis de acesso integrados aos gruposdo AD e LDAP.

3.6.13.7 Autenticação de usuários deve realizar, no mínimo:

3.6.13.7.1 Autenticação local através de usuários e senha;

3.6.13.7.2 Autenticação centralizada integrada com LDAP, LDAPS eMS AD com múltiplos DCS;

3.6.13.7.3 Autenticação centralizada integrada com RADIUS;

3.6.13.7.4 Autenticação centralizada integrada com autenticação porcertificado digital pessoal para usuários e administradores;

3.6.13.7.5 Duplo fator de autenticação nativo para acesso web ouatravés de cliente;

3.6.13.7.6 Gestão de autenticação com múltiplos autenticadoressimultan

3.6.14 Sobre o cadastro de ativos.

3.6.14.1 Deve realizar descoberta (*scan*) automática de servidores Linux e identificação de chaves SSH.

3.6.14.2 Deve permitir cadastro de equipamentos parametrizadomanualmente.

3.6.14.3 Deve possui, no mínimo, atributos de ativos tais como marca, modelo, fabricante, localidade e informações que podem ser parametrizados pelo administrador da ferramenta.

3.6.14.4 Possuir *discovery* automatizado de credencias em servidores e bancos de dados.

3.6.15 Sobre cofre de credenciais.

3.6.15.1 As senhas armazenadas devem ser criptografadas com padrões de criptografias fortes como AES 256 ou superior.

3.6.15.2 Deve realizar consolidação periódica de senhas para identificar senhas que foram alteradas em sistemas gerenciados. A consolidação deverá ser feita de forma automática ou por meio de relatórios.

3.6.15.3 Deve envio de alerta por SIEM de senhas que não estejam iguais aocofre.

3.6.16 Sobre cofre de informações privilegiadas.

3.6.16.1 Deve realizar o armazenamento de senhas pessoais.

3.6.16.2 Deve permitir alertas de vencimento das informações armazenadas.

3.6.16.3 Possuir *logs* de alteração de informações privilegiadas.

3.6.17 Sobre o compartilhamento de vídeo sem download com fluxo dentro daferramenta.

3.6.17.1 Permissão para compartilhamento de informações com outrosusuários.

3.6.17.2 Gravação de logs (vídeos e comandos).

3.6.17.3 Gravação de vídeo das sessões realizadas através de *web proxy* ou
proxy transparente em formato otimizado.

3.6.17.4 Gravação de comandos digitados em ambientes RDP e SSH.

3.6.17.5 Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeoou realizar download.

3.6.17.6 Possuir proxy transparente com gravação de logs e vídeos ao sistema alvo sem revelar aos usuários as credenciais utilizadas através cliente local utilizado pelo usuário como Putty, ou RDP Client, sem necessidade de abrir interface web ou baixar nenhum cliente adicional na máquina do usuário.

3.6.17.7 Permitir exportação de sessão em formato vídeo.

3.6.17.8 Busca de registro de sessão por usuário, sistema alvo, ip alvo, datae hora.

3.6.17.9 Busca por comandos e entradas de teclado digitados

em plataformaLinux e Windows.

3.6.17.10 Gravação de Logs de Input e Output de comandos sem necessidade de agentes locais para gravação de sessão;

3.6.17.11 Deve realizar o armazenamento e consulta de logs que forneçam aomenos, as seguintes informações:

3.6.17.11.1 Identificação do usuário que realizou determinado acesso a um dispositivo;

3.6.17.11.2 Identificação de quem aprovou o acesso do usuário;

3.6.17.11.3 Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto;

3.6.17.11.4 Prover, ao menos, os seguintes filtros para a recuperação de logs: Usuário; Sistema-alvo acessado, Tipo de atividade, Intervalo de tempo (data/hora/minuto inicial e final);

3.6.17.11.5 Permitir o acompanhamento on-line de sessões remotas pelo administrador e desligamento da sessão remotamente.

3.6.18 Sobre o bloqueio de comandos e controle de privilégios.

3.6.18.1 Permitir bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução.

3.6.18.2 Possibilidade de bloqueio e auditoria de comandos específicos.

3.6.18.3 Interface para acesso via RDP a aplicações locais com gravação desessão.

3.6.18.4 No caso de acesso a aplicação remota (*Remote App*) ao fechar aaplicação a sessão do usuário deve ser encerrada.

