Ministério da Justiça - MJ
Conselho Administrativo de Defesa Econômica - CADE
SEPN 515 Conjunto D, Lote 4 Ed. Carlos Taurisano, 1º andar - Bairro Asa Norte, Brasília/DF, CEP 70770-504
Telefone: (61) 3221-8577 - www.cade.gov.br

CONTRATO Nº 36/2018

PROCESSO nº 08700.003102/2018-39

CONTRATO DE PRESTAÇÃO DE SERVIÇOS E FORNECIMENTO DE BENS QUE ENTRE SI CELEBRAM O CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA - CADE E A EMPRESA TECHBIZ FORENSE DIGITAL LTDA PARA A CONTRATAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE, ACESSOS PRIVILEGIADOS E CORRELACIONAMENTO DE EVENTOS.

CONTRATANTE:

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA - Cade, AUTARQUIA FEDERAL, vinculada ao Ministério da Justiça, criada pela Lei nº 8.884, de 11 de junho de 1994, com sede no SEPN 515, Conjunto D, Lote 4, Ed. Carlos Taurisano, CEP 70.770-504, em Brasília–DF, inscrita no CNPJ/MF sob o nº 00.418.993/0001-16, doravante designado Contratante, neste ato representado por sua Ordenadora de Despesa pro Subdelegação, Sra. **LUANA NUNES SANTANA**, brasileira, portadora Carteira de Identidade n.º 28153792-6 – SSP/SP e do CPF n.º 221.509.228-94, no uso da atribuição que lhe confere o art. 1º, inciso II, alínea "b", da Portaria n.º 460, de 29 de setembro de 2012; e

CONTRATADA:

ISH TECNOLOGIA S/A, inscrita no CNPJ/MF sob nº 01.707.536/0001-04, com sede no endereço Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES, CEP 29.050-360, fone: (27) 3334-8900, e-mail: helio.ferreira@ish.com.br, doravante denominado(a) **CONTRATADA**, neste ato representado a por seu representante legal, **Sr. HÉLIO FERREIRA DA SILVA JUNIOR**, Identidade nº 2107159 SSP/DF CPF nº 003.868.541-81, devidamente qualificado, na forma da Lei nº 8.666, de 21 de junho de 1993, tendo em vista o que consta no Processo nº 08700.003102/2018-39, resolvem celebrar o presente **CONTRATO,** sujeitando-se as partes ao comando da Lei n. 10.520, de 17 de julho de 2002 e Lei 8.666, de 21 de junho de 1993 e alterações posteriores e demais normas pertinentes, observadas as cláusulas e condições seguintes:

DA FINALIDADE

O presente Contrato tem por finalidade formalizar e disciplinar o relacionamento contratual com vistas à execução dos trabalhos definidos e especificados na Cláusula Primeira – DO OBJETO, conforme Parecer Jurídico nº 121/2018, datado de 07/11/2018, da Procuradoria do Contratante exarada no Processo nº 08700.003102/2018-39.

DO FUNDAMENTO LEGAL

O presente Contrato decorre de adjudicação à Contratada do objeto do Pregão Eletrônico 08/2018, com base, integralmente, a Lei nº 10.520, de 19 de julho de 2002, publicada no D.O.U. de 22 de julho de 200; Decreto 7.192 de 23 de janeiro de 2013; a Lei nº 8.078, de 11 de setembro de 1990, publicada no D.O.U de 12 de setembro de 1990; a Lei n° 12.529 de 30 de novembro de 2011, publicada no D.O.U. de 1° de novembro de 2011; o Decreto nº 3.555, de 08 de agosto de 2000, publicado no D.O.U. de 09 de agosto de 2000, o Decreto. nº 5.450, de 31 de maio de 2005, que regulamentam a modalidade de Pregão; a IN-SLTI/MP nº. 05/2017; Decreto nº 8.538/2015, que estabelece o tratamento diferenciado para as MEs e EPPs; a Instrução Normativa nº 1, de 19 de janeiro de 2010 a Instrução Normativa nº 02 da SLTI/MPOG, de 11 de outubro de 2010; e, subsidiariamente, pela Lei nº 8.666/93 e alterações posteriores, conforme especificações constantes do Processo Administrativo nº 08700.003102/2018-39.

1. **CLÁUSULA PRIMEIRA - DO OBJETO**

1.1. Contratação de soluções de gerenciamento de identidade, gerenciamento de acessos privilegiados e correlacionamento de eventos, provendo ao Conselho Administrativo de Defesa Econômica - Cade - capacidade de gerenciamento de privilégios mínimos, autenticação transparente, múltiplos fatores de autenticação e adoção de provisionamento de acessos; geração de relatórios sobre eventos, otimização nas rotinas de identificação, detecção e análise de eventos e incidentes, armazenamento de registros de ativos de rede unificado, com resposta e remediação de incidentes de rede.

Grupo	Item	Descrição	Unidade de medida	Quantidade

3	9	Solução de correlacionamento de eventos com serviço de garantia pelo período de 60 (sessenta) meses	Eventos por segundo (EPS)	3000
	10	Serviço de instalação e configuração para a solução de correlacionamento de eventos	Serviço	1
	11	Treinamento oficial com o fabricante da ferramenta de correlacionamento de eventos	Pessoa	3
	12	Serviço de customização para a solução de correlacionamento de eventos	Unidade de serviço técnico (UST)	1000

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. O presente Contrato vincula-se, independentemente de transcrição, à proposta da Contratada, ao Edital do Pregão Eletrônico nº 08/2018, com seus Anexos e os demais elementos constantes do Processo nº 08700.003102/2018-39.

3. CLÁUSULA TERCEIRA - DOS REQUISITOS

	Solução de correlacionamento de eventos com serviço de garantia pelo período de 60 (sessenta) meses	1. Ser licenciada de forma que não limite o Cade à quantidade de usuários, dispositivos monitorados e/ou relatórios gerados. Caso a solução ofertada apresente modalidade de licenciamento por usuários, dispositivos monitorados e/ou relatórios gerados, deverá ser apresentado o valor prevendo licenciamento ilimitado para os itens apresentados; 2. Ser de licença perpétua para o Cade; 3. Permitir o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório como Microsoft Active Directory e LDAP; 4. A distribuição dos módulos, conectores ou agentes - o que for aplicável ao correto funcionamento da solução - no ambiente tecnológico deve ser livre, no sentido de permitir a conexão com os ativos do Cade sem a necessidade de licenças adicionais, dentro do limite de processamento e indexação licenciados; 5. A modalidade de licenciamento deverá permitir a distribuição livre de elementos de coleta, filtragem e agregação, gerados com o uso de SDK ou API (Application Programming Interface), independentemente do número e arquitetura; 6. A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar 4.000 eventos por segundo de forma sustentada, ou 150 gigabytes (GB) por dia; 1. Deve-se considerar os eventos com tamanho médio de 400 bytes; 7. Deve ter capacidade de coletar, processar e correlacionar flows de rede NetFlow v9, a uma taxa de 25.000 sessões IP únicas por minuto, de forma sustentada; 1. Cada sessão deve ser considerada como composta por 2 flows entrante (inbound) e sainte (outbound)

do tráfego monitorado de protocolos IP, TCP, UDP, ICMP, dentre outros protocolos IP;

2. A solução deve garantir o processamento do fluxo de eventos gerados pelos dispositivos, sem limitação por dispositivo em qualquer momento (pico, vale ou operação normal);

8. Permitir a instalação de todos os seus componentes em ambiente virtual ou servidores físicos;
9. Ser instalada em Hyper-V nas versões do Windows Server 2012 ou superiores;
    1. A ferramenta poderá ser instalada em outro sistema operacional, desde que compatível com o *hipervisor* acima e devidamente licenciado, se aplicável;
    2. Caso não seja compatível, a solução deverá ser entregue com *hardware* e licenças de *software* (ex.: *hypervisor* diverso ao do item acima ou sistema operacional específico) que a compatibilize com as ferramentas de infraestrutura do Cade;
    3. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação;
10. Ser virtualmente ilimitada (conforme políticas internas de retenção) no volume de dados coletados, processados e armazenados, sendo limitada apenas ao volume de dados licenciados neste certame;
11. Todas as funções abaixo deverão ser executadas pela mesma solução tecnológica. Caso sejam necessários componentes externos, os mesmos devem fazer parte da solução proposta;
12. Suportar a coleta de dados de no mínimo 250 (duzentos e cinquenta) geradores, com documentação completa individual por tecnologia;
    1. Caso a solução trabalhe sem agentes (*agentless*), deverá prover funcionalidades análogas, sem perda de caracterização da solução;
13. Capacidade de definir política de retenção dos dados em on-line, near-line e off-line, onde:
    1. on-line: dado mantido no banco de dados da solução, disponíveis para consulta imediata;
    2. near-line: dados que não estão no banco de dados da solução, mas encontram-se arquivados em dispositivos de acesso direto pelo mesmo, podendo ser recuperados imediatamente para consulta;
    3. off-line: dados que estão arquivados em mídias externas de backup (CD, DVD, fita. etc), sem acesso direto pela solução e que precisam ser restaurados e reativados para consulta.
14. Ter seu coletor de dados com funcionalidades de coletar, aplicar *parsing*, normalizar, classificar, agregar informações, sumarizar, processar regras, compactar e armazenar os dados recebidos dos elementos geradores de eventos presentes no ambiente tecnológico;
15. Ter seu correlacionador a capacidade de processar regras tanto em tempo de coleta como em tempo de análise, analisar e correlacionar eventos globais advindos dos dispositivos do ambiente tecnológico e aplicar regras de

correlacionamento e análise conforme regras configuráveis antes, durante e após o processamento. Essas regras serão definidas e customizadas na fase de instalação e configuração da solução;

