POUPEX ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO

COTAÇÃO DE PREÇO

Brasília/DF, 10 de janeiro de 2023.

Senhor Fornecedor,

Solicitamos a gentileza de nos apresentar proposta de preço para a aquisição(ões) do(s) material(is) e/ou serviço(s) especificado(s) abaixo, **até o dia 31/1/2023.**

ITEM	ESPECIFICAÇÃO	UN	QTD
1.	Contratação de solução de proteção da camada de DNS (*Domain Name System* - Sistema de Nomes de Domínio) na modalidade software como serviço (SaaS) para os usuários da Instituição, com objetivo de bloquear domínios maliciosos e indesejados, endereços IP (*Internet Protocol* - endereço exclusivo que identifica um dispositivo na internet ou em uma rede local) e aplicativos em nuvem. **As exigências, normas e procedimentos relativos à elaboração da proposta, até a assinatura do contrato padrão da POUPEX, constam neste documento.**	-	-

I) QUESTINAMENTOS

O prazo para recebimento de questionamentos é de até 3 dias úteis antes da data de recebimento da proposta comercial e da documentação.

II) NORMAS ESPECÍFICAS

1. Incluso no valor dos materiais/serviços todos os custos diretos e indiretos para perfeita execução dos trabalhos, inclusive as despesas com materiais, mão de obra, transportes, custos financeiros, encargos e impostos necessários.
2. A proposta poderá ser por e-mail para: gecoc.eqcbe@poupex.com.br.
3. A Entrega/execução deverá ser feita no end.: **Avenida Duque de Caxias S/N, Parte "A", Setor Militar Urbano. CEP: 70630-902. Brasília-DF.**
4. **A CONTRATADA, em conformidade com a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 2018, está ciente que a POUPEX coletará dados pessoais dos titulares responsáveis pela empresa, no momento da contratação, e que os dados coletados serão objeto de tratamento e estarão sujeitos à publicidade.**

III) DADOS PARA ENVIO DA PROPOSTA

Associação de Poupança e Empréstimo – POUPEX.

CNPJ: 00.655.522/0001-21.

End.: Avenida Duque de Caxias s/n°, Parte "A", Setor Militar Urbano. CEP: 70630-902. Brasília-DF.

Divisão de Licitações e Compras – Equipe de Compras de Bens – DILCO/EQCBE. FONE: (61) 3314-7780.

1 – OBJETO DA CONTRATAÇÃO

Contratação de solução de proteção da camada de DNS (*Domain Name System* - Sistema de Nomes de Domínio) na modalidade software como serviço (SaaS) para os usuários da Instituição, com objetivo de bloquear domínios maliciosos e indesejados, endereços IP (*Internet Protocol* - endereço exclusivo que identifica um dispositivo na internet ou em uma rede local) e aplicativos em nuvem.

2 – JUSTIFICAVA DA CONTRATAÇÃO

Os riscos presentes no ambiente cibernético têm se multiplicado e os agentes maliciosos têm se valido de diversas estratégias para enganar os usuários. Um dos métodos comuns é a utilização de mensagem de e-mail ou ligação por telefone, em que o *hacker* (especialista em computação que utiliza o alto conhecimento para cometer crimes virtuais) faz uso de informações que parecem legítimas, com o objetivo de fazer com que a vítima clique em um link, quando se trata de mensagem de e-mail, ou digite determinado endereço no navegador de internet e o acesse.

Nesse tipo de situação a vítima é alvo de um ataque de engenharia social, podendo ser levada a acessar um sítio falso ou malicioso na internet, por exemplo, pelo fato de o endereço apresentado ser parecido com o original ou possuir palavras que remetem ao endereço oficial.

São diversos os resultados negativos para a situação apresentada, como por exemplo: violação de dados, proliferação de *ransomware* (tipo de programa de computador que criptografa arquivos e até sistemas inteiros e, em seguida, exige pagamento de resgate para devolver o acesso) capaz de indisponibilizar serviços tecnológicos e até mesmo causar danos na imagem da Instituição.

No que se refere aos endereçamentos na internet, há um importante serviço que é utilizado para a realização de tradução de nomes em endereços IP ou vice-versa, que é o DNS.

Hackers e invasores experientes exploram vulnerabilidades na estrutura do DNS para desligar sistemas, injetar *malware* (tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas) e realizar outras explorações. Esses métodos continuam avançando e afetam os sistemas móveis, bem como os navegadores convencionais.

Os ataques de DNS ocorrem de diversas maneiras, porém um método bastante comum é o envio de *links* configurados como ataque de *phishing* (técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais) ou *spear-phishing* (golpe proveniente de e-mail ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específico). Esse método baseia-se em um nome com erros ortográficos ou outro engano visual para direcionar um usuário a um endereço na internet que insere *malware* em um computador.

Os ladrões cibernéticos também burlam registradores de DNS com o objetivo de alterar os registros e redirecionar o tráfego para um endereço IP que eles controlam.

Independentemente da abordagem específica em ataques de DNS, é necessário que se aplique medidas de segurança para proteger os ativos corporativos, sendo fundamental fazer uso de uma solução de segurança cibernética de DNS que resolva infratores conhecidos e os coloque em uma lista negra. Essa é uma maneira altamente eficaz de bloquear ataques de *phishing* e *spear-phishing*.

3 – DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Serviços		
Nº	**Serviços**	**Quantidade**
1	Subscrição de licenciamento de solução de proteção da camada de DNS na modalidade *software* como serviço (SaaS), pelo período de 12 (doze) meses.	2.000 usuários
2	Serviço de suporte técnico da solução por 12 (doze) meses	
3	Serviço de implantação da solução	1 unidade
4	Repasse de conhecimento	
5	Operação assistida	

4 – ESPECIFICAÇÂO TÉCNICA DA SOLUÇÃO

A. ESPECIFICAÇÃO TÉCNICA

1) A especificação dos itens entregáveis e requisitos obrigatórios e desejáveis a ser considerada pela CONTRATADA, consta no Anexo I desta Especificação Técnica.

B. SUPORTE TÉCNICO DA CONTRATADA

1) O serviço de suporte técnico da CONTRATADA será remoto e observará os seguintes requisitos:
   a. Operar no formato 24 x 7 x 365, com chamados ilimitados e atendimento diretamente pelo fabricante da solução, através de contato por canal único para centralização dos chamados e controles de ANS (Acordo de Nível de Serviço) conforme estabelecido no item “8 - MODELO DE GESTÃO DO CONTRATO”;
   b. Atuar na resolução de incidentes e apoio operacional por meio de acesso telefônico, e-mail, portal web, videoconferência, software de mensagens instantâneas e acesso remoto seguro; e
   c. Manter atualizada a solução de proteção da camada de DNS em sua última versão estável.

C. SERVIÇO DE PLANEJAMENTO, CONFIGURAÇÃO, REPASSE DE CONHECIMENTO E OPERAÇÃO ASSISTIDA

1) Os serviços de **planejamento**, **configuração**, **repasse de conhecimento** e **operação assistida** deverão ser prestados na modalidade remota.
2) Em relação aos serviços de **planejamento** e **configuração** da solução, a CONTRATADA deverá:
   a. elaborar, em conjunto com a equipe técnica da CONTRATANTE, os documentos de planejamento e o desenho detalhado do projeto e sua implementação;
   b. realizar a implementação da solução, considerando as melhores práticas recomendadas pelo fabricante, observando o cenário da CONTRATANTE, por meio do trabalho integrado entre os profissionais da CONTRATANTE e os especialistas da CONTRATADA;

c. detalhar, em conjunto com a CONTRATANTE, o uso pretendido dos serviços, as características de uso das aplicações, dos dados, sistemas, requisitos de alta disponibilidade e desempenho;

d. definir a forma de configuração do ambiente, baseado nas expectativas da CONTRATANTE e premissas do projeto;

e. realizar o planejamento inicial de implementação, voltado para o oferecimento do melhor desempenho dos serviços, por meio do uso dos recursos disponíveis;

f. contemplar o plano de implementação do projeto com as configurações necessárias para instalação e parametrização dos serviços e soluções; e

g. em relação à avaliação do ambiente atual da CONTRATANTE, deverá indicar os ajustes e lacunas que devem ser endereçados para que a implementação seja bem-sucedida.

3) Em relação ao serviço de **repasse de conhecimento**, a CONTRATADA deverá:

a. realizar o repasse de conhecimento com duração mínima de 4 horas para até 5 empregados da CONTRATANTE;

b. utilizar o modelo de demonstração da solução (*hands on*) para repasse de conhecimento para a equipe técnica da CONTRATANTE, demonstrando as principais funcionalidades e a operação do produto;

c. utilizar fabricante ou técnico certificado pelo fabricante para repasse de conhecimento;

d. considerar o ambiente da CONTRATANTE;

e. considerar a definição da CONTRATAÇÃO de repasse de conhecimento *on-line* (ao vivo) e gravado; e

f. durante o repasse deverá permitir a interação entre as equipes técnicas de CONTRATANTE e CONTRATADA de forma *on-line* (ao vivo) para esclarecimento de dúvidas.