3.6.18.5 Permitir a busca por comandos específicos executados pelo usuárioatravés de linha de comando em logs ou sessões gravadas.

3.6.18.6 Configuração de alertas imediatos quando realizados determinadoscomandos por usuários privilegiado.

3.6.19 Sobre rotação de senhas

3.6.19.1 Troca automática de senhas para os tipos de ativos protegidos.

3.6.19.2 Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da instituição.

3.6.19.3 Flexibilidade para configuração de força de senha gerada.

3.6.19.4 Permitir a liberação de acesso para execução de tarefas específicas em plataforma SSH.

3.6.19.5 Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.

3.6.19.6 Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado.

3.6.19.7 Armazenamento de histórico de senhas por equipamento.

3.6.19.8 Registro de troca executadas.

3.6.19.9 Relatório de acompanhamento de trocas.

3.6.19.10 Relatório de erros de trocas.

3.6.19.11 Alertas de falha ou sucesso de trocas.

3.6.19.12 *Templates* abertos e configuráveis para criação de *booking* para execução de comandos específicos, conforme perfil do usuário ou grupo de usuários.

3.6.19.13 Cadastrar automaticamente chaves públicas das chaves SSH em servidores autorizados.

3.6.19.14 Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca.

3.6.19.15 Disponibilizar os *Templates* de troca de senha de forma que possamser abertos, editáveis e auditáveis.

3.6.19.16 Possuir fluxo de aprovação de alteração de *Template* para evitar fraudes.

3.6.19.17 Rastreabilidade de Alteração de *Template.*

3.6.19.18 Troca de senhas em aplicações HTTP/HTTPS através de *Templates*.

3.6.20 Sobre análise de comportamento.

3.6.20.1 Realizar análise de sessão de usuário baseado em histórico de comportamento. Análise mínima das variáveis de estações origem, estações destino, credenciais, horários e duração de sessão.

3.6.20.2 Identificação de comportamento diferenciados com alertas de anormalidade em relatórios em tela ou alertas para SIEM/SYSLOG.

3.6.20.3 Análise de sessão de usuários a fim de apresentar comando críticos com alertas de anormalidade em relatórios em tela ou alertas paraSIEM/SYSLOG.

3.6.20.4 Possuir dashboards gráficos com informações sobre riscos eameaças.

3.6.21 Sobre *dashboards* e relatórios a solução deve possuir:

3.6.21.1 Relatórios de operação com lista e usuários cadastrados,equipamentos cadastros,

credenciais cadastradas;

3.6.21.2 Relatórios PCI;

3.6.21.3 Relatórios de Gestão de Evidências;

3.6.21.4 Relatórios de Auditoria;

3.6.21.5 Relatórios de Alertas;

3.6.21.6 Exportação para Excel (.csv);

3.6.21.7 Dashboard de utilização;

3.6.21.8 Dashboard de conexões;

3.6.21.9 Dashboard de utilização de sessões;

3.6.21.10 Dashboard de sessão;

3.6.21.11 Dashboard de usuário;

3.6.21.12 Dashboard de servidor.

3.6.22 Sobre a central gerenciamento.

3.6.22.1 Console central de gerenciamento de aplicação com capacidadepara:

3.6.22.1.1 Suporte à utilização de certificados digitais válidos pela ICP- Brasil, certificados digitais internacionais e certificados auto assinados gerados pela própria solução;

3.6.22.1.2 Criação de usuários;

3.6.22.1.3 Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download;

3.6.22.1.4 Busca de sessões gravadas;

3.6.22.1.5 Possibilidade de sessão remota através dos protocolos SSH e RDP ou programa cliente instalado na estação de trabalho do usuário sema necessidade de passar por aplicação web ou baixar nenhum cliente adicional na máquina do usuário;

3.6.22.1.6 Permitir a busca por senhas que foram trocadas em momento anterior;

3.6.22.1.7 Gestão de políticas de acesso centralizadas;

3.6.22.1.8 Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores;

3.6.22.1.9 Cadastro de dispositivos centralizados.

3.6.23 Grupo 02, itens 06, 08, 10, 12, 14, 16, 18 e 20 – Garantia do fabricante.

3.6.23.1 As garantias fornecidas pelo fabricante deverão ser por todo período mínimo de 12 meses.

3.6.23.2 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.

