PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

José André Mendes Coimbra
18/10/2022 13:28

14/10/2022 14:49

CONTRATO N. 29/2022

CONTRATO n. 29/2022 – AQUISIÇÃO DE SOLUÇÕES DE SEGURANÇA, AUDITORIA E PREVENÇÃO DE AMEAÇAS. (Processo TST N.º 6001640/2021-00 e Processo TRT23 n. 6562/2022).

A **UNIÃO**, por intermédio **TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO**, inscrito no CNPJ/MF sob o n. 37.115.425/0001-56, sediado na Rua Engenheiro Edgard Prado Arze, n. 191, Centro Político Administrativo, Cuiabá/MT, CEP 78.049-935, telefone geral (65) 3648-4000, doravante denominado simplesmente CONTRATANTE, neste ato representado por seu Diretor-Geral, Sr. MARLON CARVALHO DE SOUSA ROCHA, e a empresa **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP**, inscrita no CNPJ/MF sob o n. 24.425.034/0001-96, com sede na SCN, Quadra 02, Bloco A, n. 190, Sala 504, Parte O-1, Asa Norte, Brasília/DF, CEP 70.712-010, telefone (61) 2017-0771 e 98267-2204, e-mail andre.coimbra@petacorp.com.br e anapaula.lacerda@petacorp.com.br, doravante denominada simplesmente CONTRATADA, neste ato representada pelo sr. JOSÉ ANDRÉ MENDES COIMBRA, inscrito no CPF sob n. ***.539.***-53, considerando o julgamento **do Pregão Eletrônico TST n.º 058/2021**, publicado no Diário Oficial da União do dia 23 de dezembro de 2021, 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 Pregão Eletrônico TST n.º 058/2021.

TRT-23ª REGIÃO Mato Grosso
Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

Item	Especificação	Unidade	Quantidade	Valor Unitário (R$)	Valor total (R$)
5	*Cluster* para prover recursos para solução de acesso a usuários privilegiados	Cluster	1	249.500,00	249.500,00
6	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster	1	49.094,43	49.094,43
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin /SysDBA, VMadmin, helpdesk)	Usuários	20	1.405,00	28.100,00
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	20	291,93	5.838,60
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	378	45,73	17.285,94
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	378	9,57	3.617,46
11	Licença para estações de trabalho Windows	Estações	1570	14,41	22.623,70
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações	1570	4,18	6.562,60
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	214	23,30	4.986,20

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

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	214	4,55	973,70
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	28	1.044,00	29.232,00
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	28	223,24	6.250,72
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	Serviço	1	44.900,00	44.900,00
22	Treinamento para solução de controle de acesso de usuários privilegiados.	Turma	1	16.000,00	16.000,00
23	Serviço e suporte técnico especializado	Mês	12	12.090,00	145.080,00
TOTAL (R$)					**630.045,35**

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

Subcláusula segunda. Do regime de contratação: o objeto do presente instrumento

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

CONTRATO N. 29/2022

será executado por empreitada por preço global, 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 06, 08, 10, 12, 14, 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.

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$ 630.045,35 (seiscentos e trinta mil, quarenta e cinco reais e trinta e cinco centavos).**

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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

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.

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 PTRES 213510, Elementos de despesa 449040-01 e 449040-05 (Nota de empenho n. 774/2022), e, 339040-11 e 339040-20 (Nota de empenho n. 775/2022), emitidas em 13/10/2022.

CLÁUSULA SEXTA – DOS PRAZOS

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

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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

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

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

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

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

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

VII. 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 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: Divisão de Segurança da Informação e Proteção de Dados, Rua Engenheiro Edgard Prado Arze, n. 191, Centro Político Administrativo, Cuiabá/MT, CEP 78.049-935, telefone: (065) 3648-4026, e-mail: dsi@trt23.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 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 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;

II. 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;

III. 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;

IV. 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.

CONTRATO N. 29/2022

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.