5 – DEVERES E RESPONSABILIDADES DA CONTRATANTE

Nº	Descrição
1	Fornecer infraestrutura e informações necessárias para implantação da solução e equipe técnica para acompanhamento das atividades, devendo garantir o sigilo das informações.
2	Receber a implantação da solução fornecida pela CONTRATADA, desde que em conformidade com a proposta aceita, emitindo termo de recebimento de serviços.
3	Disponibilizar à CONTRATADA as informações necessárias para realização das atividades de implementação e parametrização necessária para prestação do serviço.
4	Permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, caso necessário, o acesso remoto da CONTRATANTE, respeitadas as normas de segurança vigentes.
5	Cumprir todas as normas e condições do instrumento contratual.
6	Prover as informações necessárias para que a CONTRATADA possa dar andamento às suas

	atividades, devendo observar o sigilo das informações.
7	Efetuar os pagamentos devidos à CONTRATADA, na forma convencionada, dentro do prazo previsto, desde que atendidas as formalidades necessárias para confirmação da utilização dos serviços faturados.
8	Aplicar as penalidades previstas para o caso de não cumprimento de cláusulas contratuais ou aceitar as justificativas apresentadas pela CONTRATADA.
9	Informar os serviços que serão consumidos junto a CONTRATADA.
10	A CONTRATANTE também acionará a CONTRATADA através de e-mails ou ligações telefônicas.
11	É responsabilidade da CONTRATADA garantir que não seja concedido acesso indevido às contas da CONTRATANTE, nem que seja feito acesso indevido pela CONTRATADA.

6 – DEVERES E RESPONSABILIDADES DA CONTRATADA

Nº	**Descrição**
1	Prover os serviços em obediência aos requisitos estabelecidos nos itens 3 - DESCRIÇÃO DA SOLUÇÃO e 4 - ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO, além da observância às recomendações aceitas nos modelos de boas práticas, normas e legislação.
2	Comunicar à CONTRATANTE, por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, fornecendo à CONTRATANTE todas as informações/dúvidas técnicas pertinentes ao serviço contratado, no prazo de 5 (cinco) dias úteis.
3	Prover sistema de gerenciamento de chamados, mantendo registro da classificação, criticidade, descrição detalhada da situação reportada, prazo de solução, dentre outras informações pertinentes acerca dos chamados abertos pela CONTRATANTE.
4	Ser acionada, prioritariamente, através do sistema de gerenciamento de chamados mencionado no item 6, além de *e-mail* ou ligações telefônicas, para prestação de serviços de suporte técnico.
5	Registrar os chamados provenientes de acionamentos por e-mails ou ligações telefônicas no sistema de gerenciamento de chamados, e enviá-lo à CONTRATANTE para controle e acompanhamento.
6	Considerar um chamado completamente concluído somente quando for aceito e aprovado pela CONTRATANTE responsável pela sua abertura.
7	Disponibilizar mensalmente relatórios, sobre atendimentos e chamados e os detalhamentos dos serviços consumidos.
8	Executar fora do horário comercial, mediante agendamento e autorização prévia da CONTRATANTE, os atendimentos que exigirem manutenção que importe riscos ao sistema ou aos processos de negócio relacionados.
9	Não realizar instalação de *software*, alteração de configuração ou correção de erros dos ambientes computacionais preexistentes, assim como de qualquer outra infraestrutura da

	CONTRATANTE. Todavia, a CONTRATADA deverá auxiliar a equipe técnica da CONTRATANTE, da melhor forma possível, para que esta possa implementar o plano de ação a fim de que o objetivo de implantação da solução seja atendido com sucesso.
10	Indicar representante junto à CONTRATANTE, que deverá responder pela fiel execução do instrumento contratual.
11	Atender prontamente quaisquer orientações e exigências do fiscal técnico da CONTRATANTE, inerentes à execução do objeto contratual.
12	Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE.
13	Propiciar todos os meios e facilidades necessárias à fiscalização do instrumento contratual pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária.
14	Administrar todo e qualquer assunto relativo aos seus profissionais.
15	Manter a confidencialidade dos dados, informações e documentos aos quais venha a ter acesso em decorrência da prestação dos serviços contratados, sendo esta obrigação extensiva a seus sócios, diretores, mandatários, assim como todos os empregados envolvidos na contratação.
16	Disponibilizar à CONTRATANTE acesso aos relatórios ou *dashboards* de monitoramento do ambiente utilizado, visando melhorar a gestão de recursos.
17	Informar de imediato à CONTRATANTE, quaisquer vulnerabilidades ou registros de incidente de segurança cibernética relacionados aos serviços prestados.
18	Excluir os dados armazenados na solução / nuvem ao término do instrumento contratual, em até 10 dias corridos.

7 – MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Prazos	**Assinatura do instrumento contratual** – Em até 5 (cinco) dias úteis após a convocação da empresa vencedora.
	Planejamento da implantação – Em até 5 (cinco) dias úteis após assinatura do instrumento contratual.
	Entrega das licenças – Em até 5 (cinco) dias úteis a partir da entrega do planejamento da implantação.
	Implantação da solução – Em até 10 (dez) dias úteis a partir da entrega das licenças.
	Repasse de conhecimento – Em até 5 (cinco) dias úteis a partir da implantação da solução.

	Serviço de suporte técnico – A partir do recebimento definitivo das licenças e observando o período de vigência do instrumento contratual.
	Operação assistida – Em até 5 (cinco) dias úteis a partir da finalização do repasse de conhecimento.
	Vigência das licenças– Por 12 (doze) meses, podendo ser prorrogado por igual(is) e sucessivo(s) período(s), mediante assinatura de Termo(s) Aditivo(s), até o limite de 60 (sessenta) meses, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea: 1. os serviços tenham sido prestados regularmente; 2. a CONTRATANTE ainda tenha interesse na realização do serviço; 3. o valor do instrumento contratual permaneça economicamente vantajoso para a CONTRATANTE; e 4. a CONTRATADA concorde com a prorrogação do instrumento contratual.
Horários	• A disponibilização da solução e os serviços de suporte técnico deverão ser prestados no formato 24 x 7 x 365. • Os serviços de planejamento, configuração, repasse de conhecimento e operação assistida deverão ser prestados no horário comercial (8h às 18h).
Locais de Entrega	Digital

Mecanismos Formais de Comunicação entre a Contratada e a Administração

A comunicação formal deverá ser realizada, através de sistema de gerenciamento de chamados, entre preposto da CONTRATADA e Gestor/Fiscal da CONTRATANTE ou por sistema de correio eletrônico.

Forma de Pagamento em Função dos Resultados

O pagamento do planejamento da implantação da solução, repasse de conhecimento, serviço de suporte técnico e operação assistida será efetuado pela CONTRATANTE, via transferência bancária, mediante entrega da Nota Fiscal/fatura, após término da prestação dos serviços, em até o 10º (décimo) dia útil, mediante atesto na Nota Fiscal/Fatura a ser apresentada com 10 (dez) dias do vencimento.

O pagamento das licenças será efetuado **mensalmente** pela CONTRATANTE, via transferência bancária, mediante atesto na Nota Fiscal/fatura, até o 10º (décimo) dia do mês subsequente ao da prestação do serviço, mediante atesto na Nota Fiscal/Fatura a ser apresentada com 10 (dez) dias do vencimento.

A CONTRATADA deverá observar este prazo ao preencher o vencimento da Nota Fiscal e enviá-la para o e-mail pagamento.gecoc@poupex.com.br

A nota fiscal juntamente com o arquivo XML somente serão recebidos no e-mail corporativo pagamento.gecoc@poupex.com.br, até o dia 20 do mês de sua emissão, para que as retenções sejam processadas pela CONTRATANTE até o último dia útil do mesmo mês. Caso não seja possível à CONTRATADA encaminhar as referidas Notas Fiscais nesse prazo, essas deverão ser emitidas com data do 1º (primeiro) dia do mês subsequente.

8 – MODELO DE GESTÃO DO CONTRATO

Acompanhamento e fiscalização (incluindo a indicação de gestor e fiscais)

- A aferição de qualidade do serviço será realizada através da apuração dos indicadores de desempenho definidos pelos critérios de aceitação;
- No momento da assinatura do instrumento contratual, a CONTRATADA indicará um representante que será responsável por acompanhar a execução do instrumento contratual e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual;
- A existência e a atuação da fiscalização pela CONTRATANTE em nada restringem a responsabilidade, única, integral e exclusiva da CONTRATADA, no que concerne à execução do instrumento contratual;
- A equipe de fiscalização da contratação, por parte da CONTRATANTE será composta pelos seguintes integrantes constantes no quadro abaixo:

Função	Nome
Gestor do Contrato	Ricardo Fernandes da Silva Neiva
Fiscal Técnico	Charles Lúcio Barbosa de Oliveira

- Os deveres da equipe da fiscalização da CONTRATANTE serão os listados abaixo:
  - Posicionar e repassar as ocorrências aos níveis hierárquicos competentes;
  - Promover a fiscalização do instrumento contratual, sob os aspectos quantitativos e qualitativos;
  - Registrar as falhas detectadas e exigir as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do instrumento contratual;
  - Conferir os serviços entregues e atestar os documentos fiscais pertinentes, podendo suspender qualquer procedimento que não esteja em acordo com os termos contratuais;
  - Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados, identificando, adotando todas as providências necessárias e tratando os desvios; e
  - Notificar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para a CONTRATANTE.