16. Ter um sistema de armazenamento de eventos capaz de receber informações e dados enviados pelos ambientes tecnológicos, ou de diferentes fontes, compactar, organizar e armazenar e gerenciar todo o ciclo de armazenamento da solução, garantida a integridade do dado no formato *raw*;
17. Ter um console de monitoramento e operação para visualizar os dados dos dispositivos do ambiente tecnológico exibindo resultados que proporcionem o controle sobre o ambiente corporativo no ponto de vista de:
    1. Análise de incidentes;
    2. Segurança da informação na perspectiva de SIEM (alertas) e forense (correlação, pesquisas ad hoc e relatórios);
    3. Análise de segurança da informação garantindo a integridade dos eventos e evidências;
18. Ter uma console de monitoramento com uma base de conhecimento na interface do usuário para pesquisa e solução relativa ao incidente e criação de novos painéis de monitoramento;
19. Ser possível visualizar os painéis de monitoramento e incidentes exibindo resultados que proporcionem o controle sobre a segurança corporativa, fornecendo várias formas de classificação e visualização dinâmicas dos eventos;
20. Ser capaz de implementar o recebimento de eventos de análise comportamental de rede;
21. Implementar a análise de fluxos (*flows*) e de eventos por uma interface de gerência;
22. Receber os fluxos por pelo menos um dos seguintes protocoloes: Netflow, sflow, flowlog e packeteer e permitir a demonstração sobre utilização da rede entrante (inbound) e sainte (outbound), visualização de protocolos utilizados na rede e criação de regras de alerta sobre protocolos indesejados;
23. Permitir investigação de ataques, anomalias, alvos de ataque, atacantes da rede e correlacionar eventos e atividades de rede, bem como identificar os alvos;
24. Emitir relatórios executivos, operacionais e de conformidade a normas de mercado e flexibilidade na criação de novos relatórios pelos próprios usuários, sem interferência de componentes externos ou a necessidade de customização em código complexa que exija serviços profissionais terceiros;
25. Visualizar os dados dos dispositivos do ambiente tecnológico de forma centralizada, fornecendo um conjunto de funções e indicadores gerenciais específicos, contemplando o panorama de monitoramento e segurança no ambiente da instituição e flexibilidade na criação de novos relatórios pelos próprios usuários, sem interferências de componentes externos ou a necessidade de customização em código complexa que exija serviços profissionais terceiros;
26. Desenvolvimento de regras para o correlacionamento para possibilitar a criação de regras de correlacionamento, através de ferramenta gráfica ou linha de comando. A solução deverá prover módulo de construção e testes de regras. Toda a construção das regras deverá ser feita em ambiente gráfico e as regras deverão possibilitar ações, como por exemplo, enviar e-mails e traps SNMP;

27. Ser capaz de agregar informações sobre a localização geográfica dos endereços IP envolvidos no evento;
28. A comunicação entre os componentes da solução deve ser feita através de criptografia, com uso de algoritmos RSA 2048, AES (128 bits ou mais) e/ou 3DES (192 bits ou mais), garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP;
29. Prover juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato de suporte, o acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento
30. Permitir a criação de usuários com diferentes níveis de acesso;
31. Permitir a coleta, processamento e normalização tanto de eventos de segurança, quanto a de negócios;
32. Ser capaz de realizar consulta por eventos em tabelas de bancos de dados MySQL, Microsoft SQL Server 2008 e superiores;
33. Permitir autenticação de usuário no mínimo em uma base LDAP/Active Directory, RADIUS, e base local;
34. Implementar IPv6;
35. A comunicação entre os dispositivos do ambiente tecnológico geradores os dados e a solução deve ser feita no mínimo por meio dos protocolos a seguir: SYSLOG, SDEE, SNMPv1, SNMPv2 e SNMPv3, além da capacidade de mapeamento de pastas de redes ou serviços nativos de coleta de dados;
36. A solução deve possuir capacidade de acesso via web de forma segura (HTTPS), para monitoração, gerenciamento e geração de relatórios;
37. A coleta de eventos de dispositivos não suportados nativamente pode ser feita através de conectores customizados. Estes conectores customizados devem utilizar padrões de mercado como CSV, arquivo texto, XML, CheckPoint LEA, ODBC, JDBC, JSON, ou pela criação de campos realizado dentro da própria solução;
38. Possuir a funcionalidade de ler e normalizar eventos de log armazenados em formato texto (w3c), SQL database, compactados ou não;
39. Ofuscar os campos sensíveis dos eventos (senhas, identidade funcional, números de cartões de crédito e outros similares);
40. Marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, divisão corporativa ou similar;
41. Filtrar e selecionar os eventos que serão inseridos na solução e permitir a criação e alteração de filtros;
42. Os conectores, ou solução similar, deverão coletar de forma nativa as plataformas: Windows, Linux (RHEL, Debian), AIX, HPUX, sempre na última versão;
43. Os conectores, ou solução similar, deverão coletar de forma nativa as soluções de:
    1. Antivírus: Symantec, Mcafee, Kaspersky e Trend;
    2. Antispam: Proofpoint, Mcafee e Trend;
    3. Firewall: Checkpoint, Fortinet, Cisco e Palo Alto;

4. IPS: Checkpoint, Sourcefire, Tipping Point e McAfee;
5. Firewall de Aplicação: Fortinet, Radware, F5 e Imperva;
6. Switches: Cisco e HP;

44. Coletar e aplicar parsing (segmento do dado) nos eventos do dispositivo monitorado em tempo próximo ao real;
45. Definir prioridade para o evento, alerta e incidente;
46. Correlacionar os eventos recebidos através de regras de correlacionamento e análise conforme regras configuráreis antes, durante e após o processamento dos dados recebidos;
47. Gerar alertas com base nas regras criadas;
48. A solução deve ser composta de agentes que têm como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução;
49. Suporte ao padrão de criptografia FIPS, em todos os conectores;
50. Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional;
51. Separar eventos por meio de anotações em campos, originados por quaisquer campos disponíveis e normalizados (ex: Cliente 1 - VLAN ID 10, Cliente 2 - VLAN ID 20) mesmo que o evento seja de um mesmo firewall;
52. Verificar conformidade com as políticas, controles e normas internas e externas;
53. A solução deve ser capaz de normalizar e categorizar os eventos em um padrão único;
54. O componente de coleta de eventos deve suportar a captura, a normalização e o tratamento de eventos em tempo próximo ao real;
55. O coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade do componente correlacionador;
56. Deve permitir a configuração do tamanho do cache;
57. O envio dos dados em cache deve ocorrer imediatamente a disponibilização do correlacionador;
58. A solução deve ser capaz de enviar o evento bruto (raw) para armazenamento e consulta futura;
59. Armazenar os eventos e os alertas, com pesquisa imediata aos eventos de origem que os geraram, apontando os eventos raw;
60. Permitir pesquisas nos eventos históricos, fornecendo capacidade de “drill-down”, ou seja, visualizar detalhes dos eventos, inclusive os dados em formato “raw”, quando aplicável, para análise forense e investigação de incidentes;
61. Efetuar a análise dos eventos de segurança da informação em tempo real, garantindo a integridade do dado raw como evidência legal;
62. Informar os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando estes eventos raw a partir do evento de alerta/incidente;
63. Deverá ter a capacidade de guardar eventos *online* brutos em forma comprimida com compactação na proporção

de pelo menos 1:4;

64. Deve permitir acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. Esse horário deve ser obtido pelo sistema através de sincronização com servidores NTP previamente definidos, e sincronizado entre todos os componentes da solução;
65. A solução deve ser capaz de marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, secretaria ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento;
66. A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos, ainda que sejam endereços privados;
67. Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução;
68. A solução deve permitir múltiplos perfis de configuração;
69. A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo;
70. Enviar mensagens por e-mail, SMS (por customização para serviço de mensageria contratado pelo Cade) e TRAP SNMP;
71. Deverá implementar alertas por syslog, SNMP e e-mail;
72. Todo serviço técnico para coleta dos dados dos dispositivos do ambiente tecnológico devem estar inclusos na proposta técnica;A solução deve ser capaz de coletar dados dos mais diversos dispositivos do ambiente tecnológico, garantindo que quaisquer alterações do atual ambiente tecnológico sejam suportados;
73. Painel de gerenciamento centralizado de todos os dispositivos do ambiente tecnológico;
74. Identificar rapidamente a causa raiz dos incidentes detectados no ambiente em console única;
75. Criação de relatórios e alertas em tempo real para todos os ativos da TI, correlacionando os eventos independente de dispositivos do ambiente tecnológico de origem;
76. Capacidade de monitoramento de ambientes virtualizados em todas as suas camadas (virtualização, aplicação, sistemas operacionais, rede, servidores físicos e storages);
77. Alertas configuráveis para: notificação em painel de monitoramento, envio de e-mail e execução de scripts;
78. Implementar relatórios do grau de conformidade com normas reguladores de mercado, para no mínimo as seguintes normas: COBIT, ISO/IEC família 27000;
79. Emissão de relatórios de conformidade do ambiente monitorado em relação à norma ISO/IEC 27001 e ISO/IEC 27002, com base nos eventos recebidos;
80. Possibilitar criação de regras, painéis gráficos (dashboards) e relatórios para monitorar normas internas;
81. Capacidade de criação de novas regras, padrões de monitoramento e alertas, além de alteração das existentes;
82. Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);
83. Permitir testar as regras com eventos reais capturados anteriormente e mantidos na base de dados da solução,

sem afetar a execução das regras em produção;