3.6.23.3 Define-se garantia do fabricante como sendo serviço efetuado mediante abertura de chamado junto ao 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 sobre configuração, uso e atualização dos produtos. Também faz parte da garantia o fornecimento de qualquer atualização de versão das licenças, sejam elas corretivas, evolutivas ou de outra natureza, durante a vigência da garantia.

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

3.6.23.5 O fabricante 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.

3.6.23.6 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. Operação prossegue 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

3.6.23.7 O nível de severidade dos chamados deverá ser comunicado ao Fabricante pela CONTRATANTE no momento de sua abertura.

3.6.23.8 O início do atendimento dos chamados técnicos de nível de severidade 1 deverá ser iniciado em até 1 (uma) hora; os de nível de severidade 2, em até 2 (duas) horas, os de nível de severidade 3 em até 8 (oito) horas e o de nível de severidade 4 em até 12 (doze) horas.

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

3.6.24 Grupo 02, item 21 - Serviço de instalação para solução de controle de acesso de usuários privilegiados.

3.6.24.1 A instalação deverá ser precedida de reunião de

planejamento com a equipe da CONTRATADA e terá como resultado o plano de instalação, quedeverá conter, no mínimo:

3.6.24.1.1 Detalhamento do Escopo;

3.6.24.1.2 Descrição de atividades em cada etapa do projeto;

3.6.24.1.3 Cronograma de atividades;

3.6.24.1.4 Definição de responsabilidades;

3.6.24.1.5 Pontos de controle;

3.6.24.1.6 Descrição detalhada dos componentes;

3.6.24.1.7 Documentação a ser entregue, incluindo todos os detalhes dasinstalações a serem realizadas onde deverá apresentar informações para procedimentos, incluindo comandos e testes aplicáveis, procedimentos de inicialização e procedimentos de configuração;

3.6.24.1.8 Requisitos necessários.

3.6.24.2 O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

3.6.24.3 O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

3.6.24.4 Eventuais ajustes no cabeamento elétrico, como troca do tipo de tomada, é de responsabilidade da CONTRATADA e não poderá gerar custos a CONTRATANTE.

3.6.24.5 A instalação deverá estar em acordo com o especificado para a solução e não poderá acarretar acréscimos de custos de licenciamento para a CONTRATANTE.

3.6.24.6 Caso seja necessário efetuar ajustes no equipamento para compatibilizar com a infraestrutura da CONTRATANTE, esses ajustes deverão ser feitos pela CONTRATADA sem ônus para a CONTRATANTE.

3.6.24.7 Caberá a CONTRATADA, na fase de instalação, realizar as devidas configurações para que os ativos licenciados sejam protegidos conforme o quantitativo de licenças contratadas, sendo eles do tipo:

3.6.24.7.1 Servidores físicos e virtuais (Linux, Windows e Storages);

3.6.24.7.2 Estações de trabalho Windows;

3.6.24.7.3 Equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP);

3.6.24.7.4 Instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL).

3.6.25 Grupo 02, item 22 - Treinamento para solução de controle de acesso deusuários privilegiados.

3.6.25.1 O treinamento deverá ser precedido de reunião de planejamento com a equipe da CONTRATANTE.

3.6.25.2 O treinamento contemplará todos os softwares e hardwares que compõem a solução.

3.6.25.3 O treinamento deverá ser realizado remotamente.

3.6.25.4 Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

3.6.25.5 O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

3.6.25.6 O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

3.6.25.7 A carga horária mínima exigida para este treinamento é de 30 horas.

3.6.25.8 A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.

3.6.25.9 Deverá ser ministrada uma turma de treinamento que terá até 10 participantes.

3.6.25.10 Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

3.6.25.11 Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o período de realização e o nome completo do participante.

3.6.25.12 O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

3.6.25.13 As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

3.6.25.14 O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

3.6.25.15 A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a CONTRATANTE.

3.6.25.16 Para ser considerado adequado, o treinamento deverá ser aprovadopor pelo menos 70% dos participantes das turmas.