Acordo de níveis de serviço - ANS

Os chamados de suporte técnico referentes à solução de proteção da camada de DNS deverão ter início de atendimento conforme tabela abaixo:

SEVERIDADE	PRIORIDADE	INÍCIO DO ATENDIMENTO
1	Urgente	4 horas
2	Alta	12 horas
3	Média	1 dia
4	Baixa	3 dias

A severidade dos chamados varia de 1 a 4 é descrita da seguinte forma:

Severidade	Descrição	
Urgente (1)	Interrupção de serviço crítico	Um serviço crítico em ambiente de produção está indisponível e nenhuma solução de contingência está disponível;
		Um serviço crítico em ambiente de produção está parado ou não responde e não está sendo possível estabilizá-lo ou reiniciá-lo; e
		Mais de 30% (trinta por cento) dos serviços suportados pela solução são afetados.
Alta (2)	Funcionalidades principais	Uma ou mais funcionalidades estão severamente prejudicadas;
		O uso da solução pode continuar de forma restrita, apesar da produtividade em longo prazo poder ser afetada;
		Possíveis problemas críticos antes de uma atualização; e
		Existe uma solução de contorno temporária para o problema.
Normal (3)	Funcionalidades menores	Uma ou mais funcionalidades não críticas não estão funcionando, existindo solução de contorno disponível;
		Funcionamento de alguns componentes prejudicados, porém permitindo que os serviços sendo prestados; e
		Possíveis problemas não críticos antes de uma atualização.
Baixa (4)	Perguntas gerais de utilização	Questões referentes à aparência da solução, incluindo erros na documentação.

A CONTRATANTE avaliará os serviços prestados pela CONTRATADA por meio da utilização de indicadores de desempenho, que são critérios objetivos e mensuráveis estabelecidos entre CONTRATANTE e CONTRATADA, no intuito de aferir aspectos de qualidade relacionados aos serviços realizados.

Prazo de Início de Atendimento: Corresponde ao prazo, em horas corridas, que a CONTRATADA possui para iniciar o atendimento das demandas solicitadas pela CONTRATANTE, seja através de *e-mails*, ligações telefônicas e/ou, prioritariamente, através de sistema de gerenciamento de chamados provido pela CONTRATADA, até a entrega à CONTRATANTE.

Por Chamado entende-se qualquer incidente, requisição, problema ou mudança relacionados aos serviços prestados pela CONTRATADA.

Para medir o desempenho da CONTRATADA quanto ao início de atendimento dos chamados, foi definido o indicador de início de atendimento mínimo de 95%, a ser aferido mensalmente, conforme formula a seguir:

$$\text{Indicador de Início de Atendimento (\%)} = \frac{CIP}{CA} * 100$$

Em que:

- CIP é a quantidade de chamados com suporte técnico iniciado no prazo definido na tabela de ANS.
- CA é a quantidade de chamados abertos no mês.

Para medir o desempenho da CONTRATADA quanto à disponibilidade da solução, foi definido o indicador de disponibilidade mínimo de 98%, a ser aferido mensalmente, conforme formula a seguir:

$$\text{Indicador de Disponibilidade (\%)} = \frac{DT + IJ}{DP} * 100$$

Em que:

- DT é a Disponibilidade Total no mês em que a solução esteve disponível para os usuários executarem os serviços de negócio da CONTRATANTE.
- DP é a Disponibilidade Prevista que será a quantidade de horas do mês em questão, considerando o período de 24 horas por dia e 7 dias per semana.
- IJ é a Indisponibilidade Justificada no mês causada por fatores fora do alcance da CONTRATADA como problemas na infraestrutura da CONTRATANTE. Consideram-se janelas programadas de mudança, ou seja, períodos previamente acordados para aplicação de qualquer mudança na solução ou na infraestrutura que a suporta. Essas mudanças devem ocorrer fora do horário comercial.

A medição da disponibilidade total da solução será composta pelo monitoramento implantado pela CONTRATANTE, que poderá ser validado pela CONTRATADA a qualquer tempo.

O monitoramento estabelecido pela CONTRATANTE poderá conter testes automatizados que irão medir:

- O acesso ao sistema;
- O processo de login;
- A execução de *scripts* ou *jobs*;
- A execução de funcionalidades no sistema;
- A conformidade de requisitos não funcionais; ou
- Qualquer teste necessário para mensurar a real disponibilidade da solução e de seus processos de negócio. Para os cálculos de Disponibilidade, será levado em consideração somente o que diz respeito à CONTRATADA excluindo falhas na infraestrutura da CONTRATANTE e calculando somente indisponibilidades causadas por eventos como falhas na aplicação, no código, nas consultas ao banco de dados, nas integrações, nas customizações ou em qualquer item da solução.

Considerações gerais

As cláusulas de cunho administrativo e/ou legais serão incluídas no instrumento contratual, conforme modelo estabelecido pela Gerência de Compras e Contratos - GECOC. Em especial deverão ser atendidas as disposições da Lei nº 13.709/2018 – LGPD.

Critério de aceitação – Métrica e periodicidade

Métrica 1	
Indicador de Qualidade	Percentual do indicador de início de atendimento, constante no item 8 – Modelo de Execução do Contrato – ANS.
Mínimo aceitável	95% da métrica de indicador de início de atendimento, definido no item 8 – Modelo de Execução do Contrato – ANS.
Métrica	Quantidade de chamados com suporte técnico iniciado no prazo vezes 100, dividido pela quantidade de chamados abertos.
Ferramentas	Relatórios de atendimento de chamados emitidos pela CONTRATADA.
Periodicidade de Aferição	Primeiro dia útil do mês subsequente da prestação do serviço.

Sanções

O não cumprimento total ou parcial das obrigações assumidas, na forma e nos prazos estabelecidos, sujeitará a CONTRATADA as seguintes penalidades:

1. advertência, em casos de inexecução total ou parcial do contrato, conforme a gravidade;
2. multa de:
    - até 5% (cinco por cento) sobre o valor total do contrato, em caso de inexecução parcial da obrigação assumida, sem prejuízo à eventual indenização suplementar, nos termos da segunda parte do parágrafo único do artigo 416 do Código Civil;
    - até 10% (dez por cento) sobre o valor total do contrato, em caso de inexecução total da obrigação assumida;
    - 0,5% (cinco décimos por cento) ao dia sobre o valor total do contrato, no caso da não correção de serviços que estejam em desacordo com o contrato e com a proposta técnica da CONTRATADA, imediatamente após a notificação da CONTRATANTE;
3. Rescisão unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais.

Os casos de descumprimento do percentual mínimo aceitável, referente aos indicadores de início de atendimento e de disponibilidade da solução, constante no item 8 – Modelo de Gestão do Contrato, conforme definido nesta Especificação Técnica de Serviços como mínimo aceitável, serão enquadrados como inexecução parcial do contrato.

Será considerado como inexecução total do contrato, podendo incorrer rescisão contratual, as situações a partir de 3 (três) enquadramentos parciais consecutivos.

Em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstâncias do caso específico.

As multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades.

Não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves.

Sendo rescindido o presente contrato, o pagamento devido à CONTRATADA será proporcional aos serviços prestados até a data da resolução.

Para se ressarcir de eventuais prejuízos causados pela CONTRATADA e cobrar o valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar o valor do prejuízo e da multa do pagamento decorrente deste contrato, dos valores devidos à CONTRATADA.

Caso o procedimento previsto no item anterior não seja suficiente para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará cobrança à CONTRATADA.

No processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

9 – DOTAÇÃO ORÇAMENTÁRIA	
Nº	**Conta Contábil**
1	817390010400001 - DESENVOLVIMENTO, LICENÇA DE USO E MANUT. DE SISTEMA

10 – CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

ADJUDICAÇÃO DO OBJETO ☐ **Preço global** ☒ **Técnica e Preço** ☐ **Por lote** ☐ **Por item**

Documentação

A empresa participante deverá encaminhar a seguinte documentação:

1 Proposta Técnica Comercial:

1.1 Proposta de preços, contendo especificação completa da solução ofertada, em atendimento ao solicitado neste documento, que deverá ser entregue em papel timbrado da empresa, **devidamente assinada pelo responsável**;

1.2 Planilha do Anexo I – Especificação dos itens entregáveis e requisitos obrigatórios e desejáveis, **devidamente preenchida e assinada pelo responsável;**

1.3 Dados da empresa (CNPJ, razão social e contato do responsável);

1.4 Valor unitário, valor total e unidade de medida (valores em reais);

1.5 Valor de implantação da solução, do serviço de suporte técnico, do repasse de conhecimento e da operação assistida;

1.6 Declarar na Proposta comercial a concordância com a forma de faturamento estabelecido no item 7 - Modelo de Execução do Contrato, subitem Forma de Pagamento em Função dos Resultados;

1.7 Dados bancários da empresa (conta jurídica);

1.8 Data da proposta atualizada, com validade de pelo menos 60 (sessenta) dias corridos.

1.9 Incluir nos preços todos os custos e despesas que, direta ou indiretamente, que decorram das obrigações a serem, tais como e sem se limitar a: telefone, transporte, passagens e diárias, hospedagem, deslocamento, alimentação, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, *softwares*, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.

2 Declarações:

2.1 Declaração de menor - Documento que comprove que a empresa não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII, do art. 7º da Constituição Federal, conforme modelo anexo.

2.2 Declaração Auditoria e Plano de Continuidade de Negócio - A empresa participante deverá declarar se é acompanhada por auditoria interna ou externa, se responsabilizando pela veracidade das informações prestadas, estando sujeita a sanções na forma da lei e sobre a existência de plano de continuidade de negócios, garantindo a prestação de serviços conforme estabelecido nos itens 3 - DESCRIÇÃO DA SOLUÇÃO e 4 ESPECIFICAÇÃO DA

SOLUÇÃO, se responsabilizando pela veracidade das informações prestadas, conforme modelo anexo.