CLÁUSULA NONA - DO PAGAMENTO

O pagamento será efetuado da seguinte forma:

I. 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.

II. 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 Divisão de Governança - STIC, Rua Engenheiro Edgard Prado Arze, n. 191, Centro Político Administrativo, Cuiabá/MT, CEP 78.049-935, e-mail: dggc@trt23.jus.br.

Subcláusula segunda. Durante o período da pandemia do Coronavírus, os documentos indicados na subcláusula anterior deverão ser encaminhados exclusivamente ao e-mail dggc@trt23.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.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

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 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 Divisão de Segurança da Informação e Proteção de Dados, Rua Engenheiro Edgard Prado Arze, n. 191, Centro Político Administrativo, Cuiabá/MT, CEP 78.049-935, telefone: (065) 3648-4026, e-mail: dsi@trt23.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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

execução do objeto, bem como atender prontamente às suas observações e exigências e prestar os esclarecimentos solicitados;

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

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

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

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

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

IX. guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do Contratante, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros.

X. garantir a segurança das informações do TRT23 e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do TRT23 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 TRT23.

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 TRT23, 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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

responsabilidade do profissional da Contratada.

c. divulgar aos seus profissionais a Política de Segurança da Informação do TRT23, PSI-TRT23, e assegurar-se de sua observação e cumprimento no cursoda prestação de serviços no Tribunal. A PSI-TRT23 está formalizada na Resolução Administrativa TRT23 n. 177/2019, DE 27 DE JULHO DE 2019 e pode ser consultada no endereço eletrônico: *https://portal.trt23.jus.br/portal/sites/portal/files/solr//mnt/publicos/STP/Resolu%C3%A7%C3%B5es%20Administrativas/RESOLU%C3%87%C3%95ES%20DE%202019/RA%20177.docx*

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 TRT23;

XVI. responder, integralmente, por perdas e danos que vier a causar diretamente ao TRT23 ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua oudos 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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

obrigações contratuais, inclusive permitir o acesso dos funcionários da Contratada às dependências do TRT23, 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 ou e-mail para Divisão de Segurança da Informação e Proteção de Dados, Rua Engenheiro Edgard Prado Arze, n. 191, Centro Político Administrativo, Cuiabá/MT, CEP 78.049-935, telefone: (065) 3648-4026, e-mail: dsi@trt23.jus.br.

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.

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 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 quarta. O atraso injustificado na entrega do plano de instalação sujeitará

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

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 quinta. 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 sexta. 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 sétima. 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 oitava. 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 nona. 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 dez. As penalidades serão obrigatoriamente registradas no SICAF, e a sua aplicação será precedida da concessão da oportunidade de ampla defesa para a Contratada, naforma da lei.

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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

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.

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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

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 TRT23, 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.

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.

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

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 rescisãodo 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

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)

CONTRATO N. 29/2022

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 Justiça Federal em Cuiabá-MT, Seção Judiciária do Estado de Mato Grosso, como competente para dirimir quaisquerquestões 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.

Cuiabá, 14 de outubro de 2022.

TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO
MARLON CARVALHO DE SOUSA ROCHA
Diretor-Geral

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP
JOSÉ ANDRÉ MENDES COIMBRA
Representante Legal

ANEXO I

DOS REQUISITOS TÉCNICOS E FUNCIONAIS

Rua Engenheiro Edgard Prado Arze, 191 | Centro Político e Administrativo | Cuiabá/MT | CEP: 78049-935
Telefone:(65) 3648-4363 | contratos@trt23.jus.br

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 àCONTRATANTE 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 emperíodo 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.

PROAD 6562/2022

CERTIDÃO DE ASSINATURA

O seguinte documentos foi assinado em 14/10/2022 por José André Mendes Coimbra (CPF: 47153989153)

62 - DOCUMENTO - Contrato 29/2022 assinado pelas partes

Certidão gerada automaticamente pelo sistema.

00038-2022. Entrega das Propostas: a partir de 18/10/2022 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 04/11/2022 às 10h00 (horário de Brasília/DF) no site www.gov.br/compras. Informações Gerais: Conforme edital.