3.6.25.17 A avaliação dos treinamentos levará em consideração as questõeslistadas a seguir:

3.6.25.17.1 Avaliação do conteúdo:

3.6.25.17.1.1 Adequação dos conteúdos aos objetivos propostos;

3.6.25.17.1.2 Adequação das atividades desenvolvidas para alcancedos objetivos propostos;

3.6.25.17.1.3 Adequação do tempo para o alcance dos objetivospropostos;

3.6.25.17.1.4 Profundidade com que o conteúdo foi abordado,considerando os objetivos propostos;

3.6.25.17.1.5 Integração entre teoria, pesquisa, prática e/ou aspectosda realidade;

3.6.25.17.1.6 Qualidade dos exemplos utilizados;

3.6.25.17.1.7 Aplicabilidade dos conhecimentos adquiridos notrabalho;

3.6.25.17.1.8 Contribuição para melhoria do desempenho notrabalho;

3.6.25.17.1.9 Qualidade do material instrucional (apostilas, gráficosetc.).

3.6.25.17.2 Avaliação do instrutor:

3.6.25.17.2.1 Formas/métodos de apresentação dos conteúdos;

3.6.25.17.2.2 Conhecimento dos temas tratados;

3.6.25.17.2.3 Visão prática dos conteúdos tratados;

3.6.25.17.2.4 Uso de estratégias para motivar os alunos em relação aoconteúdo;

3.6.25.17.2.5 Incentivo à participação dos alunos em sala de aula;

3.6.25.17.2.6 Incentivo à realização de atividades adicionais deaprofundamento do aprendizado.

3.6.25.17.3 Avaliação de ambiente e recursos:

3.6.25.17.3.1 Qualidade dos recursos tecnológicos

utilizados peloinstrutor (áudio, vídeo, recursos para demonstração etc.);

3.6.25.17.3.2 Qualidade do ambiente virtual disponibilizado para ocurso;

3.6.25.17.3.3 Qualidade da conexão disponibilizada pela CONTRATADA.

3.6.25.18 Cada participante deverá indicar uma nota de 1 a 10 para cada item e letra da avaliação.

3.6.25.19 A nota do treinamento será calculada pela média das respostas de todos os itens e letras, e de todos os participantes indicados.

3.6.25.20 O treinamento será considerado com qualidade suficiente, casoatinja uma nota igual ou superior a 7,5.

3.6.25.21 Para comprovação da nota do treinamento, deverá ser encaminhado o detalhamento do cálculo realizado pela CONTRATADA, juntamente com uma cópia dos formulários preenchidos pelos participantes.

3.6.25.22 Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da CONTRATADA, ela estará sujeita às sanções previstas neste termo de referência.

3.6.26 Grupo 02, item 23 – Serviço e suporte técnico especializado.

3.6.26.1 Deverá ser prestado suporte técnico e manutenção pela CONTRATADA por todo período mínimo de 12 meses.

3.6.26.2 Define-se serviço de suporte técnico sendo aquele efetuado mediante abertura de chamado junto à CONTRATADA, 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.

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

3.6.26.4 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.

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

3.6.26.6 Caberá a CONTRATADA realizar a manutenção evolutiva dos *softwares* da solução, fornecendo, instalando e

configurando as novas versões e/ou releases e atualizações lançadas durante a vigência da garantia, mantendo-os funcionais e compatíveis com o ambiente utilizado pela CONTRATANTE.

3.6.26.7 A CONTRATADA deverá garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços, configurações e fornecimento "fixes" e "releases", durante toda a vigência da garantia.

3.6.26.8 Executar, durante o período de vigência da garantia, suporte preventivo e corretivo da solução objeto do contrato, para as seguintes atividades:

3.6.26.8.1 Parametrização e auditoria técnica de disponibilidade e funcionamento da solução;

3.6.26.8.2 Manutenção e suporte a todo o ambiente de software básico da solução, atuando em casos de incidentes escalonados pela equipe técnica do CONTRATANTE, mediante identificação da causa raiz do problema, definição e implantação da solução de contorno para garantir o nível de disponibilidade do ambiente, aplicação da solução definitiva;

3.6.26.8.3 Promover o escalonamento dos incidentes e problemas graves ou de solução que demore mais tempo que o previsto contratualmente ao suporte especializado do fabricante, para rápida normalização doambiente;

3.6.26.8.4 Relatar e implementar melhorias, atualizações e ajustes finos para aprimorar a solução de proteção de dados.

3.6.26.8.4.1 As implementações deverão ser fruto de análise das atualizações e correções disponibilizadas pelo fabricante, da análise do ambiente e do conjunto de melhores práticas para o ambiente;

3.6.26.8.4.2 As implementações deverão ser planejadas, detalhadas em atividades, com análise dos riscos e impacto no ambiente e de indicação de benefícios para sua execução.