2.3 Declaração de atendimento quanto à especificação técnica e aceitação da minuta de contrato - Documento que comprove que a empresa atende aos requisitos e critérios estabelecidos na Especificação Técnica, conforme modelo anexo.

3 Atestado de Capacidade técnica

3.1 Para fins de qualificação técnica a empresa participante deverá apresentar à POUPEX atestado(s) de capacidade técnica, em seu nome (incluindo o CNPJ), que comprove(m) a prestação de serviços conforme descritos nesta especificação técnica, com data de emissão de até 12 meses contados da data da sua apresentação.

3.2 No caso de atestados emitidos por empresas privadas, não serão aceitos aqueles emitidos por empresas do mesmo grupo empresarial da própria empresa.

3.3 Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras desta ou que possuam pelo menos uma mesma pessoa física ou jurídica que conste no quadro societário da empresa emitente e da empresa proponente.

4 Certidão Negativa de Falência ou Recuperação Judicial

5 Demais exigências

5.1 Documentação informando os critérios utilizados na contratação de serviços em nuvem; e

5.2 Documentação informando os controles de segurança adotados referentes aos serviços em nuvem para assegurar a proteção e privacidade dos dados dos clientes.

6 Qualificação econômico-financeira

6.1 Declaração de Regime de Tributação

6.2 Serão aceitos o balanço patrimonial e demonstrações contábeis assim apresentados:

6.2.1 Para as sociedades anônimas: cópia da publicação em Diário Oficial; ou em jornal de grande circulação, devidamente autenticada na Junta Comercial ou em Ofício de Registro de Títulos e Documentos Civis das Pessoas Jurídicas da sede ou domicílio da empresa; ou balanço patrimonial e demais demonstrações contábeis juntamente com o recibo de entrega da Escrituração Contábil Digital;

6.2.2 Para as sociedades por cotas de responsabilidade limitada: balanço patrimonial e demais demonstrações contábeis juntamente com o recibo de entrega da Escrituração Contábil Digital; ou balanço patrimonial e demais demonstrações contábeis devidamente autenticadas na Junta Comercial ou em Ofício de Registro de Títulos e Documentos Civis das Pessoas Jurídicas da sede ou domicílio da empresa;

6.2.3 Para as sociedades sujeitas à Legislação do Simples: balanço patrimonial e demais demonstrações contábeis juntamente com o recibo de entrega da Escrituração Contábil Digital; ou balanço patrimonial e demais demonstrações contábeis devidamente autenticados na Junta Comercial ou em Ofício de

Registro de Títulos e Documentos Civis das Pessoas Jurídicas da sede ou domicílio da empresa.

6.3 A boa situação financeira será verificada pelos índices resultantes da aplicação das fórmulas a seguir, com resultado superior a 1 (um), com base no balanço patrimonial e demais demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados, quando encerrados há mais de 3 (três) meses da data de apresentação da proposta.

6.4 Excepcionalmente, no caso de empresa recém-constituída e que ainda não tenha encerrado seu primeiro exercício social, poderá ser apresentado no lugar do balanço patrimonial e demonstrações contábeis, o balancete referente ao período compreendido entre o início de suas atividades e o mês anterior à data de apresentação dos documentos para participação neste processo. É obrigatório que a condição de empresa recém-constituída seja devidamente comprovada para aceitação da excepcionalidade ora citada.

Liquidez Geral (LG)

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

Liquidez Corrente (LC)

$$LC = \frac{ATIVO\ CIRCULANTE}{PASSIVO\ CIRCULANTE}$$

Solvência Geral (SG)

$$SG = \frac{ATIVO\ TOTAL}{PASSIVO\ CIRCULANTE + PASSIVO\ NÃO\ CIRCULANTE}$$

6.5 Participação SPE ou de consórcio

6.5.1 Em caso de participação na modalidade de SPE (Sociedade de Propósito Específico) ou consórcio deverão ser apresentados os seguintes documentos:

6.5.1.1 comprovação de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados; e

6.5.1.2 indicação da empresa líder do consórcio, que será responsável por sua representação perante a POUPEX.

6.5.2 Será admitida, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, do somatório dos valores de cada consorciado;

6.5.3 Fica impedida de a empresa consorciada participar, no mesmo processo de compra, de mais de um consórcio ou de forma isolada;

6.5.4 Os integrantes são responsáveis solidariamente pelos atos praticados em consórcio, tanto na fase de cotação quanto na de execução do contrato.

6.5.5 Deverão ser considerados:

6.5.5.1 acréscimo de 10% (dez por cento) sobre o valor exigido de patrimônio líquido para cada participante individual na habilitação econômico-financeira;

6.5.5.2 o vencedor é obrigado a promover, antes da celebração do contrato, a constituição e o registro do consórcio.

6.5.5.3 a substituição de consorciado deverá ser expressamente autorizada pela POUPEX e condicionada à comprovação de que a nova empresa do consórcio possui, no mínimo, os mesmos quantitativos para efeito de habilitação técnica e os mesmos valores para efeito de qualificação econômico-financeira apresentados pela empresa substituída para fins de habilitação do consórcio no processo de compra que originou o contrato.

6.5.5.4 em caso de apresentação de atestado de desempenho anterior emitido em favor de consórcio do qual tenha feito parte, se o atestado ou o contrato de constituição do consórcio não identificar a atividade desempenhada por cada consorciado individualmente, serão adotados os seguintes critérios na avaliação de sua qualificação técnica:

6.5.5.4.1 caso o atestado tenha sido emitido em favor de consórcio homogêneo, as experiências atestadas deverão ser reconhecidas para cada empresa consorciada na proporção quantitativa de sua participação no consórcio; e

6.5.5.4.2 caso o atestado tenha sido emitido em favor de consórcio heterogêneo, as experiências atestadas deverão ser reconhecidas para cada consorciado de acordo com os respectivos campos de atuação.

6.5.5.5 para fins de comprovação do percentual de participação do consorciado, caso este não conste expressamente do atestado ou da certidão, deverá ser juntada ao atestado ou à certidão cópia do instrumento de constituição do consórcio.

Caso a POUPEX considere necessário, poderá solicitar esclarecimentos e/ou documentos adicionais.

Critérios de julgamento	Justificativa
A POUPEX realizará o julgamento conforme a seguinte metodologia: 1. Somente serão aceitas as soluções que atendam a todos os itens obrigatórios; 2. A pontuação da qualificação técnica será calculada conforme fórmula: NQT = (NQE / MNQA) * 70, sendo:	Buscar a proposta mais vantajosa para a POUPEX, por meio do atendimento dos critérios técnicos, prioritariamente, e de preço especificados neste documento.

• NQT = Nota da Qualificação Técnica; • NQE = Nota do Questionário da Empresa em questão; • MNQA = Maior Nota dos Questionários Apresentados. 3. A pontuação da proposta de preço será calculada conforme fórmula: NPP = (MPVO / VP) * 30, sendo: • NPP = Nota da Proposta de Preço; • MPVO = Menor Preço Válido Ofertado; • VP = Valor da Proposta em questão. 4. A pontuação final do fornecedor será calculada conforme fórmula: NFF = NQT + NPP, sendo: • NFF = Nota Final do Fornecedor; • NQT = Nota da Qualificação Técnica; • NPP = Nota da Proposta de Preço. Obs.: O arredondamento será feito até a quarta casa decimal após a vírgula.	

Anexo I - Especificação dos itens entregáveis e requisitos obrigatórios e desejáveis