João Pessoa-PB, 17 de outubro de 2022.
RONALDO VIEIRA DE ARAGÃO
Pregoeiro

TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO

EXTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

PROAD Nº 4989/2022. Objeto: contratação direta de empresa para ministrar a palestra "APOSENTADORIA - prioridades da vida para ser bem vivida", a ser realizada em 20 de outubro de 2022, das 10h às 11h30 (horário de Brasília), de modo telepresencial, com carga horária de 1h30 (uma hora e trinta minutos), tendo como público-alvo magistrados, servidores, estagiários, terceirizados e demais colaboradores do TRT14, bem como o público externo interessado, participantes do evento "Encontro de Saúde - edição 2022". Empresa: INSTITUTO ZANELLI - TREINAMENTO, DESENVOLVIMENTO E EDUCAÇÃO NAS ORGANIZAÇÕES E NO TRABALHO LTDA. Valor Total: R$ 9.000,00. Amparo legal: inciso II, do art. 25 c/c inciso VI, do art. 13, ambos da Lei nº 8.666/93 - Decisões TCU 535/1996-Plenário e 439/1998- Plenário. Reconhecimento: Desembargadora Maria Cesarineide de Souza Lima, Diretora da Escola Judicial do TRT-14ª Região.

TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO

DIRETORIA-GERAL

SECRETARIA DA ADMINISTRAÇÃO

COORDENADORIA DE CONTRATOS

SEÇÃO DE ANÁLISE CONTRATUAL

EXTRATO DE CONTRATO

Proad nº 23882/2022 - Contrato: 88/2022. Partes: TRT e ARCON ENGENHARIA E SERVIÇOS EIRELI. CNPJ: 20.608.820/0001-78. Objeto: prestação de serviços de manutenção predial e outros serviços comuns de engenharia (Sede Administrativa - Campinas/SP). Fundamento: Lei 8.666/1993. LO: 14.303, de 21/01/2022. Classificação: 02.122.0033.4256.0035 339039 16. Valor total: R$29.728,17. Nota de empenho: 2022NE001522, de 07/10/2022. Vigência: 120 dias, a contar da data da assinatura. Assinam: pelo TRT, Vera Lucia de Oliveira Ramires; e, pela empresa, Luiz Carlos Palmeira. Data: 11/10/2022.

EXTRATO DE TERMO ADITIVO

PROAD 22538/2020 Contrato: 62/2018. Espécie: IV TA. Partes: TRT e LIDERANÇA LIMPEZA E CONSERVAÇÃO LTDA. CNPJ: 00.482.840/0001-38. Objetos: I- prorrogação da vigência do contrato por 6 meses, de 06/11/2022 a 05/05/2023; e II- Repactuação de preços do contrato. Fundamento: Lei 8.666/1993, artigo 57, inciso II e artigo 65, § 5º c/c artigo 54 da IN 05/2017. LO: 14303, de 21/01/2022. Assinam: pelo TRT, Vera Lucia de Oliveira Ramires; e, pela empresa, Willian Lopes de Aguiar. Data: 14/10/2022.

TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO

EXTRATO DE CONTRATO

PROCESSO: TRT/18ª n° 4824/2022. CONTRATO: SLC-SEC 42/2022. CONTRATADA: RJR SERVIÇOS DE INFORMÁTICA LTDA. CNPJ: 11.508.825/0001-38. OBJETO: Serviço de acesso à solução integrada de colaboração e comunicação corporativa. VALOR TOTAL: R$ 935.626,00. VIGÊNCIA: 30 meses, contados a partir do 01/11/2022. FUNDAMENTO LEGAL: PE/SRP TRT2 n° 98/2021; Leis n.º 10.520/02, n.º 8.666/93 e nº 13.709/18, Decreto n.º 10.024/19. RECURSOS ORÇAMENTÁRIOS: Programas de Trabalho: 02.122.0033.4256.0052. Natureza da Despesa: 3390.40. DATA DE ASSINATURA: 17/10/2022.