3.6.26.8.5 Ações de aperfeiçoamento de funcionalidade, disponibilidadee configuração dos produtos da solução;

3.6.26.8.6 Execução de procedimentos de instalação em conformidade com as recomendações do fabricante, documentações existentes e as boaspráticas de mercado;

3.6.26.8.7 Execução dos procedimentos descritos na documentação e proposições para a melhoria contínua desses procedimentos;

3.6.26.8.8 Suporte, configuração, customização,

parametrização e implantação de sistemas auxiliares, visando manter a disponibilidade e o desempenho da solução;

3.6.26.8.9 Análise e proposição de soluções adequadas para o ambiente contratado, sob orientação da equipe técnica do CONTRATANTE;

3.6.26.8.10 Detecção, análise e resolução dos problemas de funcionalidade, configuração e parametrização, atuando preventivamente para evitar ocorrência de incidentes, identificação de pontos de falhas,

análise de potenciais de riscos da infraestrutura de backup e identificação de tendências de capacidade e disponibilidade do ambiente de backup;

3.6.26.8.11 Análise de "logs" e registros dos equipamentos, ferramentas e softwares envolvidos na solução, com anotações e geração de relatórios estatísticos;

3.6.26.8.12 Geração de relatórios de ocorrências para todas as falhas de serviços classificados pelo CONTRATANTE como críticos, com informações de causa e efeito, providências e correções aplicadas e recomendações sobre as lições aprendidas;

3.6.26.9 A CONTRATADA deverá realizar manutenção preventiva programada, que se destina a prevenir indisponibilidades e/ou falhas dos componentes da solução contratada, em suas instalações, subsistemas e componentes envolvidos, mantendo-as em perfeito estado de funcionamento e conservação, conforme especificado em projeto, manuais e normas técnicas específicas.

3.6.26.9.1 A manutenção preventiva programada deverá ser realizada mediante visita mensal da CONTRATADA, visando analisar desempenho e funcionalidade da solução, emitindo relatório mensal de serviços e resultados, com as sugestões de melhoria possíveis, visando garantir melhor performance da solução e segurança cibernética das credenciais.

3.6.26.9.2 A manutenção preventiva programada deverá ser realizada, preferencialmente, de forma remota, salvo quando houver impossibilidade técnica de acesso ao ambiente da CONTRATANTE.

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

3.6.26.11 Na impossibilidade do suporte remoto por alguma questão técnica, a CONTRATADA deverá realizar o suporte presencialmente nasdependências da CONTRATANTE.

3.6.26.12 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. Operação prossegue 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

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

3.6.26.14 O início do atendimento dos chamados técnicos de nível de severidade 1 deverá ser iniciado em até 1 (uma) hora; os de nível de

severidade 2, em até 2 (duas) horas, os de nível de severidade 3 em até 8(oito) horas e o de nível de severidade 4 em até 12 (doze) horas.

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

Nível de severidade	Período máximo para solução
1	24 horas
2	36 horas
3	48 horas úteis
4	72 horas úteis

3.6.26.16 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.

3.6.26.17 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.

3.6.26.18 A CONTRATANTE poderá CONTRATADA deverá ser realizado suporte proativo, a critério da CONTRATANTE,

3.6.26.19 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.

3.6.26.20 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.

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

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

ANEXO II

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Eu nome, nacionalidade, estado civil, cargo, inscrito (a) no CPF sob o nº XXX.XXX.XXX-XX, declaro ter ciência da obrigatoriedade, a partir desta data, quanto ao cumprimento das regulamentações descritas na Política de Segurança da Informação do TRIBUNAL SUPERIOR DO TRABALHO (TST), instituída por meio da Resolução CNJ nº 363/2021. Comprometo-me ainda a observar o disposto na Lei Geral de Proteção de Dados – LGPD, Lei nº 13.709, de 14 de agosto de 2018, e cumprir o dever em salvaguardar a informação sigilosa e pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício de minhas atribuições sob pena de responsabilização administrativa, civil e penal.

Para efeitos deste Termo, além das definições constantes do artigo 5º da LGPD, aplicam-se as seguintes definições:

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal.