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.1	A solução deve implementar a função de DNS Recursivo, ou seja, ser capaz de resolver nomes para IP de forma recursiva utilizando o protocolo DNS sem a necessidade de alterações de código, drivers, pilhas TCP/IP ou substituição do cliente padrão presente nos sistemas operacionais.	OBRIGATÓRIO	
1.1.1.	A solução deve operar exclusivamente sobre o protocolo DNS, não sendo aceitas soluções que oferecem segurança a apenas determinados protocolos ou aplicações como, por exemplo, HTTP(S) e FTP	OBRIGATÓRIO	
1.2	Deve possuir licenciamento válido, garantia e suporte técnico do fabricante por 12 (doze) meses;	OBRIGATÓRIO	
1.3	A solução deverá ser ofertada em nuvem, e deve ser entregue com todos os licenciamentos e subscrições necessários para seu funcionamento.	OBRIGATÓRIO	
1.3.1.	A solução deve implementar mecanismos de alta disponibilidade que não exijam reconfigurações de *appliances* e agentes e intervenções manuais na solução;	OBRIGATÓRIO	
1.3.1.1.	A comunicação do agente com a nuvem deve ser autenticada e criptografada;	OBRIGATÓRIO	
1.3.1.2.	Os serviços em nuvem devem estar localizados em pelo menos 02 (dois) continentes, contendo pelo menos 02 (dois) Datacenters no Brasil localizados em cidades diferentes;	DESEJÁVEL	
1.3.1.3.	Para integração da infraestrutura da CONTRATANTE diretamente com a solução em nuvem, a implantação da solução deve ser através da configuração de DNS *Forwarder* nos servidores internos de DNS da CONTRATANTE, qualquer que seja o sistema operacional ou solução de servidores de DNS, incluindo servidores Windows, Linux, roteadores, firewalls, switches ou outros equipamentos;	OBRIGATÓRIO	
1.3.1.4.	A solução na nuvem deve operar sem a necessidade de instalação de software ou componentes na infraestrutura interna da CONTRATANTE, exceto:	OBRIGATÓRIO	
1.3.1.4.1	Instalação de máquinas virtuais na rede da CONTRATANTE (rede corporativa interna ou tenant na nuvem) para receber as requisições DNS e permitir a identificação de cada dispositivo. Neste caso, a CONTRATANTE fornecerá a infraestrutura para operação das máquinas virtuais;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.3.14.2	Instalação de agentes nos dispositivos (computadores e dispositivos móveis);	OBRIGATÓRIO	
1.4	O sistema deve suportar pelo menos 100 (cem) bilhões de requisições DNS por dia;	OBRIGATÓRIO	
1.5	A solução deve permitir identificar em cada requisição de resolução de nomes o IP interno (privado) da estação, servidor e qualquer outro dispositivo conectado a LAN ou WLAN;	OBRIGATÓRIO	
1.6	1.6. A solução deve permitir visualizar o IP interno (privado) de uma estação mesmo quando esta estação estiver utilizando NAT (*Network Address Translation*);	OBRIGATÓRIO	
1.6.1	É admitido o uso de agente na estação do usuário para esta identificação;	OBRIGATÓRIO	
1.7	Se a solução necessitar o uso de agentes, estes devem ser licenciados para todos os usuários da CONTRATANTE;	OBRIGATÓRIO	
1.7.1	Os agentes devem ser compatíveis com sistemas operacionais Windows 7, 8/8.1 e 10 e superiores e Mac OS X 10.11 e superiores;	OBRIGATÓRIO	
1.8	As informações sobre resoluções de consultas DNS não devem permanecer armazenadas ou em cache nos appliances e nos agentes das estações;	OBRIGATÓRIO	
1.9	A solução deve ser capaz de encaminhar resoluções de domínios customizados para servidores internos da CONTRATANTE, incluindo domínios internos e consulta reversa de DNS;	OBRIGATÓRIO	
1.10	O fabricante da solução deve possuir centro de inteligência contra ameaças em escala global, com mecanismo dinâmico de reputação de domínios, operando 24x7, todos os dias do ano, conectado a diversas fontes de informações sobre atividades e comportamentos na Internet, incidentes de segurança, capaz de realizar análises de malwares, ransomwares e outros agentes maliciosos com atualizações constantes de proteção;	OBRIGATÓRIO	
1.11	A solução deve ser efetiva e permanecer ativa em todo momento, independentemente da conectividade do cliente;	OBRIGATÓRIO	
1.12	Os dispositivos remotos (fora do ambiente da CONTRATANTE) devem poder utilizar o serviço sem que haja necessidade de conectividade com a rede interna da CONTRATANTE;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.13	A solução de filtro de DNS deverá funcionar para os dispositivos remotos em qualquer combinação de configuração a seguir: com dispositivos conectados via VPN ou não e operando em *split tunneling* ou não.	OBRIGATÓRIO	
1.14	Deve permitir no mínimo duas maneiras de funcionamento:		
1.14.1	Por meio de agente instalado no dispositivo;	OBRIGATÓRIO	
1.14.2	Configuração de servidor DNS utilizado pelo dispositivo;	OBRIGATÓRIO	
1.15	Deve possuir inteligência de ameaças atualizada de forma contínua em escala global (Internet) e customizada, criando um mecanismo dinâmico de reputação além de recursos padronizados de forma estática;	OBRIGATÓRIO	
1.16	Dever causar impacto mínimo de performance para o usuário e no *endpoint*;	OBRIGATÓRIO	
1.17	Deve operar nativamente e permitir o uso de uma política geral de segurança na camada DNS;	OBRIGATÓRIO	
1.18	Deve integrar de forma simples no sistema de DNS atual do ambiente de produção, especificamente substituindo as referências de servidores recursivos externos em uso;	OBRIGATÓRIO	
1.19	Deve permitir proteger todas as plataformas cliente e servidor do ambiente que utilizem comunicação internet através de resolução DNS;	OBRIGATÓRIO	
1.20	Deve implementar proteção dos dispositivos quando forem iniciadas conexões para IPs identificados como maliciosos, mesmo quando não houver resolução de nomes;	OBRIGATÓRIO	
1.20.1	Essa proteção deve permanecer quando o usuário estiver dentro e fora da rede corporativa, sem impacto para as demais políticas de segurança configuradas para o local do usuário;	OBRIGATÓRIO	
1.20.2	É admitido o uso de agente instalado nas estações;	DESEJÁVEL	
1.20.3	Não serão aceitas soluções que fazem o redirecionamento de todo o tráfego do usuário;	OBRIGATÓRIO	
1.20.4	A atualização da lista de IPs suspeitos deve ser automática;	OBRIGATÓRIO	
1.20.5	A lista de IPs suspeitos não deve ser armazenada em disco, devendo ser mantida em memória;	OBRIGATÓRIO	
1.21	Suportar todos os tipos de dispositivos, estações de trabalho, servidores, dispositivos móveis, sensores e outros dispositivos *IoT, appliances* e outros, gerenciados e não gerenciados, que se comunicam com a Internet e utilizam o protocolo DNS;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.22	Deve disponibilizar em uma única console recursos de visibilidade, prevenção e contenção de infecções *malware* no ambiente local e usuários remotos;	OBRIGATÓRIO	
1.23	Deve implementar a prevenção (bloqueio) de *malware* avançado em diversos vetores de ataque, abrangendo no mínimo e-mail e acesso Web;	OBRIGATÓRIO	
1.24	Deve bloquear tráfego de Comando e Controle (C&C, C2, *CallBack*, *PhoneHome*) para evitar exfiltração de dados e outros mecanismos de controle remoto implementados por *malware* e *botnets*;	OBRIGATÓRIO	
1.25	Deve possuir a capacidade de estabelecer reputação, *tagging* e inteligência de domínios por mecanismos preditivos e dinâmicos, utilização de modelagem estatística, Aprendizado de Máquina (*Machine Learning*) e aproveitamento automático de utilização de domínios globalmente;	OBRIGATÓRIO	
1.26	Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas e domínios por modelos automáticos de co-ocorrência em escala global (concorrência de acessos);	OBRIGATÓRIO	
1.27	A solução deve utilizar e correlacionar informações relacionadas aos domínios incluindo, pelo menos, IPs para onde aquele domínio resolve, outros domínios que resolvem para os mesmos IPs, usuários que registraram aquele domínio e outros domínios, *Autonomous Systems* que detêm os IPs relacionados e histórico de alterações da resolução do domínio;	OBRIGATÓRIO	
1.28	A solução deve ser capaz de reconhecer padrões de ataques para proteção contra domínios maliciosos novos ou desconhecidos;	OBRIGATÓRIO	
1.29	Deve realizar a detecção e prevenção de DGA's (*Domain Generation Algorithm*) em tempo real, permitindo a obtenção de inteligência e elementos de correlação com outras infraestruturas globais em uso no contexto observado;	OBRIGATÓRIO	
1.30	Deve suportar o uso de API programável e documentada para consulta, integração e complemento de inteligência de ameaças com sistemas externos;	OBRIGATÓRIO	
1.31	Não deve conflitar com nenhum sistema antivírus local ou posicionado em *gateway*;	OBRIGATÓRIO	
1.32	Quando a consulta de resolução de domínio for para domínios seguros, o serviço deve ser transparente para o usuário final, resolvendo o domínio para a resposta correspondente;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.33	O mecanismo de proteção proativo e automático atuante na monitoração em tempo real da solução durante as pesquisas DNS não pode ser um elemento tipo *add-on*, ou seja, deve ser uma funcionalidade núcleo da solução, que não dependa de repasse de ações de bloqueio para sistemas externos como *firewalls*, IPS ou proxy no controle de acesso;	OBRIGATÓRIO	
1.34	A solução deve incorporar a capacidade de controle de acesso por categorias implementado em nível DNS mesmo quando não relacionadas à segurança;	OBRIGATÓRIO	
1.35	Deve permitir a criação de políticas de segurança com base nos endereços IP públicos utilizados pelos servidores de DNS locais;	OBRIGATÓRIO	
1.36	Deve permitir a definição de listas personalizadas de acesso, para permitir (*whitelisting*) e para bloqueio (*blacklisting*), incluindo a capacidade de fazer o *upload* delas;	OBRIGATÓRIO	
1.37	Deve permitir a criação de objetos para identificação de redes internas a partir dos IPs privados;	OBRIGATÓRIO	
1.38	Deve permitir a criação de objetos para identificação de redes a partir do IP público;	OBRIGATÓRIO	
1.38.1	Deve permitir estabelecer configurações que viabilizem a monitoração, prevenção e controle em redes remotas onde o endereçamento Internet mude em intervalos de tempo (dinâmico);	OBRIGATÓRIO	
1.39	Deve permitir a criação de políticas atribuídas a objetos de redes de IPs privados e públicos;	OBRIGATÓRIO	
1.40	Deve permitir a criação de múltiplas políticas de segurança com diferentes critérios de seleção com base no IP interno, IP público, usuário, grupo de usuário, estação de trabalho, segmento de rede;	OBRIGATÓRIO	
1.41	As políticas de segurança devem fornecer, pelo menos, as seguintes funcionalidades:		
1.41.1	Opção de bloqueio de domínios relacionados com artefatos maliciosos e domínios comprometidos, independente da aplicação, protocolo ou porta utilizada pela aplicação;	OBRIGATÓRIO	
1.41.2	Opção de bloqueio de domínios de serviços de DDNS (*Dynamic* DNS);	OBRIGATÓRIO	
1.41.3	Opção de bloqueio de domínios recentemente ativados;	OBRIGATÓRIO	
1.41.4	Opção de bloqueio de domínios potencialmente nocivos que apresentam comportamento suspeito e possam estar relacionados a ameaças;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.41.5	Opção de bloqueio de domínios utilizados para túneis sobre o protocolo DNS (DNS *Tunneling* VPN);	OBRIGATÓRIO	
1.41.6	Opção de bloqueio de domínios relacionados a *botnets* e redes de Comando e Controle (C2), independente da aplicação, protocolo ou porta da aplicação;	OBRIGATÓRIO	
1.41.7	Opção de bloqueio de domínios relacionados com *phishing* ou fraudes para obter dados pessoais ou financeiros;	OBRIGATÓRIO	
1.41.8	Opção de bloqueio de domínios com base na classificação da categoria do domínio;	OBRIGATÓRIO	
1.41.8.1	Deve suportar, no mínimo, as seguintes categorias: *Command & Control callbacks, Malware, Phishing, Cryptomining, Pornography, Gambling, Illegal Activities, Terrorism, Proxy/Anonymizer, Personal VPN* ou equivalentes.	OBRIGATÓRIO	
1.41.9	Opção de bloqueio de domínios utilizados para mineração de criptomoedas;	OBRIGATÓRIO	
1.41.10	Opção de bloqueio de aplicativos incluindo, pelo menos, os aplicativos *Anonymizers*, Amazon Drive, Dropbox, Box, Google Drive, Mega, Microsoft OneDrive, BitTorrent, Amazon Video, Google Play Movies, Google Play Music, HBO Now, Netflix, Spotify, YouTube e Twitch;	OBRIGATÓRIO	
1.41.11	Opção de permissão de aplicativos que foram bloqueados por determinadas categorias, incluindo, pelo menos, os aplicativos listados no item anterior;	OBRIGATÓRIO	
1.41.12	Permitir a criação de listas brancas (*whitelist*) e listas negras (*blacklist*) globais de domínios, ou seja, aplicada a todas as políticas, e específicos por política de segurança;	OBRIGATÓRIO	
1.41.13	Permitir que políticas de segurança funcionem em modo restrito permitindo somente acessos a domínios de uma lista branca;	OBRIGATÓRIO	
1.42	As alterações de configuração das políticas de segurança devem ser efetivadas imediatamente, sem necessidade de atualização de bases ou assinaturas nos agentes;	OBRIGATÓRIO	
1.43	O bloqueio aos domínios maliciosos deve ser implementado através da resposta da consulta DNS para um IP seguro;	OBRIGATÓRIO	
1.44	A solução deve permitir o controle de acesso baseado em políticas que incorporem identidades como elementos de decisão de contexto de acesso, incluindo os decorrentes de capacidade de integração com Microsoft Active Directory como:	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.44.1	Usuários;	OBRIGATÓRIO	
1.44.2	Grupos;	OBRIGATÓRIO	
1.44.3	Sistemas/endpoints;	OBRIGATÓRIO	
1.44.4	Redes, IP's, CIDR;	OBRIGATÓRIO	
1.45	A solução não deve depender de listas locais, *feeds*, antivírus ou *proxies* para:		
1.45.1	Manutenção e automação do conteúdo das categorias de segurança padrão;	OBRIGATÓRIO	
1.45.2	Prover visibilidade e detecção de condições de "*Fast Fluxing*" (redes utilizadas por várias *botnets* para esconder os domínios utilizados para baixar *malware* ou hospedar sites web com *phishing*) de infraestruturas e domínios suspeitos, maliciosos e dinâmicos;	OBRIGATÓRIO	
1.45.3	Prover visibilidade e prevenção de exposição contra ataques incorporando "*Domain-Shadowing*" (processo de criação de subdomínios por proprietários de domínio usando credenciais) e cadeias de acesso aos portais de distribuição de *malware* e ataques;	OBRIGATÓRIO	
1.46	A solução deve ser acessível para usuários localizados na rede local da CONTRATANTE e remotamente, de qualquer local conectado à Internet, sendo admitida a instalação de agentes nas estações de trabalho remotas;	OBRIGATÓRIO	
1.46.1	Deve ser fornecida, sem ônus adicional para a CONTRATANTE, toda a infraestrutura incluindo hardware, software, licenças e assinaturas e demais componentes em alta disponibilidade necessários para o uso da solução por usuários remotos;	OBRIGATÓRIO	
1.46.2	A comunicação do agente com a nuvem deve ser autenticada e criptografada;	OBRIGATÓRIO	
1.47	A utilização da solução por usuários localizados na rede LAN ou WLAN não deve exigir a instalação de agentes;	OBRIGATÓRIO	
1.48	Deve ser licenciado para todos os usuários corporativos, independentemente do local de trabalho;	OBRIGATÓRIO	
1.49	Deve permitir a personalização de múltiplas páginas de bloqueio de acesso e uso em distintas políticas de forma simultânea;	OBRIGATÓRIO	
1.50	Caso o usuário esteja utilizando um navegador web através de HTTP e HTTPS, a solução deve exibir uma página indicado o motivo do bloqueio;	OBRIGATÓRIO	
1.50.1	Deve permitir a definição de um texto que deve ser apresentado na página de bloqueio;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.50.2	Permitir a criação de páginas personalizadas diferenciadas por tipo de bloqueio, incluindo bloqueios por categoria, lista negra, *phishing* e política de segurança;	OBRIGATÓRIO	
1.50.3	Permitir a configuração de uma URL para redirecionamento do usuário;	OBRIGATÓRIO	
1.50.4	Permitir a configuração de um formulário para contato com o administrador;	OBRIGATÓRIO	
1.50.5	Para acesso utilizando HTTPS, a solução deve disponibilizar o certificado utilizado para criptografia da sessão ou permitir a importação de um certificado e a chave privada correspondente;	OBRIGATÓRIO	
1.51	Todas as configurações do serviço devem ser realizadas através de ferramenta gráfica a partir de um portal com acesso via web utilizando protocolo seguro (HTTPS);	OBRIGATÓRIO	
1.52	Permitir o acesso simultâneo de múltiplos administradores;	OBRIGATÓRIO	
1.53	Permitir a criação de administradores com perfis de acesso total, somente leitura e somente geração de relatórios;	OBRIGATÓRIO	
1.54	Deve permitir que condições de bloqueio sejam tratadas de forma diferente, incluindo recursos de by-pass configurável por usuários e códigos com tempos de duração preestabelecidos para contextos específicos de acesso e categorias;	OBRIGATÓRIO	
1.55	Deve permitir integração para SSO (*Single Sign-On*) através do padrão aberto SAML (*Security Assertion Markup Language*) para autenticação com provedores SAML, como Okta, PingID, Onelogin e outros, por definição de metadata, devendo suportar adicionalmente, pelo menos, ADFS (Active *Directory Federation Services*).	OBRIGATÓRIO	
1.56	Deve permitir a utilização de mecanismo para implementar dois fatores de autenticação para acesso a console de gerenciamento através de SMS ou aplicativo para dispositivos móveis compatível com Android e iOS;	OBRIGATÓRIO	
1.56.1	O aplicativo deve estar disponível para download por todos os usuários da CONTRATANTE;	OBRIGATÓRIO	
1.57	Não deve conflitar com nenhum sistema *sandbox* posicionado como *endpoint* em segmentos de rede ou plataforma *gateway*;	OBRIGATÓRIO	
1.58	Não deve precisar de um mecanismo de *firewall* para bloqueio de exposição a ameaças em tempo real;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.59	Não deve precisar realizar nenhum tipo de inspeção profunda no tráfego internet para permitir o bloqueio de acesso a infraestruturas dinâmicas suspeitas, realizando a distribuição de ameaças ou comprometidas em tempo real;	OBRIGATÓRIO	
1.60	Não deve precisar de integração com *proxy* para bloqueio de ameaças em tempo real;	OBRIGATÓRIO	
1.61	Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo;	OBRIGATÓRIO	
1.62	Não deve ser uma solução para substituição de infraestrutura de DNS interno, serviço DHCP ou *firewall*;	OBRIGATÓRIO	
1.63	Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas pela monitoração automática de endereçamento IP e suas respectivas ASN incluindo atribuição DNS e correlação WHOIS automática;	OBRIGATÓRIO	
1.64	Deve nativamente e automaticamente permitir a monitoração através de uma modelagem contínua que quantifica, estabelece *ranking* e identifica padrões de utilização de infraestruturas, estabelecendo critérios de detecção e correlação com campanhas e mecanismos direcionados de ataques;	OBRIGATÓRIO	
1.65	A solução deve possuir um mecanismo automático de roteamento por *Anycast* em escala global;	OBRIGATÓRIO	
1.66	A solução deve permitir páginas de bloqueio customizáveis, configuração de *Bypass* ou *Sinkhole*;	OBRIGATÓRIO	
1.67	Deve permitir um mecanismo de busca de inteligência para domínios, IP's, HASH, incluindo a automação destas por uso de API's;	OBRIGATÓRIO	
1.68	Não serão aceitas soluções IPAM (IP *Address Management*);	OBRIGATÓRIO	
1.69	Deve permitir implementar um mecanismo de integração com RSA *NetWitness*;	DESEJÁVEL	
1.70	Deve permitir proteger sistemas dentro e fora do perímetro de segurança;	OBRIGATÓRIO	
1.71	Deve ser capaz de alimentar inteligência de ameaças a plataformas SIEM (*Security Information and Event Management*);	OBRIGATÓRIO	
1.72	Deve ser capaz de monitorar a atividade de rede em tempo real;	OBRIGATÓRIO	