EXTRATO DE CONTRATO

PROCESSO: TRT/18ª n° 6324/2022. CONTRATO: SLC-SEC 41/2022. CONTRATADA: TORINO INFORMÁTICA LTDA. CNPJ: 03.619.767/0005-15. OBJETO: Aquisição de 128 monitores. VALOR TOTAL: R$ 120.320,00. VIGÊNCIA: 12 meses, contados a partir da assinatura. FUNDAMENTO LEGAL: PE/SRP/TRT22 n° 20/2022; Leis n° 8.666/93, n° 10.520/02; LC. nº 123/06. RECURSOS ORÇAMENTÁRIOS: Programas de Trabalho: 02.122.0033.4256.0052. Natureza da Despesa: 4490.52. DATA DE ASSINATURA: 17/10/2022.

EXTRATO DE TERMO ADITIVO

PROCESSO: TRT/18ª 7517/2018. CONTRATADA: SECURITY SEGURANÇA LTDA. ESPÉCIE: 9º termo aditivo ao contrato nº 25/2019. OBJETO: Incluir na execução dos serviços, diretrizes a serem seguidas no período do Recesso Forense. FUNDAMENTO LEGAL: Art.65, inciso II, da Lei nº 8.666/93. DATA DE ASSINATURA: 14/10/2022.

TRIBUNAL REGIONAL DO TRABALHO DA 21ª REGIÃO

DIRETORIA-GERAL

SECRETARIA ADMINISTRATIVA

EXTRATO DE DISPENSA DE LICITAÇÃO

PROAD: Nº 3154/2022. Objeto: Contratação de empresa de montagem, monitoramento e desmontagem do sistema de escoramento da estrutura metálica de cobertura de área do TRT 21ª Região. Empresa: Ícone Engenharia Ltda. Valor: R$ 59.692,30 (cinquenta e nove mil seiscentos e noventa e dois reais e trinta centavos). Fundamentação Legal: art. 24, inciso IV da Lei nº 8.666/93. Autorização: Diretor Geral/Ordenador de Despesa do TRT-21ª Região, Márcio de Medeiros Dantas, em 14/10/2022. Ratificação: Desembargadora Presidente do TRT-21ª Região, Maria do Perpetuo Socorro Wanderley de Castro, em 14/10/2022.

SEÇÃO DE CONTRATOS ADMINISTRATIVOS

EXTRATO DE TERMO ADITIVO

PROAD nº 2923/2020. Espécie: Segundo Termo Aditivo ao Convênio TRT/DLC Nº 003/2020, firmado entre o TRT da 21ª Região e a SOCIEDADE EDUCACIONAL CARVALHO GOMES LTDA. OBJETO: Prorrogação do prazo de vigência pelo período de 12 meses (20/10/2022 a 19/10/2023). ASSINATURA: 02/09/2022. SIGNATÁRIOS: Desembargadora Maria do Perpétuo Socorro Wanderley de Castro, Presidente, pelo TRT21, e Guilherme Dantas Cardoso, procurador, pela Instituição de ensino.

TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO

EXTRATO DE CONTRATO

Proad 6562/2022. Contrato 29/2022. OBJETO: 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. CONTRATADA: JAMC Consultoria e Representação de Software Ltda EPP, CNPJ: 24.425.034/0001-96. VALOR TOTAL R$: 630.045,35. ASSINATURA: 14/10/2022. VIGÊNCIA: 12 meses, contados da data da sua assinatura. FUNDAMENTAÇÃO LEGAL: art. 22 do Decreto 7892/2013, LC 123/2006, Leis 8.666/93, 10.520/2002, 8.078/90 e 9.784/99 e nos Decretos 7.892/2013, 8.538/2015 e 10.024/2019. PROGRAMA DE TRABALHO: PTRES 213510. SIGNATÁRIOS: Marlon Carvalho de Sousa Rocha/TRT; José André Mendes Coimbra/Contratada.

TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 25/2022 - UASG 80026

Nº Processo: 23012/2022. Objeto: Registro de preços para eventual aquisição de materiais de copa, cozinha, limpeza e higienização e umidificador de ambientes.. Total de Itens Licitados: 20. Edital: 18/10/2022 das 08h00 às 17h59. Endereço: R.delegado Carlos Roberto Bastos de Oliveira,208 - Jdim Veraneio, Parque Dos Poderes - Campo Grande/MS ou https://www.gov.br/compras/edital/80026-5-00025-2022. Entrega das Propostas: a partir de 18/10/2022 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 03/11/2022 às 14h30 no site www.gov.br/compras.

CARLOS ALBERTO BARLERA COUTINHO
Chefe da Seção de Licitações

(SIASGnet - 14/10/2022) 80026-00001-2022NE000022

DIRETORIA-GERAL

EXTRATO DE ACORDO DE COOPERAÇÃO TÉCNICA

Proc. 22.604/2022. Acordantes: TRT da 24ª Região, CNPJ nº 37.115.409/0001-63 e a Associação dos Magistrados da Justiça do Trabalho da 24ª Região - AMATRA XXIV, CNPJ nº 70.353.529/0001-74. Espécie: Acordo de Cooperação Técnica nº 11/2022. Objeto: Estabelecer condições relativas à dedução da mensalidade para custeio da CONSIGNATÁRIA (AMATRA XXIV) e consequente consignação em folha de pagamento, dos magistrados ativos e inativos do Tribunal Regional do Trabalho da 24ª Região. Vigência: 60 (sessenta) meses a contar de 18 de janeiro de 2023. Fundamento legal: Lei nº 8.666/1993. Data assinatura: 17.10.2022.

JUSTIÇA FEDERAL

1ª REGIÃO

SEÇÃO JUDICIÁRIA NO ACRE

EXTRATO DE CREDENCIAMENTO

Espécie: Termo de Credenciamento N. 16458932/2022 celebrado entre a União Federal, através da Justiça Federal de 1ª Instância - Seção Judiciária do Estado do Acre e L. HERTZ RODRIGUES (LUMINI PILATES). OBJETIVO: prestação de serviços de fisioterapia previstos na Cláusula Primeira do referido Termo de Credenciamento. DATA DE ASSINATURA: 14/10/2022 DATA DE VIGÊNCIA: a partir 14/10/2022, pelo tempo que for conveniente às partes. ASSINAM O INSTRUMENTO: Dr. JOSE GERALDO AMARAL FONSECA JUNIOR, Juiz Federal Diretor do Foro, pela Justiça Federal de 1ª Instância - Seção Judiciária do Estado do Acre - Pro Social, e LUISA HERTZ RODRIGUES, Administradora da empresa L. HERTZ RODRIGUES.

SEÇÃO JUDICIÁRIA NO AMAPÁ

EXTRATO DE DISPENSA DE LICITAÇÃO

Espécie: Dispensa de Licitação nº 24/2022. Processo: 0001013-47.2022.4.01.8003. OBJETO: aquisição e instalação de um painel central de detecção e alarme contra incêndio endereçável, com 4 laços, GEKKO 4L, da marca "Ezalpha", conforme Estudo Técnico Preliminar. Fundamento Legal: art. 75, II, da Lei n. 14.133/2021. Justificativa: Em razão do valor apresentado. Declaração de Dispensa: 8/9/2022. Maurício Pinheiro de Santana. Diretor da Secretaria Administrativa. Ratificação em 9/9/2022. Anselmo Gonçalves da Silva. Diretor do Foro. Valor Global: R$ 37.503,00. CONTRATADO: CRAVAL SOLUÇÕES, inscrita no CNPJ sob o n. 38.650.409/0001-26