84. Executar regras de correlação pré-programadas. Deve permitir a criação de novas regras e a edição das existentes;
85. Identificar anomalias baseadas em eventos e análise de dados históricos;
86. Permitir o correlacionamento de eventos e alerta com dados existentes em listas (watchlist), criação de novas listas e edição das existentes, tanto de forma automatizada quanto manual;
87. Deve ter capacidade de sumarizar múltiplos alertas idênticos automaticamente;
88. Deve identificar e correlacionar diferentes assinaturas de diferentes dispositivos possibilitando a identificação única de ataques particulares;
89. Permitir execução de regras agendadas, que rodam em frequência e horário especifico, sem ficarem ativas em tempo real;
90. Capacidade de fazer o correlacionamento entre eventos oriundos de qualquer tipo de dados dos dispositivos do ambiente tecnológico, nativamente e em tempo real;
91. Reinserir no próprio fluxo de correlacionamento os alertas gerados a partir de regras de correlação, visando correlacionar este alerta como novos eventos e/ou outros alertas no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade;
92. Priorizar os eventos e alertas com base pelo menos nos critérios de severidade do evento e criticidade do ativo;
93. Armazenar os eventos, alertas e incidentes na base de dados da solução de forma indexada;
94. Fazer a agregação de eventos semelhantes que ocorrem dentro de um limite de tempo ou quantidade de eventos específicos, sendo que permite agregar tanto os eventos cuja única diferença seja o horário de ocorrência;
95. Suportar pesquisa automática dos ataques que foram detectados e permitir o armazenamento destas informações para fins de forense computacional e referências futuras;
96. Deve implementar funcionalidade de agendar relatórios de segurança em múltiplos perfis. Os relatórios deverão ser gerados automaticamente (agendados) com frequência e intervalo de tempo a serem definidos pela instituição, conforme perfis dos elementos gerenciados;
97. Deverá possuir detalhes sobre cada incidente, incluindo:
    1. contexto adicional a partir de fontes de ativos e de identidade externa;
    2. o evento (s) – prima que constitui o incidente;
    3. capacidade de alterar manualmente severidade do incidente, proprietário e status, bem como adicionar notas a um incidente.
98. O sistema deverá detectar o uso indevido da rede, como tentativa de acessar arquivos que o usuário não tenha permissão;
99. O sistema deverá detectar ataques como de força bruta ou exploração de alguma vulnerabilidade;
100. Prever acesso único e exclusivo aos dados, implementação de políticas de controle de acesso, auditoria e controle de tráfego dos dados;

101. Possuir a compressão automática de dados indexados para reduzir os requisitos de armazenamento;
102. Possuir controle granular sobre o que acontece com os dados à medida que envelhece, sendo capaz de transferir dados mais antigos para armazenamento externo/mais barato e/ou excluídos;
103. Solução deve possuir capacidade de se integrar com Storages (SAN/NAS) de mercado para armazenamento de dados;
104. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada;
105. Os dados dos dispositivos do ambiente tecnológico devem ser armazenados em base de dados única (parte integrante da solução);
106. Deve ser capaz de realizar a classificação de alertas em níveis de criticidade;
107. Deve possuir mecanismos que proporcionem a exibição da informação de forma amigável e compreensível após coleta e normalização dos eventos;
108. Deve classificar eventos de acordo com os grupos de ativos afetados e sua criticidade para o negócio da empresa, por meio de parâmetros pré-definidos;
109. Permitir a categorização manual de eventos (já normalizados) inéditos não categorizados por padrão. Esta categorização deverá ser aplicada nos eventos futuros de mesma característica;
110. Deve possuir regras de correlação de segurança prontas baseados em padrões de mercado;
111. Deve permitir a criação de regras de correlação específicas e customizadas, diferentes da nativa, e possuir capacidade de copiá-las para outras instâncias;
112. Deve suportar criação de regras de maneira gráfica, não necessitando de linguagem de script ou de programação;
113. Deve permitir a identificação de anomalias a partir de eventos inéditos e através de análise histórica do comportamento de rede (flows);
114. Deverá funcionar com banco de dados especializado em eventos do próprio fabricante, não sendo permitida a utilização de banco de dados open source ou comerciais de propósito genérico.
    1. Caso seja utilizado banco de dados de terceiros, as licenças devem ser fornecidas juntamente com a solução;
    2. Deve possibilitar que os dados no banco sejam extraídos em forma de relatório em CSV ou encaminhados via CEF ou LEEF para outras soluções.
115. Gerenciamento de ciclo de vida do dado, da coleta, armazenamento (como movimentação automática entre disco local e storage) e rotação (armazenamento externo e/ou eliminação do dado) – com regras e parâmetros;
116. Arquitetura tolerante a falhas, com replicação dos dados e serviços;
117. Indexar todos os dados, não modificando o formato original e torná-lo pesquisável (nenhum esquema pré-definido, ou normalização de dados / redução em tempo de coleta);
118. A solução deve possuir sistema de auditoria de uso. Cada evento de auditoria deve possuir, no mínimo, os seguintes campos:

1. data e horário da ação executada pelo usuário;
2. identificação do usuário que executou a ação;
3. informação sobre a ação executada.

119. Permitir o agendamento de geração de relatórios periódicos e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;
120. Deverá apresentar painéis gráficos (dashboards) com indicativos de situações diversas, facilmente configuráveis e com ferramentas que facilitem a criação pelos usuários;
121. Deverá permitir a fácil criação de uma vasta gama de efeitos visuais (não se limitando a, relatórios pré-definidos e fixos):
    1. tabelas;
    2. gráfico com agrupamento em período de tempo;
    3. gráficos de linhas;
    4. gráficos de barras;
    5. gráficos de área;
    6. gráficos de pizza;
    7. mapas Geo – IP;
122. Deverá permitir para todos os gráficos, capacidade fácil mudar títulos, legendas e rótulos do eixo e as configurações;
123. Deverá ter capacidade de integração com as estruturas externas de visualização e opções (Qlikview, Tableau, etc..) para visualizações adicionais por meio de conectores ODBC ou similares;
124. Capacidade de geração de relatórios Ad Hoc e compartilhamento do resultado final com outros usuários;
125. Gerar relatórios ocultando campos sensíveis dos eventos (senhas, números de cartões de credito, importâncias monetárias e outros similares);
126. Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;
127. Capacidade de criação de modelos de relatórios e alteração dos existentes através de interface gráfica;
128. Funcionalidades para a administração da solução com interface gráfica via browser que atenda de forma intuitiva, utilizada para as atividades de administração, configuração e gerenciamento do ambiente;
129. Possuir capacidade de integração com Microsoft Active Directory e bases LDAP (Lightweight Directory Access Protocol) inclusive na sua versão Open Source OPENLDAP, para autenticação de usuários;
130. Fornecer visualização e ações diferenciadas por perfis de acesso;
131. As visualizações e ações devem ser customizadas por grupos de usuários, conforme critério do Cade;
132. Ter capacidade de efetuar a segregação de funções dos usuários da solução;
133. Segregação de visualização de eventos, alertas, conteúdo de dashboard e de relatórios por usuários, sem necessidade de criar visualizações, dashboards e relatórios customizados para cada grupo de usuários;
134. Capacidade de gerenciamento e configuração centralizados de todos os componentes distribuídos da solução;

135. Capacidade de atualização centralizada de todos os componentes da solução.
136. Deve possuir integração com soluções de gestão de patches como, no mínimo, o Microsoft System Center Configuration Manager (SCCM).
137. A solução deve poder coletar dados de feeds externos;
138. Para a coleta de dados e feeds externos deve suportar, no mínimo, os seguintes formatos/protocolos/fontes:
    1. STIX/TAXII;
    2. Bases de reputação de endereço IP e URL's;
    3. Bases de índice de comprometimento (IOC) próprios do fabricante;
139. Para coletar de logs deve suportar, no mínimo, os seguintes métodos:
    1. Syslog (UDP, TCP e TLS);
    2. CIFS;
    3. FTP;
    4. SCP;
    5. MySQL;
    6. MS SQL;
    7. Postgres;
    8. API.
140. Prover mecanismo de coleta de logs de dispositivos não suportados nativamente, através de personalização de coletores, ou solução similar, porém sem linguagem de programação ou kits de desenvolvimento;
141. Prover um IP virtual a ser configurado como destino das fontes geradoras de evento syslog;
142. Armazenar os dados: eventos, alertas, incidentes, bases de conhecimento, workflow nativo e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração.
143. Permitir o expurgo dos dados de forma automática com a personalização do período de tempo do expurgo;
144. Deverá permitir exportar eventos para formato csv em estruturas NFS, SAN e localmente. Deverá permitir que o usuário defina quais campos do evento serão exportados;
145. Deverá implementar acesso autenticado, caso não use usuário de domínio;
146. Deverá permitir a livre customização da interface, com dashboards customizados;
147. Deverá permitir a configuração de tempo de inatividade, após o qual o usuário será desconectado automaticamente;
148. Deverá ser fornecido com dashboards pré-configurados e permitir a criação de novos dashboards;
149. Deverá implementar dashboards de monitoração de resultados históricos e em tempo real;
150. Deverá permitir a criação de dashboards diretamente dos resultados da pesquisa, sem necessidade de configuração manual;
151. Deverá possuir dashboard pré-configurados pelo menos para firewall, entre outros;
152. Deverá permitir a procura por texto, campos pré-definidos, palavras chaves, operações boleanas e expressões regulares;
153. Deverá permitir a utilização de procuras complexas através do encadeamento de comandos de consulta (pipeline

format ou similar a SQL);
154. Deverá permitir a configuração da visualização do resultado em formato de tabela e gráfico;
155. Deverá permitir a configuração do escopo de procura como local e distribuída por alguns ou todos os elementos da solução;
156. Deverá permitir a gravação da query de procura em formato de filtro para utilização futura;
157. Deverá permitir a gravação dos resultados da pesquisa em arquivo;
158. Deverá implementar assistente gráfico para criação de queries;
159. Deverá implementar funcionalidade de sugestão de termos de procura enquanto se digita os critérios de pesquisa (recurso auto completar);
160. Deverá implementar indexação baseada em campo e palavra-chave para acelerar buscas;
161. Deverá permitir visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário;
162. Possuir relatórios pré-configurados separados em categorias;
163. Possuir a funcionalidade de apresentação de relatórios de eventos, alertas e incidentes em nível técnico e gerencial;
    1. Deverá suportar os seguintes formatos de relatóros: HTML, PDF, CSV, RTF, XLS e XML;
164. Permitir a publicação de relatórios e a configuração de expiração do relatório;
165. Permitir o agendamento de relatórios e o envio dos mesmos por e-mail;
166. Possuir ferramenta gráfica para desenho de modelos de relatórios personalizados;
167. A partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e fazer drill-down do mesmo para efetiva investigação e identificação de causa raiz;
168. Permitir pesquisa nos eventos históricos, fornecendo capacidade de drill-down, ou seja, visualizar os detalhes dos eventos, inclusive dados raw, quando aplicável, para análise forense e investigação de incidentes;
169. O algoritmo de integridade utilizado no armazenamento pode ser configurado entre os seguintes: MD5, SHA-1, SHA-256 e SHA-512;
170. Capacidade de armazenar eventos em dispositivos externos;
171. A solução deve permitir a geração de relatórios baseados em queries personalizadas e relatórios consolidados, onde o nível de detalhamento da informação possibilite a análise aprofundada das ocorrências coletadas pela solução, pemitindo uma remediação maior entre a decisão do gestor e o atingimento do resultado esperado.
172. A solução deve possuir a capacidade de gerenciar o armazenamento de longo prazo de dados de inteligência de TI em um repositório central (mínimo de 3 anos);
173. Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria (Ex: HMAC com SHA-2) devidamente reconhecidos como seguros
174. Deverá implementar a correlação entre informações de arquivos externos e logs coletados pela solução;
175. Deverá permitir que os campos de logs de fontes diferentes estejam presentes no mesmo resultado. Deverá ser possível a seleção dos campos que estarão presentes no resultado;
176. Deverá permitir acrescentar campos de uma fonte em outra fonte;