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
1.73	Deve ser capaz de monitorar a utilização de serviços em nuvem (*Cloud Services*) para identificar riscos e desenvolver atividades de conformidade de forma automática;	OBRIGATÓRIO	
1.74	Deve permitir a identificação de ataques direcionados;	OBRIGATÓRIO	
1.75	Deve permitir a comparação do tráfego DNS local e utilização de um domínio contra os padrões globais de tráfego;	OBRIGATÓRIO	
1.76	Deve permitir a visualização de informações além de endereços IP ou DNS, como o relacionamento inteiro com a ASN (*Autonomous System Number*);	OBRIGATÓRIO	
1.77	Deve permitir exportar logs DNS para um repositório terceiro para análise posterior;	OBRIGATÓRIO	
1.78	Deve permitir, nativamente, o uso de inteligência gerada por tecnologia de virtualização de artefatos, sejam suspeitos ou maliciosos, incorporando-o diretamente no processo de defesa proativa em nível DNS de forma automática;	OBRIGATÓRIO	
1.79	Permitir a criação de usuários com autorização de transpor o bloqueio por categoria de conteúdo e lista de domínios, sem a necessidade de reconfigurar os servidores DNS destes usuários;	OBRIGATÓRIO	
1.79.1	Permitir a criação de códigos temporários com autorização de transpor o bloqueio por categoria de conteúdo e lista de domínios, sem a necessidade de reconfigurar os servidores DNS destes usuários;	OBRIGATÓRIO	
1.80	Deve permitir o uso de uma API programável e documentada para:	OBRIGATÓRIO	
1.80.1	Automação de envios, pesquisas (*query*) em históricos e processo de análise;	OBRIGATÓRIO	
1.80.2	Automação na utilização de inteligência de ameaças para segurança de DNS, incluindo domínios, IP, URL e *hashes* de arquivos;	OBRIGATÓRIO	
1.81	Deve permitir consolidar, em uma única interface e de forma automática, a correlação de reputação de inteligência DNS de forma individualizada por domínios em escala global com resultados de análise dinâmica e estática de artefatos e indicadores comportamentais para ameaças malware (incluindo *Advanced Persistent Threats*) em escala global.	OBRIGATÓRIO	