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

Informação pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem, como: resultado de exames médicos; lista de nomes, e-mail dos servidores ou colaboradores do TST e respectivos dados, armazenados sob qualquer forma; Informações referentes a salários e benefícios dos servidores.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo, tais como: Sigilos Decorrentes de Direitos de Personalidade: Sigilo Fiscal, Sigilo Bancário, Comercial, Sigilo Empresarial, Sigilo Contábil; Sigilos de Processos e Procedimentos: Acesso a Documento Preparatório, Sigilo do Procedimento Administrativo Disciplinar em Curso, Sigilo do Inquérito Policial, Segredo de Justiça no Processo Civil, Segredo de Justiça no Processo Penal; Informação de Natureza Patrimonial: Segredo Industrial, Direito Autoral e Propriedade Intelectual de Programa de Computador, Propriedade Industrial. Serão, ainda, consideradas informações confidenciais todas aquelas que assim forem identificadas pelo TST, por meio de legendas ou quaisquer outras marcações, ou que, devido às circunstâncias da revelação ou à própria natureza da informação, devam ser consideradas confidenciais.

MINUTA

Incidente de segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que seja ameaça á integridade, autenticidade ou disponibilidade de qualquer ativo de TI do TST.

Proprietário da informação: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal 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, quando vinculado a uma pessoa natural;

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Encarregado: 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);

Agentes de tratamento: o controlador e o operador;

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

MINUTA

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitida por esses entes públicos, ou entre entes privados;

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Por este termo de responsabilidade e confidencialidade, comprometo-me a:

1. Não utilizar informações sigilosa (protegida por legislação específica) ou pessoal a que tiver acesso, para lograr benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros. Estas informações nos diversos formatos (impresso, magnético ou digital) devem ser tratadas com absoluta reserva em qualquer condição e não podem ser divulgadas ou dadas a conhecer a terceiros não autorizados, inclusive aos próprios usuários (servidores públicos, estagiários, prestadores de serviço ou terceirizados) do TST, sem a autorização do proprietário da informação;

MINUTA

2. Não efetuar gravação ou cópia da documentação sigilosa ou pessoal a que tiver acesso para fins diversos não relativos à função ou cargo;

3. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

4. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador, bloquear estação de trabalho, garantindo assim a impossibilidade de acesso indevido por terceiros;

5. Não revelar minhas senhas a ninguém, visto que são de uso pessoal e intrasferível e de conhecimento exclusivo, e tomar o máximo de cuidado para que elas permaneçam somente de meu conhecimento.

6. Alterar minha senha regularmente e sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

7. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

8. Não navegar em sites pornográficos, defensores do uso de drogas, de pedofilia ou sites de cunho racistas e similares ou realizar qualquer atividade tipificada como crime, bem como não fazer download de material protegido por direitos autorais ou com conteúdo impróprio;

9. Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição, bem assim observar as normas e limites para o tratamento de dados pessoais estabelecidos na LGPD.

10. Informar imediatamente à Secretaria de Tecnologia da Informação do TST (SETIN) e/ou ao controlador/encarregado dos dados pessoais, designado pela ComLGPD, a respeito de qualquer incidente de segurança da informação, ou relacionado ao tratamento de dados pessoais, ou violação, intencional ou não, das regras descritas na Política de Segurança da Informação e normas legais e regulamentares correlacionadas.

De acordo com o Código Penal Brasileiro (Decreto-Lei 2.848, de 1940) constitui infração inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano (Incluído pela Lei nº 9.983, de 2000).

A observância da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, com apoio na legislação federal e nas normas regulamentares que regem a matéria,

MINUTA

possui caráter irrevogável e irretratável, e vigência enquanto a confidencialidade das informações/dados por mim tratados persistir, na forma da Lei nº 13.709/2018 e demais legislação e normativos que disponham sobre a matéria.

Não será considerada quebra de confidencialidade a divulgação de informações ordenadas pela legislação ou por autoridade judiciária ou administrativa competente.

O não cumprimento deste Termo implicará, para os que estiverem envolvidos na violação do sigilo e uso das informações do TST, sem prejuízo da responsabilidade civil e criminal, nas seguintes sanções: Para Servidores: sanções internas, variando de simples advertência à demissão por justa causa, conforme Art. 132, inciso IX da Lei 8112/90. Para parceiros, estagiários, prestadores de serviço ou terceirizados: variando de advertência à rescisão do respectivo contrato de prestação de serviço, com aplicação de todas as multas nele previstas por inadimplemento.

Para dirimir quaisquer dúvidas oriundas do presente Termo, fica eleito o foro de Brasília, Distrito Federal, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

Local e data

_____

Representante da empresa
(nome da empresa)

MINUTA