177. Apresentar painéis de controles gráficos (dashboards) que mostrem o status do ambiente, dos logs de eventos, além de apresentar resultados de Queries tempestivas, quando se fizerem necessárias.
178. Deverá implementar dashboards com visualização de EPS de entrada, EPS de saída e utilização de CPU;
    1. Caso a ferramenta utilize outra métrica, como GB/dia, a visualização acima deverá ser do licenciamento padrão da solução;
179. Permitir a pesquisa (queries) no histórico de eventos, fornecendo capacidade de drill-down, ou seja, visualizar os detalhes dos eventos, inclusive o raw event (dado cru), quando aplicável, para análise forense e investigação de incidentes.
180. Módulo de User Behavior Analytics (UBA) licenciado para processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM, quando aplicável, ou devem considerar o total de contas monitoradas (contas de usuários + contas de serviços) de 500 contas;
181. Deve integrar nativamente com a solução de SIEM e ser capaz de extrair os dados de usuário e ações executadas dos eventos coletados para geração de score de risco;
182. Deve ser capaz de importar dados de usuário em bases LDAP e Windows AD para identificação da pessoa associada a conta do sistema monitorado, deve ser capaz de coletar e associar no mínimo: nome completo, departamento, contas associadas, email e cargo;
183. Permitir a criação de listas de observação com os principais usuários sob monitoração;
184. Deve permitir a isenção de determinadas identidades do processo de score de risco. Essas identidades não teriam riscos computados relacionados as suas atividades;
185. Deve permitir a inclusão de anotações dentro da monitoração de cada identidade com o objetivo de melhor gerenciamento de risco e do histórico e ações tomadas;
186. Deve possuir dashboards dos usuários com maior pontuação de risco e realizar um drill-down para entender quais as categorias de risco e as ações que contribuiram para o score atual;
187. Deve permitir ajustar os critérios e pontuações de riscos já existentes na ferramenta como também criar novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou precisam ser monitoradas;
188. Deve ser capaz de aprender de forma supervisionada e/ou não supervisionada os padrões de cada usuário;
189. A monitoração de desvios de comportamento de usuário deve detectar no mínimo:
    1. Tentativa de acesso a contas suspensas;
    2. Usuário acessando a VPN a partir de uma localidade atípica;
    3. Usuário acessando a VPN a partir de horários atípicos;
    4. Conta utilizada numa quantidade atípica de atividades;
    5. Primeiro uso de um recurso importante por um usuário;
    6. Acesso a endereços considerados suspeitos (Threat feed e IP reputation); e
    7. Detecção de usuário que execute comandos contidos em blacklist.
190. A Contratada deverá fornecer suporte da solução por um período mínimo de 60 (sessenta) meses para

atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante se necessário, além do nível de suporte prestado pela Contratada.

191. Esse serviço poderá ser renovado conforme inciso II, art. 57 da Lei n º 8.666/1993.
192. A Contratada deverá apoiar o Cade em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura;
193. A Contratada deverá realizar visitas proativas mensais para verificação do correto funcionamento e eventuais dúvidas do Cade. Durante o primeiro ano, as visitas proativas serão quinzenais durante os primeiros 6 meses e mensais para os 6 meses seguintes;
194. As visitas ocorrerão a partir da primeira semana após a assinatura do Termo de Recebimento Definitivo da instalação e configuração do respectivo grupo de ferramentas contratadas;
195. A Contratada deverá realizar a configuração das ferramentas que compõem as soluções, a fim de garantir o uso eficiente delas;
196. A Contratada deverá obedecer critérios de nível de serviço;
197. Sempre que houver atendimento, a contratada deverá enviar relatório de atividades por email para o Cade;
198. O prazo de garantia será contado a partir da emissão do Termo de Recebimento Definitivo da solução;
199. Em caso de mudança da sede deste Conselho para outro local no Distrito Federal, a execução de garantia deverá continuar sendo prestada, nas condições estabelecidas no Edital no endereço da nova sede;
200. O suporte técnico da contratada deve ser 8x5, ou seja, 8 (oito) horas por dia em 5 dias da semana, em horário comercial, em língua portuguesa;
201. A contratada deverá acionar o fabricante da solução sempre que necessário, sem nenhuma custo adicional para o Cade.
202. Os serviços de suporte técnico têm por finalidade garantir a sustentação e a plena utilização da solução durante a vigência do contrato. Inclui o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software e dos equipamentos ou para correção de problemas desses, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução. Deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TI (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução;
203. Deve contemplar a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e *release*, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a contratada deverá comunicar o fato a contratante e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção;

		204. A contratada será responsável pelos serviços de implantação das novas versões e *releases* dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos *patches* de correção e pacotes de serviço (*service packs*) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos *patches*, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na contratante; 205. Deverá ser prestado suporte técnico presencial e/ou remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela contratada e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução contratada; 206. Em caso de *hardware*, as peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento; 207. A contratada auxiliará o Cade na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta; 208. A contratada deverá auxiliar o Cade na comunicação junto ao fabricante; 209. A contratada deverá disponibilizar os seguintes canais de acesso ao suporte técnico: Portal Web, E-mail, Central 0800 e/ou telefone fixo.
12	Serviço de instalação e configuração para a solução de correlacionamento de eventos	1. Compreende-se nesta etapa a instalação das soluções deverá ser realizada no prazo abaixo, a contar do Termo de Recebimento Provisório da entrega das soluções: 1. Correlacionamento de eventos - até 60 (sessenta) dias. 2. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Cade. 3. As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana. 4. Para esta etapa o Cade disponibilizará a infraestrutura de *hardware* e *software* necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados (exceto para a solução de correlacionamento de eventos), e outros, para a instalação e configuração da solução. 5. A montagem e instalação de todos os componentes que componham solução adquirida são de responsabilidade da Contratada; 6. Os componentes de *software* deverão estar na versão mais atualizada da solução; 7. A Contratada deverá listar ao Cade todas as informações necessárias para a correta instalação e configuração da solução; 8. O Cade deverá providenciar as informações necessárias para a correta instalação da solução. 9. A Contratada prestará a transferência de conhecimento no formato *hands-on* para a equipe técnica da instituição na implantação da solução, ao longo das atividades de configuração, bem como durante atividades de suporte e customização; 10. A Contratada elaborará manuais e procedimentos técnicos e operacionais da solução durante a implantação.

13	Treinamento oficial com o fabricante da ferramenta de correlacionamento de eventos	1. O treinamento oficial do fabricante será de, no mínimo, 40 horas; 2. O treinamento será realizado preferencialmente no modelo presencial, nas dependências do Cade, ou em instalações providas pela Contratada; 3. O treinamento poderá ser realizado no modelo telepresencial (*online* por videoconferência), em português, utilizando ferramenta própria disponibilizada pela fabricante (ex.: Cisco Webex, Adobe Connect, etc.), de acordo com autorização da Contratante; 1. O Cade disponibilizará os computadores a serem utilizados pelos participantes do curso; 2. A empresa disponibilizará ambiente virtual para execução do treinamento; 4. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento; 5. Caso não haja disponibilidade para realização nos modelos presencial ou telepresencial, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.
14	Serviço de customização para a solução de correlacionamento de eventos	1. A Contratada prestará o serviço de customização com a equipe técnica do Cade no decorrer da vigência do contrato oriundo do presente processo. 2. As customizações são incrementos no uso da ferramenta que extrapolem a mera configuração dos recursos já existentes ou não se caracterizem como serviço de suporte; 3. Sobre a customização das soluções, os serviços abrangem casos como: 1. Realizar customizações que demandem desenvolvimento de scripts, automações avançadas, *dashboards* e congêneres; 2. Integração da solução com novas tecnologias adquiridas pelo Cade; 3. Instalação nova da solução em função de recuperação de desastre de ambiente; 4. Consultoria utilizando as melhoras práticas adotadas para as soluções. 4. A Unidade de Serviço Técnico - UST representa 1 hora de trabalho da Contratada. 5. Antes de iniciar uma ordem de serviço, a Contratada deverá estimar o esforço para execução do serviço em UST. 6. A Contratante acompanhará e contabilizará a utilização das UST utilizadas.

3.1. **REQUISITOS DA ENTREGA (TEMPORAL)**

3.1.1. A entrega dos equipamentos físicos da solução, caso existam, ocorrerá em Brasília, na Conselho Administrativo de Defesa Econômica, situado no SEPN 515, Conjunto D, Lote 04 - Edifício Carlos Taurisano, Asa Norte, em Brasília/DF;

3.1.2. O prazo da entrega, contado a partir da assinatura do contrato e/ou a entrega da Ordem de Serviço ou Fornecimento de Bens à Contratada, considerando o que acontecer primeiro, será de até 45 (quarenta e cinco) dias.

3.1.3. A entrega da solução dos equipamentos deverá ser agendada em data e hora a ser combinada previamente com a Coordenação-Geral de Tecnologia da Informação - CGTI, por meio do telefone (61) 3221-8552 e/ou e-mail cgti@cade.gov.br;

3.1.4. O transporte dos equipamentos até o Conselho Administrativo de Defesa Econômica deverá ser realizado pela Contratada, inclusive os procedimentos de seguro, embalagem e transporte até o espaço alocado pelo Cade para guarda;

3.1.5. Caberá ao Cade rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Contrato.

3.1.6. O recebimento dos equipamentos será efetivado pela equipe designada pelo Cade, e dar-se-á da forma provisória e definitiva.