Nº	FUNCIONALIDADE DE RELATÓRIOS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
2.1	Possuir relatório de informações gerais contendo, pelo menos, as seguintes informações:		
2.1.1	Gráfico com total de requisições de resolução de domínios realizadas ao longo do tempo;	OBRIGATÓRIO	
2.1.2	Gráfico com total de requisições de resolução de domínios que foram bloqueadas por critérios de segurança, categoria e listas ao longo do tempo;	OBRIGATÓRIO	
2.1.3	Gráfico com total de requisições de resolução de domínios que foram bloqueadas por critérios de segurança, incluindo *malwares*, *phishings*, *botnets* e outros ao longo do tempo;	OBRIGATÓRIO	
2.1.4	Listagem dos, pelo menos, 10 destinos mais solicitados que foram bloqueados e suas quantidades de resoluções;	OBRIGATÓRIO	
2.1.5	Listagem dos clientes com mais solicitações e suas quantidades de resoluções;	OBRIGATÓRIO	
2.1.6	Listagem dos motivos de bloqueio, com as suas quantidades;	OBRIGATÓRIO	
2.1.7	Permitir escolher os períodos destes dados considerando, pelo menos, as janelas de tempo das últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.2	Possuir relatório gráfico com o total de requisições de resolução de domínios ao longo de um período;	OBRIGATÓRIO	
2.2.1	Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.2.2	Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;	OBRIGATÓRIO	
2.3	Possuir relatório com sumário das requisições informando os bloqueios por critérios de segurança, categorias, listas de bloqueio e as resoluções que foram permitidas normalmente;	OBRIGATÓRIO	
2.3.1	Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;	OBRIGATÓRIO	
2.4	Possuir relatório gráfico do volume de requisições de resolução de domínios informando os bloqueios por critérios de segurança, categorias e listas de bloqueio;	OBRIGATÓRIO	
2.4.1	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.5	Possuir relatório com listagem dos domínios resolvidos, informando a data e hora da requisição, o cliente, o destino, o IP privado, IP público, tipo de requisição DNS e a resposta;	OBRIGATÓRIO	

Nº	FUNCIONALIDADE DE RELATÓRIOS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
2.5.1	Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.5.2	Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;	OBRIGATÓRIO	
2.5.3	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.5.4	Permitir a filtragem por critério de segurança;	OBRIGATÓRIO	
2.5.5	Permitir a filtragem por respostas bloqueadas e permitidas;	OBRIGATÓRIO	
2.5.6	Permitir o download do resultado em formato CSV;	OBRIGATÓRIO	
2.6	Possuir relatório com listagem dos domínios mais solicitados, apresentando a classificação da categoria do domínio e o volume de requisições;	OBRIGATÓRIO	
2.6.1	Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.6.2	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.6.3	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.6.4	Permitir a busca e filtragem por IP;	OBRIGATÓRIO	
2.6.5	Permitir a filtragem por critérios de ameaça e risco dos domínios;	OBRIGATÓRIO	
2.7	Possuir relatório com listagem de categorias de domínios mais solicitados, apresentando o volume de requisições;	OBRIGATÓRIO	
2.7.1	Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.7.2	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.7.3	Permitir a filtragem para resoluções bloqueadas e permitidas;	OBRIGATÓRIO	
2.8	Possuir relatório com listagem de origens, incluindo segmentos de rede, IPs públicos, agentes e outros, por quantidade de solicitações, apresentando o volume de requisições;	OBRIGATÓRIO	
2.8.1	Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.8.2	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.8.3	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.8.4	Permitir a filtragem por critérios de ameaça e risco dos domínios;	OBRIGATÓRIO	

Nº	FUNCIONALIDADE DE RELATÓRIOS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
2.9	Possuir relatório por cliente apresentando gráfico da quantidade de solicitações ao longo do tempo com resoluções bloqueadas e permitidas, listagem dos domínios mais acessados, das categorias de riscos e ameaças e das últimas resoluções de nomes realizadas;	OBRIGATÓRIO	
2.9.1	Deve exibir o IP público utilizado para resolução;	OBRIGATÓRIO	
2.9.2	Deve exibir o IP privado do cliente;	OBRIGATÓRIO	
2.9.3	Permitir filtros de, pelo menos, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.10	Possuir relatório por domínio apresentando gráfico da quantidade de solicitações ao longo do tempo com resoluções bloqueadas e permitidas e comparação com o volume de resoluções feitas por outros usuários do serviço no contexto global para aquele domínio, listagem dos clientes que mais solicitaram resolução, das últimas resoluções de nomes realizadas;	OBRIGATÓRIO	
2.10.1	Deve exibir o IP público utilizado para resolução;	OBRIGATÓRIO	
2.10.2	Deve exibir o IP privado do cliente;	OBRIGATÓRIO	
2.10.3	Permitir filtros de, pelo menos, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.11	Possuir relatório de domínios agrupados por serviços online disponíveis na Internet incluindo, por exemplo, porém, não se limitando a, Office 365, Dropbox, Salesforce, LinkedIn, Google Docs, Reddit, Facebook, Gmail e outros;	OBRIGATÓRIO	
2.11.1	Deve informar a classificação do serviço;	OBRIGATÓRIO	
2.11.2	Deve informar o volume de solicitações de resoluções realizadas e a quantidade bloqueada;	OBRIGATÓRIO	
2.11.3	Deve informar o volume de clientes que fizeram requisições;	OBRIGATÓRIO	
2.11.4	Deve informar a data da primeira requisição e a última data;	OBRIGATÓRIO	
2.11.5	Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.11.6	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.11.7	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.11.8	Permitir a busca por um serviço;	OBRIGATÓRIO	
2.12	Possuir relatório de aplicações *online* identificadas informando o nome da aplicação, o fornecedor da aplicação, a categoria da aplicação e as quantidades de aplicações da mesma categoria;	OBRIGATÓRIO	
2.13	Possuir ferramenta de extração de relatórios permitindo busca a partir de:		