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 18/2022 - UASG 90037

Nº Processo: 0000684-35.2022.4. Objeto: Contratação de empresa para execução dos serviços comuns de engenharia para lavagem e pintura das fachadas do prédio Sede da Justiça Federal no Amapá, contemplando: fachadas envidraçadas, áreas revestidas com pastilhas, áreas revestidas com granito, áreas revestidas com ACM, bem como lavagem e pintura das platibandas, pequeno reparo estrutural e demais superfícies externas em fachadas do edifício sede da Justiça Federal no Amapá.. Total de Itens Licitados: 1. Edital: 18/10/2022 das 10h00 às 17h00. Endereço: Rodovia Norte Sul, S/nº, Infraero Ii, - Macapá/AP ou https://www.gov.br/compras/edital/90037-5-00018-2022. Entrega das Propostas: a partir de 18/10/2022 às 10h00 no site www.gov.br/compras. Abertura das Propostas: 03/11/2022 às 10h00 no site www.gov.br/compras.

SANDRO ROGERIO MARQUES DE CARVALHO
Pregoeiro

(SIASGnet - 17/10/2022) 90037-00001-2022NE000032

SEÇÃO JUDICIÁRIA NA BAHIA

EXTRATO DE CONVÊNIO

Espécie: Convênio 16724265 celebrado entre a Justiça Federal de 1º Grau-Seção Judiciária da Bahia e a INSTITUIÇÃO BAIANA DE ENSINO SUPERIOR - FACULDADE DOM PEDRO II. CNPJ 05.817.107/0001-40. OBJETO: Propiciar a alunos de cursos de graduação (autorizados ou reconhecidos), da INSTITUIÇÃO DE ENSINO, regularmente matriculados e com freqüência efetiva, a realização de estágio na CONCEDENTE. BASE LEGAL: Lei n. 11.788/2008, da Resolução Presi - 7029958- do TRF1, da Resolução nº. CF-RES-2012/00208, de 04/10/2012, do Conselho da Justiça Federal, Resolução 315/2014 do Conselho de Justiça Federal e PAe - SEI 0010492-37.2017.4.01.8004. VIGÊNCIA: 24/10/2022 e término previsto para 23/10/2027. Dotação Orçamentária: PT nº 02.061.0569.4257.0001 - Julgamento de Causas na Justiça Federal - Nacional - ND nº 3.33.90.36.07 - Estagiários, Fonte 0127000000. Ass. em 13/10/2022. Representantes: Dr. Durval Carneiro Neto, pela Justiça Federal da Bahia e a Sr. Nelson Piauhy Dourado Neto, pela Instituição de Ensino.

EXTRATO DE DISPENSA DE LICITAÇÃO Nº 129/2022 - UASG 090012

Nº Processo: 11115282022 . Objeto: Contratação de empresa especializada para prestação dos serviços de recarga e testes hidrostáticos nos extintores de incêndio da Justiça Federal-Subseção Judiciária de Itabuna, com o fornecimento de todo material e ferramentas necessárias. Total de Itens Licitados: 00001. Fundamento Legal: Art. 24º, Inciso II da Lei nº 8.666 de 21º/06/1993.. Justificativa: Dispensa em razão do valor Declaração de Dispensa em 14/10/2022. TARCISIO JOSE FILGUEIRAS DOS REIS. Diretor Secad. Ratificação em 14/10/2022. DURVAL CARNEIRO NETO. Diretor do Foro. Valor Global: R$ 1.670,00. CNPJ CONTRATADA : 74.061.714/0001-46 PREVINCENDIO PREVENCAO CONTRA INCENDIO LTDA.

(SIDEC - 17/10/2022) 090012-00001-2022NE090012

AVISO DE DISPENSA DE LICITAÇÃO Nº 134/2022

DISPENSA DE Aquisição e instalação de ar condicionado
OBJETO: Aquisição e instalação de ar condicionado de 18.000BTU Split, Ciclo frio, tecnologia Inverter, 220V, com fornecimento de peças e ferramentas necessárias, para a Subseção Judiciária de Feira de Santana-SSJFSA.. PROC ADM SEI N. 0012072-29.2022.4.01.8004. Total de Itens Licitados: 01. Fundamento Legal: Art. 24º, Inciso II da Lei nº 8.666 de 21/06/1993. Justificativa: Dispensa em razão do valor. Declaração de