3.1.7. A instalação das ferramentas será realizadas nos prazos estipulados no item 3.17.11;

3.1.8. A garantia do fabricante de 60 (sessenta) meses são contados nos prazos estipulados no item 3.17.11;

3.1.9. O serviço de suporte técnico será válido mediante abertura de Ordem de Serviço, após a conclusão da instalação e configuração dos produtos;

3.1.10. A assistência técnica da garantia será realizada a pedido do Cade pela contratada ou suas autorizadas;

3.1.11. A Contratada para a solução de gerenciamento de identidades deverá seguir os seguintes prazos:

Descrição	Início da Execução	Finalização da Execução
Entrega da solução de gerenciamento de identidades	1º dia útil após a assinatura do contrato	Até 45 (quarenta e cinco) dias contados da data de assinatura do contrato
Instalação e configuração da solução de gerenciamento de identidades	1º dia útil após a assinatura do Termo de Recebimento Provisório da solução	Até 300 (trezentos) dias contados da data de assinatura do Termo de Recebimento Provisório da entrega da solução
Serviço de suporte técnico e garantia	1º dia após a assinatura do Termo de Recebimento Definitivo da instalação e configuração	60 (sessenta) meses após o Termo de Recebimento Definitivo da instalação e configuração
Treinamento oficial com o fabricante	Em até 5 (cinco) dias úteis após a emissão da O.S.	Conforme definido na O.S.
Serviço de customização	1º dia útil após a emissão da O.S.	Conforme definido na O.S.

3.1.12. A Contratada para a solução de gerenciamento de acessos privilegiados deverá seguir os seguintes prazos:

Descrição	Início da Execução	Finalização da Execução
Entrega da solução de gerenciamento e monitoramento do acesso	1º dia útil após a assinatura do contrato	Até 45 (quarenta e cinco) dias contados da data de assinatura do contrato
Instalação e configuração da solução de gerenciamento e monitoramento do acesso	1º dia útil após a assinatura do Termo de Recebimento Provisório da solução	Até 90 (noventa) dias contados da data de assinatura do Termo de Recebimento Provisório da entrega da solução
Serviço de suporte técnico e garantia	1º dia após a assinatura do Termo de Recebimento Definitivo da instalação e configuração	60 (sessenta) meses após o Termo de Recebimento Definitivo da instalação e configuração
Treinamento oficial com o fabricante	Em até 5 (cinco) dias úteis após a emissão da O.S.	Conforme definido na O.S.
Serviço de customização	1º dia útil após a emissão da O.S.	Conforme definido na O.S.

3.1.13. A Contratada para a solução de correlacionamento de eventos deverá seguir os seguintes prazos:

Descrição	Início da Execução	Finalização da Execução
Entrega da solução de correlacionamento de eventos	1º dia útil após a assinatura do contrato	Até 45 (quarenta e cinco) dias contados da data de assinatura do contrato
Instalação e configuração da solução de correlacionamento de eventos	1º dia útil após a assinatura do Termo de Recebimento Provisório da entrega da solução	Até 60 (sessenta) dias contados da data de assinatura do Termo de Recebimento Provisório da entrega da solução
Serviço de suporte técnico e garantia	1º dia após a assinatura do Termo de Recebimento Definitivo da instalação e configuração	60 (sessenta) meses após o Termo de Recebimento Definitivo da instalação e configuração
Transferência de conhecimento	Em até 5 (cinco) dias úteis após a emissão da O.S.	Conforme definido na O.S.
Serviço de customização	1º dia útil após a emissão da O.S.	Conforme definido na O.S.

3.2. **REQUISITOS DE SEGURANÇA**

3.2.1. Portaria do Cade nº 79/2012 e nº 88/2016 - Política de Segurança da Informação e Comunicações do Cade;

3.2.2. Portaria do Ministério da Justiça 3.530/2013 - Política de Segurança da Informação e Comunicações do Ministério da Justiça;

3.2.3. Instrução Normativa GSI/PR n° 01, de 13 de junho de 2008, e suas normas complementares - Gestão de Segurança da Informação;

3.2.4. Conforme legislação em vigor e termo de compromisso assinado, a Contratada responderá caso ocorra divulgação ou uso de informação sigilosa a que tenha tido acesso em virtude da presente contratação.

3.3. **REQUISITOS AMBIENTAIS, SOCIAIS E CULTURAIS**

3.3.1. Não se aplica.

3.4. **REQUISITOS DE SUSTENTABILIDADE**

3.4.1. Não se aplica.

3.5. **REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO**

3.5.1. A contratante e a contratada deverão elaborar conjuntamente o projeto de implementação da solução.

3.6. **REQUISITOS DA ARQUITETURA TECNOLOGIA**

3.6.1. Os itens da solução devem ser instalados em Hyper-V nas versões do Windows Server 2012 e superiores;

3.6.1.1. Caso não seja compatível, a solução deverá ser entregue com *hardware* e licenças de *software* (ex.: *software* incompatível com os equipamentos de infraestrutura da autarquia, hypervisor diverso ao do item acima, sistema operacional específico, etc) dimensionados de forma que a solução funcione adequadamente e seja compatível com as ferramentas de infraestrutura do Cade;

3.6.1.2. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação.

3.7. **REQUISITOS DE EXPERIÊNCIA PROFISSIONAL E DE FORMAÇÃO DA EQUIPE**

3.7.1. A equipe da CONTRATADA deverá ter experiência e formação adequada para executar o objeto dessa licitação.

4. **CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA**

4.1. As obrigações da Contratada estão estipuladas no item 4.2. do Termo de Referência (nº SEI 0546630).

5. **CLÁUSULA QUINTA - DAS OBRIGAÇÕES DO CONTRATANTE**

5.1. As obrigações da Contratante estão estipuladas no item 4.1. do Termo de Referência (nº SEI 0546630).

6. CLÁUSULA SEXTA - DA FISCALIZAÇÃO E DO ACOMPANHAMENTO

6.1. DO FISCAL TÉCNICO

6.1.1. Participar da reunião inicial;

6.1.2. Receber da Contratada os serviços especificados na Ordem de Serviço;

6.1.3. Analisar junto com o Fiscal Requisitante se as não conformidades são passíveis de correção;

6.1.4. Emitir Termo de Recebimento Provisório;

6.1.5. Realizar, juntamente com o Fiscal Requisitante, a avaliação da qualidade dos serviços realizados, com apoio das Listas de Verificação e de acordo com os Critérios de Aceitação previamente definidos, para verificar a existência de não conformidades;

6.1.6. Apoiar o Fiscal Requisitante na identificação das não conformidades para encaminhamento ao Gestor do Contrato;

6.1.7. Verificar a manutenção das condições definidas no Modelo de Execução do contrato;

6.1.8. Analisar, juntamente com o Fiscal Requisitante, o Termo de Suporte e os cadastros do Cade junto a Central de Suporte da Contratada;

6.1.9. Verificar, com apoio do Fiscal Requisitante, se os requisitos de necessidade, economicidade e oportunidade da contratação continuam sendo satisfeitos;

6.1.10. Encaminhar as demandas de correção à Contratada.

6.1.11. Encaminhar a solicitação da abertura de processo de Apuração de Responsabilidade Contratual ao Gestor do Contrato, caso sejam identificadas irregularidades por parte da Contratada na prestação de serviços.

6.2. DO FISCAL REQUISITANTE

6.2.1. Participar da reunião inicial;

6.2.2. Avaliar a qualidade dos serviços prestados;

6.2.3. Analisar os desvios de qualidade de serviço;

6.2.4. Identificar não conformidades da solução;

6.2.5. Elaborar e assinar o Termo de Recebimento Definitivo;

6.2.6. Verificar, com apoio do Fiscal Técnico, manutenção da necessidade, economicidade e oportunidade da contratação;

6.2.7. Assinar a Ordem de Serviço;

6.2.8. Assinar do Termo de Recebimento Definitivo;

6.2.9. Verificar a manutenção das condições de habilitação definidas na licitação continuam satisfeitas;

6.2.10. Analisar, juntamente com o Fiscal Técnico, o Termo de Suporte e os cadastros do Cade junto a Central de Suporte da Contratada;

6.2.11. Verificar a manutenção das condições definidas no Modelo de Gestão do Contrato.

6.2.12. Encaminhar a solicitação da abertura de processo de Apuração de Responsabilidade Contratual ao Gestor do Contrato, caso sejam identificadas irregularidades por parte da Contratada na prestação de serviços.

6.3. **DO FISCAL ADMINISTRATIVO**

6.3.1. Participar da reunião inicial;

6.3.2. Avaliar a aderência aos termos contratuais;

6.3.3. Indicar termos não aderentes

6.3.4. Verificar a manutenção das condições classificatórias.

6.3.5. Verificar regularidades fiscais, trabalhistas e previdenciárias.

6.3.6. Solicitar da Contratada a emissão das notas fiscais após a emissão do Termo de Recebimento Definitivo.

6.3.7. Encaminhar a solicitação da abertura de processo de Apuração de Responsabilidade Contratual ao Gestor do Contrato, caso sejam identificadas irregularidades fiscais, trabalhistas ou previdenciárias Contratada.

6.3.8. Atestar as Notas Fiscais do Serviço prestado após a emissão do Termo de Recebimento Definitivo e encaminhar a documentação para liquidação/pagamento.

6.4. **DO GESTOR DO CONTRATO**

6.4.1. Convocar reunião inicial e elaborar sua pauta;

6.4.2. Conduzir reunião inicial;

6.4.3. Encaminhar sanções para área administrativa;

6.4.4. Encaminhar pedido de alteração contratual, devidamente justificados indicando as condições que não mais atendem os quesitos de manutenção da necessidade, economicidade e oportunidade da contratação e aquelas que estão em desacordo com as condições definidas no Modelos de Execução e Gestão do contrato para Diretoria Administrativa;

6.4.5. Solicitar a autorização ao Coordenador-Geral de Orçamento Finanças e Logística a abertura de processo de Apuração de Responsabilidade Contratual, caso sejam identificadas irregularidades da Contratada na prestação de serviços.

7. **CLÁUSULA SÉTIMA - DO MODELO DE EXECUÇÃO DO CONTRATO** (conforme art. 19, da IN 04/2014)

7.1. **Prazos e condições**

7.1.1. Após a assinatura do contrato, a empresa contratada deverá instalar as licenças no prazo máximo de 45 (quarenta e cinco) dias corridos;

7.1.2. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

7.1.2.1. As licenças forem entregues e instaladas pela contratada atendendo às especificações contidas neste Contrato;

7.1.2.2. O fornecedor emitir certificado de garantia junto ao fabricante de 60 meses para as licenças entregues;

7.1.2.3. A qualidade do serviço tiver sido avaliada e aceita pela área de TI.

7.1.3. A documentação deverá ser fornecida em sua forma original, preferencialmente em formato eletrônico;

7.1.4. Todas as características exigidas deverão ser comprovadas, independente da descrição da proposta, através de documentos do fornecedor como catálogos, manuais, ficha de especificação técnica, conforme Proposta de Preços da Licitante.

7.2. **Rotinas de execução**

7.2.1. Ordem de Serviço ou Fornecimento de Bens

7.2.2. A emissão da Ordem de Serviço ou Fornecimento de Bens deverá acontecer a qualquer momento através do SEI.

7.3. **Entrega do objeto**

7.3.0.1. A Contratada deverá disponibilizar, pelo meio mais adequado (via download em site oficial, mídia digital, etc.), no prazo de 45 (quarenta e cinco) dias úteis após a assinatura do contrato e/ou a emissão da Ordem de Serviço, considerando o que acontecer primeiro, os softwares contratados de acordo com os quantitativos solicitados.

7.3.0.2. As novas versões das licenças adquiridas, quando aplicável, deverão ser comunicadas ao Cade em até 15 (quinze) dias, a partir do lançamento oficial da nova versão.

7.3.0.3. A Contratada deverá disponibilizar para o Cade o acesso a Central de Licenças, serviço disponibilizado pela Fabricante para acompanhamento e uso das licenças e benefícios do contrato.

7.3.0.4. Na Central de Licença, a Contratada deverá vincular todas as licenças ao usuário do Cade - cgti@cade.gov.br

7.4. **Do Termo de Recebimento Provisório**

7.4.1. O Termo de Recebimento Provisório será emitido em até 5 (cinco) úteis após a entrega das licenças e vinculação do usuário do Cade (cgti@cade.gov.br) na Central de Licenças da Fabricante, para efeito de posterior verificação da conformidade dos materiais ofertados com as especificações constantes do Edital e seus Anexos. Para tal, será emitido Termo de Recebimento Provisório pela Equipe de Fiscalização indicada pela Portaria específica conforme Art. 6º da Portaria Cade nº 212, de 12 de Julho de 2017.

7.4.2. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Contrato e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação à Contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.4.3. O prazo para emissão do Termo de Recebimento não será contado enquanto não for entregue os bens rejeitados no todo e/ou em parte.

7.5. **Do Termo de Recebimento Definitivo**

7.5.1. O Termo de Recebimento Definitivo deverá ser feito em até 15 (quinze) dias úteis após a implantação da solução e respectiva integração na infraestrutura tecnológica do Cade, e depois de ter sido examinado, e considerado em perfeitas condições de uso pela Equipe de Fiscalização do Contrato. Para tal, será emitido Termo de Recebimento Definitivo.

7.5.2. O recebimento provisório ou definitivo não exclui a responsabilidade civil, nem ético-profissional pelo perfeito cumprimento das obrigações assumidas, dentro dos limites estabelecidos pela Lei.

7.5.3. O prazo de garantia inicia a sua contagem a partir da emissão do Termo de Recebimento Definitivo.

7.6. **Quantitativos**

7.6.1. A estimativa levou em conta levantamento do quantitativo de funcionários, computadores em rede, equipamentos de missão crítica, que demonstrou a necessidade de aquisição e consequentemente a atualização do quantitativo de licenças, conforme tabela apresentada no item 1.1.

7.7. **Mecanismo formais de comunicação**

7.7.1. A comunicação entre o Contratante e a Contratada se dará preferencialmente por meio de escrito, sempre que se entender necessário o registro de ocorrência relacionada a execução do objeto, nas formas da tabela abaixo:

7.7.2. Conforme Resolução Cade nº 11/2014, disponível no endereço eletrônico http://www.cade.gov.br/assuntos/normas-e-legislacao/resolucao/despacho-339-resolucao-no-11-de-2014.pdf/view, o Cade utiliza como sistema oficial de gestão de processo eletrônico o Sistema Eletrônico de Informações – SEI. A Contratada deverá se cadastrar no sistema SEI, no endereço eletrônico http://sei.cade.gov.br/sei/institucional/usuarioexterno/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0.

7.7.3. Em caso de dúvidas, poderá entrar em contato com o núcleo gestor do sistema pelo telefone (61) 30311825 ou email sei@cade.gov.br. Desta forma, os instrumentos formais de comunicação entre o Cade e a Contratada serão tramitados por meio do SEI. São eles:

Documento	Função	Emissor	Destinatário	Periodicidade
Ofício	Informações diversas	Contratante/Contratada	Contratante/Contratada	Sempre que necessário
E-mail	Informações diversas	Contratante/Contratada	Contratante/Contratada	Sempre que necessário
Ordem de serviço	Autorização para prestação de serviço	Contratante	Contratada	Sempre que necessário
Termo de recebimento provisório	Recebimento provisório dos serviços	Contratante	Contratada	Sempre que necessário
Termo de recebimento definitivo	Recebimento definitivo dos serviços	Contratante	Contratada	Sempre que necessário
Ata de reunião	Informações diversas	Contratante/Contratada	Contratante/Contratada	Sempre que necessário
Termo de Encerramento do Contrato	Encerramento oficial do contrato	Contratante	Contratada	No final do contrato

A comunicação para o serviço de garantia e assistência técnica será através de um Central de Atendimento via Web e o 0800 fornecida pela CONTRATADA.

7.8. **Condições de manutenção de sigilo**

7.8.1. A CONTRATADA é integralmente responsável pela manutenção de sigilo sobre quaisquer dados, informações e artefatos fornecidos pelo Cade, ou contidos em quaisquer documentos e mídias, de que venha a ter acesso durante a execução contratual, não podendo, sob qualquer pretexto e forma, divulga-los, reproduzi-los ou utilizá-los para fins alheios à exclusiva necessidade dos serviços contratados.

7.8.2. A Contratada firmará, em termo próprio, compromisso de manutenção de sigilo e segurança das informações, Anexo III - Termo de Compromisso. Adicionalmente, cada profissional a serviço da Contratada deverá assinar termo próprio atestando ciência da existência de tal compromisso, Anexo IV - Termo de Ciência.

7.8.3. A Contratada, na execução dos serviços contratados, deverá observar a Política de Segurança da Informação e Comunicação do contratante, os normativos vigentes e as boas práticas relativas à segurança da informação, especialmente as indicadas nos normativos internos da Administração Pública Federal, em todas as atividades executadas.

7.9. **Transferência de conhecimento**

7.9.1. A transferência de conhecimento da solução será realizada através dos itens "Treinamento" e "Operação Assistida" deste Contrato.

7.10. **Propriedade da solução**

7.10.1. A solução adquirida será de propriedade do Cade, ressalvados os direitos de propriedade intelectual e industrial de terceiros.

8. **CLÁUSULA OITAVA- DAS SANÇÕES ADMINISTRATIVAS**

8.1. Pela inexecução total ou parcial do objeto do contrato, o CONTRATANTE poderá, garantida a prévia defesa e o devido processo legal, aplicar as seguintes sanções:

I - Advertência, com base no art. 87, I, da Lei 8.666/93;

II - Multa de:

a) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

b) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima ou de inexecução parcial da obrigação assumida;

c) 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

d) 0,2% a 3,2% por dia sobre o valor do contrato, conforme detalhamento constante das **tabelas 1 e 2** abaixo; e

e) 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião

de prorrogação), observado o máximo de 2% (dois por cento. O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

f) As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

g) A aplicação das multas seguirá o detalhamento das tabelas a seguir

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor do contrato
2	0,4% ao dia sobre o valor do contrato
3	0,8% ao dia sobre o valor do contrato
4	1,6% ao dia sobre o valor do contrato
5	3,2% ao dia sobre o valor do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou conseqüências letais, por ocorrência;	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04
3	Servir-se de funcionário sem qualificação para executar os serviços contratados, por empregado e por dia;	03
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
Para os itens a seguir, deixar de:		
5	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
6	Substituir empregado alocado que não atenda às necessidades do serviço, por funcionário e por dia;	01
7	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência	03

	formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	
8	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	01
9	Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA	01

III - Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos, com base no art. 87, III, da Lei 8.666/93;

IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, com base no art. 87, IV, da Lei 8.666/93;

V - Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos, com base no art. 7º, da Lei 10.520/2002.

8.2. A multa moratória incidirá a partir do 2º (segundo) dia útil da inadimplência.

8.3. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a Contratada pela sua diferença, a qual será descontada dos pagamentos devidos pelo Contratante ou, quando for o caso, cobrada judicialmente.

8.4. As sanções previstas nos incisos I, III, IV e V do item 10.6.12 poderão ser aplicadas juntamente com as do inciso II, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis, contados da notificação.

8.5. A contratada ficará sujeita, ainda, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Falhar na execução do contrato: Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 12 (doze) meses.

b) Fraudar na execução do contrato: Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 30 (trinta) meses.

8.6. As penas previstas nas alíneas "a" a "b" serão agravadas em 50% (cinquenta por cento) de sua pena-base, para cada agravante, até o limite de 60 (sessenta) meses, quando restar comprovado que a contratada tenha sofrido registro de 3 (três) ou mais penalidades no Sistema de Cadastramento Unificado de Fornecedores – SICAF em decorrência da prática de qualquer das condutas tipificadas no presente termo nos 24 (vinte e quatro) meses que antecederam o fato em decorrência do qual será aplicada a penalidade

8.7. Em qualquer hipótese de aplicação de sanções, será assegurado à licitante vencedora e ao contratado o contraditório e a ampla defesa, conforme previsto nos §§ 2° e 3°, do art.86 da Lei n° 8.666/93.

8.8. Decorridos 30 (trinta) dias sem que a contratada tenha iniciado a prestação da obrigação assumida, estará caracterizada a inexecução contratual, ensejando a sua rescisão, conforme determina o art. 77, da Lei 8.666/93.

8.9. As penalidades serão obrigatoriamente registradas no SICAF.

9. CLÁUSULA NONA- DA SUBCONTRATAÇÃO

9.1. Não será admitida a subcontratação do objeto deste contrato.

10. CLÁUSULA DEZ - DA VIGÊNCIA

10.1. O prazo de vigência da contratação é de 12 (doze) meses contados de sua assinatura, prorrogáveis até 48 (quarenta e oito) meses, na forma do art. 57, IV, da Lei 8.666/93.

10.2. O item 10 poderão ter seus contratos prorrogados até limite 48 (quarenta e oito) meses, nos termos da Lei 8.666/93 Art.57, IV;

11. CLÁUSULA ONZE - DOS ACRÉSCIMOS E SUPRESSÕES

11.1. O futuro contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento), calculados sobre o valor inicial atualizado do contrato.

11.2. Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no subitem anterior, salvo as supressões por acordo celebrado entre as partes.

12. CLÁUSULA DOZE - DO VALOR DO CONTRATO

12.1. O valor total estimado do presente Contrato é de **R$ 715.500,00 (setecentos e quinze mil e quinhentos reais)**, discriminado unitariamente na tabela abaixo, correndo a despesas a conta dos recursos consignados ao Contratante, no Orçamento Geral da União, sendo sua totalidade para o exercício de 2018, sob a seguinte classificação: Programa de Trabalho **145923**, Elemento de Despesa 44904006, 44904003, 33904020 e 44904003, devidamente empenhado, conforme Nota de Empenho nº 2018NE800395, 2018NE800397, 2018NE800398, 2018NE800399, datadas de 19/12/2018.

12.2. A despesa do exercício subsequente correrá à conta da Dotação Orçamentária consignada para essa atividade no respectivo exercício.

Grupo	Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
3	9	Solução de correlacionamento de eventos com serviço de garantia pelo período de 60 (sessenta) meses	Eventos por segundo (EPS)	3.000	102,00	306.000,00
	10	Serviço de instalação e configuração para a solução de correlacionamento de eventos	Serviço	1	162.000,00	162.000,00

	11	Treinamento oficial com o fabricante da ferramenta de correlacionamento de eventos	Pessoa	3	11.500,00	34.500,00
	12	Serviço de customização para a solução de correlacionamento de eventos	Unidade de serviço técnico (UST)	1000	213,00	213.000,00

13. **CLÁUSULA TREZE - DO PAGAMENTO**

13.1. O pagamento será efetuado pela Contratante no prazo de 30 (trinta) dias corridos, contados da apresentação da Nota Fiscal/Fatura, contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

13.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

13.3. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 10 (dez) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

13.4. A Nota Fiscal deverá ser digitalizada, em formato **PDF**, e encaminhada por endereço eletrônico a ser repassado pela contratante, para fins de comprovação, liquidação e pagamento.

13.5. O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados, devidamente acompanhada das comprovações mencionadas no §1º do art. 36, da IN/SLTI nº 02, de 2008.

13.6. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

13.7. Será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

I. não produziu os resultados acordados;
II. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;
III. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada,

13.8. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

13.9. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

13.10. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

13.11. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

13.12. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

13.13. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

13.14. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente no SICAF.

13.15. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993.

13.16. A Contratada regularmente optante pelo Simples Nacional, exclusivamente para as atividades de prestação de serviços previstas no §5º-C, do artigo 18, da LC 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, observando-se as exceções nele previstas. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

13.17. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX/100) I = (6/10) I = 0,00016438

336 336

13.18. O Cade não estará sujeito à compensação financeira a que se refere o item anterior, se o atraso decorrer da prestação irregular dos serviços ou com ausência total ou parcial de documentação hábil, ou pendente de cumprimento pela CONTRATADA de quaisquer das cláusulas do contrato.

14. CLÁUSULA CATORZE - DO REAJUSTE CONTRATUAL

14.1. O preço consignado no contrato será corrigido anualmente, observado o interregno mínimo de um ano, contado a partir da data limite para a apresentação da proposta, pela variação do Índice de Custos da Tecnologia da Informação (ICTI), calculado e divulgado pelo Instituto de Pesquisa Econômica Aplicada (Ipea), com base na seguinte fórmula:

R = [(I - Io).P]/Io

Em que:

Para o primeiro reajuste:

R = reajuste procurado;

I = índice relativo ao mês do reajuste;

Io = índice relativo ao mês da data limite para apresentação da proposta;

P = preço atual dos serviços.

Para os reajustes subsequentes:

R = reajuste procurado;

I = índice relativo ao mês do novo reajuste;

Io = índice relativo ao mês do início dos efeitos financeiros do último reajuste efetuado;

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

14.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

15. **CLÁUSULA QUINZE - MODELO DE GESTÃO DO CONTRATO** (Conforme art. 20, da IN 04/2014)

15.1. **CRITÉRIOS DE ACEITAÇÃO, ALTERAÇÃO E CANCELAMENTO DOS SERVIÇOS PRESTADOS**

15.1.1. O objeto licitado deverá ser entregue e instalado pelo próprio fornecedor ou por técnico(s) da empresa fornecedora;

15.1.2. A Solução de Tecnologia da Informação fornecida poderá, a qualquer tempo, ser manuseada por técnicos habilitados do Cade;

15.1.3. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

15.1.3.1. a) A Solução de Tecnologia da Informação for entregue e instalada, atendendo às especificações contidas neste Contrato;

15.1.3.2. b) O fornecedor emitir certificado de garantia junto ao fabricante de 60 (sessenta) meses para as licenças entregues; e

15.1.3.3. c) A qualidade do serviço for avaliada e aceita pela área de tecnologia da informação.

15.1.4. O objeto será recebido provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização para efeito de posterior verificação de sua conformidade com as especificações constantes neste Contrato, no prazo de até 05 (cinco) dias úteis;

15.1.5. Após 15 (quinze) dias corridos da emissão do Termo de Recebimento Provisório, conforme documento SEI 0513359, sendo confirmada sua operação e desempenho a contento, nos termos deste Contrato, a contratante emitirá o Termo de Recebimento Definitivo, conforme documento SEI 0513361;

15.1.6. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Contrato, devendo ser substituído no prazo de até 15 (quinze) dias úteis, à custa da contratada, sob pena de aplicação das penalidades previstas neste Contrato; e

15.1.7. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do fornecimento, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos em Lei.

15.2. **ALTERAÇÃO SUBJETIVA**

15.2.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

15.3. **NÍVEIS DE SERVIÇOS**

DA INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

15.3.1. A contratante disponibilizará o espaço adequado no CPD e refrigeração suficiente para comportar os equipamentos novos a serem adquiridos e os já existentes, assim como, a infra-estrutura elétrica até o quadro de energia com capacidades (corrente e tensão) suficientes de suportar todos os equipamentos novos e os já existentes, durante todo o período de instalação e/ou migração. A contratante se responsabilizará por manter o ambiente que sofrerá intervenção com a última cópia de segurança completa (backup full), realizada e válida.

15.3.2. A contratada deverá instalar a solução ofertada nas instalações do contratante;

15.3.3. A solução deverá ser configurada de acordo com as melhores práticas do fabricante e configurações específicas já utilizadas na solução

atual do Cade;

DAS CONDIÇÕES DE SUPORTE DA SOLUÇÃO

15.3.4. A contratada deverá fornecer suporte direto do fabricante da solução por um período mínimo de 60 (sessenta) meses contados da emissão do Termo de Recebimento Definitivo para garantia de atualizações de versão, suporte técnico e acionamento em nível de resolução de problemas pelo próprio fabricante, e apoiar o Cade na resolução de demandas junto ao fabricante;

15.3.5. A contratada deverá apoiar o Cade em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura;

15.3.6. A contratada deverá realizar visitas proativas quinzenais para verificação do correto funcionamento e eventuais dúvidas do Cade durante os primeiros 6 meses e mensais para os 6 meses seguintes, a contar da emissão do Termo de Recebimento Definitivo do serviço de instalação e configuração para cada produto;

15.3.7. Prestar a transferência de conhecimento no formato *hands-on* para a equipe técnica da instituição durante a implantação da solução, ao longo das atividades de configuração, bem como durante atividades de suporte e customização;

15.3.8. A contratada deverá auxiliar o Cade na configuração das ferramentas que compõem a solução, a fim de garantir o uso eficiente delas;

15.3.9. A contratada deverá obedecer critérios de nível de serviço contidos na tabela do item abaixo;

15.3.10. O suporte técnico deverá ser prestado para a solução e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento *on-site*, se requerido pelo contratante, conforme os índices de criticidade a seguir:

<table>
<tr><th>Criticidade</th><th>Descrição</th><th>Prazo Máximo de Atendimento</th><th>Prazo Máximo de Restauração de Serviço</th></tr>
<tr><td rowspan="3">Severidade 1 (Alta)</td><td rowspan="3">Sistema parado ou produto inoperante com impacto na operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.</td><td>Em até 2 horas deve ter um técnico do fornecedor on-site.</td><td rowspan="2">Em até 8 horas</td></tr>
<tr><td rowspan="2">Em até 15 min. um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.</td></tr>
<tr><td>Entrega da Solução pelo fabricante em até 6 dias.</td></tr>
</table>

Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor *on-site.* Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas Entrega da Solução pelo fabricante em até 10 dias.
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 8 horas deve ter um técnico do fornecedor *on-site* ou atendimento remoto. Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Em até 24 horas Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato. No mesmo dia ou no próximo dia útil comercial	Em até 72 horas Entrega da Solução pelo fabricante em até 20 dias ou considerado para as próximas atualizações da ferramenta

15.3.11. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;

15.3.12. Deverá ser fornecido um serviço a nível mundial de monitoramento proativo para ameaças de segurança que encaminhe notificações técnicas via email;

15.3.13. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os métodos: telefone 0800, email, *site* do fabricante;

15.3.14. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, email, *site* da contratada ou do fabricante;

15.3.15. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;

15.3.16. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;

15.3.17. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado;

15.3.18. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

15.3.19. Os serviços de atendimento de garantia para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);

15.3.19.1. Os chamados de garantia de severidades 1 e 2 deverão contar com suporte *in loco* da contratada para prover celeridade no reestabelecimento do serviço;

15.3.20. O fornecedor emitirá relatório sempre que solicitado pelo contratante, em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período, incluindo:

15.3.20.1. Quantidade de ocorrências (chamados) registradas no período;

15.3.20.2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;

15.3.20.3. Data e hora de abertura;

15.3.20.4. Data e hora de inicio e conclusão do atendimento;

15.3.20.5. Identificação do técnico do contratante que registrou o chamado;

15.3.20.6. Identificação do técnico do contratante que atendeu o chamado da garantia;

15.3.20.7. Descrição do problema;

15.3.20.8. Descrição da solução;

15.3.20.9. Informações sobre eventuais escalações;

15.3.20.10. Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido;

15.3.20.11. Total de chamados no mês e o total acumulado até a apresentação do relatório.

15.3.21. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante;

15.3.22. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e *patches* de correção, desde que comprovados pelo fabricante da solução;

15.3.23. Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante;

15.3.24. Esta solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um *patch/fix*;

15.3.25. Durante o período de garantia, o licitante compromete-se a substituir, em até 15 (quinze) dias úteis, os equipamentos que apresentarem, em um período de 60 (sessenta dias), duas ocorrências de defeitos por inoperância do produto ou 3 (três) ocorrências de deficiência operacional do produto;

15.3.26. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da contratada;

15.3.27. Nos casos em que as manutenções necessitarem de paradas da solução, o contratante deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo contratante, para execução das atividades de manutenção;

15.3.28. A contratada deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do ambiente tecnológico do Cade, caso requeiram;

15.3.29. O relatório deve ser assinado por representante do contratante, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;

15.3.30. Por questão de segurança, o servidor nunca deverá ser removido da dependência do contratante com os discos rígidos. Nesse caso, o disco rígido do equipamento deverá ser removido e entregue à equipe da Coordenação-Geral de Tecnologia da Informação - CGTI - do Cade para destruição e descarte seguro da mídia;

15.3.31. Durante o período de garantia o fornecedor executará, sem ônus adicionais, correções de falhas (*bugs*) de *hardware* e *software*;

15.3.32. Durante o período de vigência da garantia o contratante terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos *softwares* e *firmwares* que fazem parte da solução ofertada.

DAS CONDIÇÕES DE MANUTENÇÃO DA SOLUÇÃO

15.3.33. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

15.3.34. As manutenções preventivas e corretivas serão de responsabilidade do fornecedor, sem custos adicionais ao contratante;

15.3.35. Durante o período de garantia, qualquer componente que apresente defeito ou mau funcionamento, sem indicação de solução, deve ser substituído imediatamente;

DAS CONDIÇÕES DE GARANTIA DA SOLUÇÃO

15.3.36. O fornecedor garante por, no mínimo, 60 (sessenta) meses o fornecimento dos componentes de *software*, para manutenções, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas;

15.3.37. Durante o período de garantia, deve ser efetuada manutenção preventiva, em intervalos predeterminados e de acordo com critérios prescritos pelo contratante, destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução, para tanto, a contratada deve auxiliar, sempre que solicitado;

15.3.38. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

15.3.39. As manutenções preventivas e corretivas serão de responsabilidade do fabricante, sem custos adicionais ao contratante;

15.3.40. Durante o período de garantia, qualquer componente que apresente defeito ou mau funcionamento, sem indicação de solução, deve ser substituído imediatamente.

15.4. **Canais de Atendimento:**

15.4.1. O suporte técnico do fabricante deverá ser prestado para a solução adquirida e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento *on-site* ou remoto, se requerido pelo contratante, conforme os índices de criticidade do item 9.2.10;

15.4.2. O atendimento pelo fabricante deve estar disponível para os produtos de segurança, disponibilidade e pela combinação de ambos;

15.4.3. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto no item anterior, deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;

15.4.4. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;

15.4.5. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;

15.4.6. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado;

15.4.7. Será disponibilizado canal de atendimento e chamado técnico do fabricante para 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800;

15.4.8. disponibilizado, os chamados técnicos poderão ser abertos via e-mail, *site* da contratada ou do fabricante, telefone, etc;

15.4.9. O fornecedor deve informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos dos equipamentos, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo contratante para o acesso.

15.5. **Procedimento para retenção ou glosa do pagamento**

15.5.1. A retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, só deverá ocorrer quando a Contratada:

15.5.2. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

15.5.3. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

16. CLÁUSULA DEZESSEIS - DA PROPRIEDADE, SIGILO E RESTRIÇÕES

16.1. A Contratada deverá garantir a segurança das informações do Cade e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido deste Conselho no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal;

16.2. Toda a documentação gerada durante a vigência do contrato deve ser repassada ao Cade com todos os direitos de propriedade;

16.3. Todos os produtos fornecidos como resultado da execução do projeto serão de propriedade do Cade, aplicando-se as restrições relativas aos direitos de propriedade intelectual e direitos autorais da solução de tecnologia da informação, conforme regula a lei nº 9.610/98;

16.4. A Contratada deverá submeter-se à Política de Segurança da Informação e Comunicações do Cade e abster-se de veicular publicidade ou qualquer outra informação acerca das atividades desempenhadas, sem prévia autorização do Cade; execução dos serviços deverão assinar o Termo de Compromisso e Manutenção de Sigilo, comprometendo-se a preservar as informações a que tiverem acesso em virtude dos serviços prestados.

16.5. Após a assinatura do contrato, os profissionais responsáveis pela execução dos serviços deverão assinar o Termo de Compromisso e Manutenção de Sigilo, comprometendo-se a preservar as informações a que tiverem acesso em virtude dos serviços prestados.

17. CLÁUSULA DEZESSETE - DO REGIME DE EXECUÇÃO

17.1. **Regime de execução do contrato**

17.1.1. O regime de execução da contratação será empreitada por preço global, para os itens 1, 2, 5, 6, 9 e 10 e de empreitada por preço unitário, para os itens 3, 4, 7, 8, 11 e 12.

17.2. **Requisitos de qualificação das equipes técnicas**

17.2.1. Os profissionais que prestarão serviços suporte dos bens adquiridos através da presente contratação deverão ter conhecimentos técnicos da solução.

17.3. **Da Subcontratação**

17.3.1. Não haverá subcontratação, salvo para eventual manutenção de *hardware* que venha a compor a solução, conforme item 3.14 do Termo de Referência.

17.4. **Níveis mínimos de serviço**

17.4.1. Durante a execução do contrato a CONTRATADA deve observar os seguintes níveis mínimos de serviços.

Severidade	Descrição	Prazo para solução do problema
1	Solução fora de operação ou com alguma funcionalidade comprometida	8 horas a partir da abertura do chamado, mediante a solução do defeito ou envio e instalação de um equipamento com as mesmas características e configurações do defeituoso.
2	Solução com falha grave, mas ainda operacional	2 dias úteis a partir da abertura do chamado, mediante a solução do defeito ou envio e instalação de um equipamento com as mesmas características e configurações do defeituoso.
3	Solicitações diversas (configurações, atualizações de software não críticas, Esclarecimentos de dúvidas, implementações de novas funcionalidades).	4 dias úteis a partir da abertura do chamado, mediante a solução do defeito ou envio e instalação de um equipamento com as mesmas características e configurações do defeituoso.

17.5. **DOS REQUISITOS DE QUALIFICAÇÃO DAS EQUIPES TÉCNICAS**

17.5.1. Os profissionais que prestarão serviços objeto da presente contratação deverão ter conhecimentos técnicos avançados da solução e serem certificados pelo fabricante;

18. **CLÁUSULA DEZOITO – DA RESCISÃO**

18.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no neste Contrato.

18.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

18.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

18.4. O termo de rescisão, sempre que possível, deverá indicar:

18.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos em relação ao cronograma físico-financeiro, atualizado;

18.4.2. Relação dos pagamentos já efetuados e ainda devidos;

18.4.3. Indenizações e multas.

19. CLÁUSULA DEZENOVE - DOS CASOS OMISSOS

19.1. Os casos omissos ou situações não explicitadas nas cláusulas deste Contrato regular-se-ão pela Lei nº 8.666/1993 e pelos preceitos de direito público, aplicando-se-lhes, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, na forma dos arts. 54 e 55, inciso XII, da Lei n. 8.666, de 21 de junho de 1993 e alterações posteriores.

20. CLÁUSULA VINTE - DA PUBLICAÇÃO

20.1. Caberá ao Contratante providenciar a publicação do presente Contrato, por extrato, no Diário Oficial da União, no prazo de 20 (vinte) dias a contar do quinto dia útil do mês seguinte à data da assinatura, com indicação da modalidade de licitação e de seu número de referência, conforme dispõe a legislação vigente, Lei nº 10.520, de 17 de julho de 2002 e Lei nº 8.666, de 17 de junho de 1993 e alterações posteriores.

21. CLÁUSULA VINTE E UM - DO FORO

21.1. As partes elegem, de comum acordo, com renúncia a qualquer outro, por mais privilegiado que seja, o Foro da Justiça Federal da Seção Judiciária do Distrito Federal para dirimir as questões decorrentes do presente Contrato.

E, por assim estarem justas e acertadas, foi lavrado o presente **CONTRATO** e disponibilizado por meio eletrônico através do Sistema Eletrônico de Informações – SEI, conforme Resolução Cade n° 11, de 24 de novembro de 2014, publicada no D.O.U. Seção 1, no dia 02 de dezembro de 2014, o qual, depois de lido e achado conforme, vai assinado pelas partes, perante duas testemunhas a tudo presente.

Documento assinado eletronicamente por **Hélio Ferreira da Silva Junior**, **Usuário Externo**, em 21/12/2018, às 19:23, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Luana Nunes Santana**, **Ordenador de Despesas por Subdelegação**, em 24/12/2018, às 10:33, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Isaque Moura da Silva**, **Testemunha**, em 24/12/2018, às 10:42, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Luciana Chaves Simões de Oliveira**, **Testemunha**, em 24/12/2018, às 10:43, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0562119** e o código CRC **88373727**.

Referência: Processo nº 08700.003102/2018-39 SEI nº 0562119