Nº	FUNCIONALIDADE DE RELATÓRIOS	REQUISITO	RESPOSTA DO FORNECEDOR (S/N)
2.13.1	Tipo de resposta: permitida, bloqueada, lista de bloqueio ou de permissão;	OBRIGATÓRIO	
2.13.2	Tipo do cliente: estação de trabalho, usuário, agente, dispositivos de rede, rede ou local;	OBRIGATÓRIO	
2.13.3	Categoria da ameaça;	OBRIGATÓRIO	
2.13.4	Categoria do domínio;	OBRIGATÓRIO	
2.13.5	Permitir a exclusão de domínios que resolvem para CDNs;	OBRIGATÓRIO	
2.14	Deve armazenar todos os registros de acesso por pelo menos 30 dias e permitir seu download em formato CSV;	OBRIGATÓRIO	
2.15	Deve permitir o agendamento para geração e envio automático de relatórios de, pelo menos, os seguintes tipos:		
2.15.1	Listagem das resoluções realizadas, permitindo a filtragem por cliente, domínio, IP de cliente, permissão ou bloqueio, categoria do domínio e risco e ameaça do domínio;	OBRIGATÓRIO	
2.15.2	Listagem de eventos de segurança incluindo *malware*, *botnet* e outras ameaças e riscos, permitindo a filtragem por cliente, domínio, IP de cliente e risco e ameaça do domínio;	OBRIGATÓRIO	
2.15.3	Listagem dos serviços agrupados por domínio, permitindo a filtragem pelo serviço, cliente e a categoria;	OBRIGATÓRIO	
2.15.4	Listagem do volume de requisições, indicando permissão ou bloqueio, permitindo filtragem por cliente;	OBRIGATÓRIO	
2.15.5	Gráfico do volume total, permitindo filtragem por cliente;	OBRIGATÓRIO	
2.15.6	Listagem dos domínios mais resolvidos, permitindo filtragem por cliente, permissão ou bloqueio, domínio, categoria e riscos e ameaça do domínio;	OBRIGATÓRIO	
2.15.7	Listagem das categorias mais resolvidas, permitindo filtragem por cliente, permissão ou bloqueio;	OBRIGATÓRIO	
2.15.8	Listagem dos clientes que mais fazem requisições de resolução, permitindo filtragem por cliente, categoria e riscos e ameaça do domínio;	OBRIGATÓRIO	
2.15.9	Relatório executivo gráfico com o resumo das ameaças bloqueadas, eventos de segurança mais recorrentes e serviços mais acessados;	OBRIGATÓRIO	
2.15.10	Entende-se por cliente qualquer origem da requisição de resolução de nomes, podendo ser um usuário, estação de trabalho, agente, IP público, rede com IP privado ou local, conforme configurações das funcionalidades de segurança	OBRIGATÓRIO	

ANEXO II

Papel Timbrado da Empresa

Declaração de Menor

_____ (Razão Social), inscrita no CNPJ nº._____,declara que não empregar menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14(quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII, do art. 7º da Constituição Federal.

Brasília,___de_____de 2023.

_____

Carimbo, nome e assinatura do Diretor ou representante legal da empresa

Cédula de Identidade (número e órgão expedidor)
CPF/MF (número) e carimbo

ANEXO III

Papel Timbrado da Empresa

Declaração Auditoria e Plano de Continuidade de Negócio

A_____(razão social – nome fantasia)_____, sediada noendereço_____, CEP_____, inscrita no CNPJ n.º_____, (IE ou IMou CF/DF)_____, neste ato, representada por seu (sua)_____ _____(cargo),conforme (documento - contrato social, procuração), Sr.(a) (nome completo)

_____, CPF n.º_____, da CI n.º (número e órgão emissor) _____,(nacionalidade)_____, (estado civil)_____, (profissão) _____,residente e domiciliado (a) em_____ _____, DECLARA que possui:

( ) acompanhamento de auditoria interna;

( ) acompanhamento de auditoria externa, empresa_____;

( ) plano de continuidade de negócios, garantindo a prestação de serviços.

Brasília-DF,___de_____de 2023.

_____

Carimbo, nome e assinatura do Diretor ou representante legal da empresa

Cédula de Identidade (número e órgão expedidor)
CPF/MF (número) e carimbo

ANEXO IV

Papel Timbrado da Empresa

Declaração de Atendimento quanto à Especificação Técnica

A_____(razão social – nome fantasia)_____, sediada noendereço_____, CEP_____, inscrita no CNPJ n.º_____, (IE ou IMou CF/DF)_____, neste ato, representada por seu (sua)_____ _____(cargo),conforme (documento - contrato social, procuração), Sr.(a) (nome completo)

_____, CPF n.º_____, da CI n.º (número e órgão emissor) _____,(nacionalidade)_____, (estado civil)_____, (profissão) _____,residente e domiciliado (a) em_____ _____, DECLARA que atende a Especificação Técnica da solução de proteção da camada de DNS (*Domain Name System*) para os usuários da Instituição, com objetivo de bloquear domínios maliciosos e indesejados, endereços IP (*Internet Protocol* - endereço exclusivo que identifica um dispositivo na internet ou em uma rede local) e aplicativos em nuvem, bem como ACEITA a minuta de contrato anexa à referida especificação técnica.

Brasília-DF,___de_____de 2023.

_____

Carimbo, nome e assinatura do Diretor ou representante legal da empresa

Cédula de Identidade (número e órgão expedidor)
CPF/MF (número) e carimbo

ANEXO V

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ____/2023 - POUPEX

CONTRATO DE PRESTAÇÃO DE SERVIÇOS PARA SOLUÇÃO DE PROTEÇÃO DA CAMADA DE DNS (*DOMAIN NAME SYSTEM* - SISTEMA DE NOMES DE DOMÍNIO) FIRMADO ENTRE A POUPEX E A _____.

A **ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO - POUPEX**, sediada nesta Capital, na Av. Duque de Caxias s/n.º, Parte A, Setor Militar Urbano - SMU, CEP 70630-902, inscrita no CNPJ n.º 00.655.522/0001-21, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) (cargo) _____, na forma autorizada por (documento) _____, Sr.(a) (nome completo) _____, CPF n.º _____, CI n.º (número e órgão emissor) _____, (nacionalidade) _____, (estado civil) _____, (profissão)_____,residente e domiciliado(a) em _____, doravante denominada **CONTRATANTE**, e a (razão social – nome fantasia) _____, sediada no endereço _____, CEP _____, inscrita no CNPJ n.º _____, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) _____ (cargo), conforme (documento - contrato social, procuração)_____, Sr.(a) (nome completo) _____, CPF n.º _____, da CI n.º (número e órgão emissor) _____, (nacionalidade) _____, (estado civil) _____,(profissão)_____, residente e domiciliado (a) em _____, doravante denominada **CONTRATADA**, têm justo e avençado o presente contrato de prestação de serviços, conforme Especificações Técnicas da Solução de TI, de __/__/____ e Proposta Técnica Comercial de ___/___/____, parte integrante deste instrumento, regido pelas cláusulas seguintes e pelas normas de Direito Privado.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente contrato é a contratação de empresa especializada na Solução de proteção da camada de DNS (*Domain Name System* - Sistema de Nomes de Domínio) na modalidade *software* como serviço (SaaS) para os usuários da Instituição, com objetivo de bloquear domínios maliciosos e indesejados, endereços IP (*Internet Protocol* - endereço exclusivo que identifica um dispositivo na internet ou em uma rede local) e aplicativos em nuvem, bem como o suporte técnico da solução, implantação, repasse de conhecimento e operação assistida.

1.1.1. A modalidade SaaS – *Software* como Serviço é aquela em que as aplicações do fornecedor são executadas em uma infraestrutura de nuvem.

2. CLÁUSULA SEGUNDA – CONDIÇÕES PARA EXECUÇÃO DOS SERVIÇOS

2.1. Os serviços serão prestados de forma remota, com disponibilidade de atendimento por telefone, e-mail, *web*, *whatsapp* e/ou videoconferência para as resoluções de incidentes.

2.2. A especificação dos itens entregáveis e requisitos obrigatórios e desejáveis a ser considerada pela CONTRATADA, consta no Apêndice I deste contrato.

2.3. Os serviços de suporte técnico da CONTRATADA será remoto e observará os seguintes requisitos:

2.3.1. operar no formato 24 x 7 x 365, com chamados ilimitados e atendimento diretamente pelo fabricante da solução, através de contato por canal único para centralização dos chamados e controles de ANS (Acordo de Nível de Serviço);

2.3.2. atuar na resolução de incidentes e apoio operacional por meio de acesso telefônico, e-mail, portal web, videoconferência, *software* de mensagens instantâneas e acesso remoto seguro; e

2.3.3. manter atualizada a solução de proteção da camada de DNS em sua última versão estável.

2.4. Os serviços de planejamento, configuração, repasse de conhecimento e operação assistida deverão ser prestados na modalidade remota.

2.5. Em relação aos serviços de planejamento e configuração da solução, a CONTRATADA deverá:

2.5.1. elaborar, em conjunto com a equipe técnica da CONTRATANTE, os documentos de planejamento e o desenho detalhado do projeto e sua implementação;

2.5.2. realizar a implementação da solução, considerando as melhores práticas recomendadas pelo fabricante, observando o cenário da CONTRATANTE, por meio do trabalho integrado entre os profissionais da CONTRATANTE e os especialistas da CONTRATADA;

2.5.3. detalhar, em conjunto com a CONTRATANTE, o uso pretendido dos serviços, as características de uso das aplicações, dos dados, sistemas, requisitos de alta disponibilidade e desempenho;

2.5.4. definir a forma de configuração do ambiente, baseado nas expectativas da CONTRATANTE e premissas do projeto;

2.5.5. realizar o planejamento inicial de implementação, voltado para o oferecimento do melhor desempenho dos serviços, por meio do uso dos recursos disponíveis;

2.5.6. contemplar o plano de implementação do projeto com as configurações necessárias para instalação e parametrização dos serviços e soluções; e

2.5.7. em relação à avaliação do ambiente atual da CONTRATANTE, deverá indicar os ajustes e lacunas que devem ser endereçados para que a implementação seja bem-sucedida.

2.6. Em relação ao serviço de repasse de conhecimento, a CONTRATADA deverá:

2.6.1. realizar o repasse de conhecimento com duração mínima de 4 (quatro) horas para até 5 empregados da CONTRATANTE;

2.6.2. utilizar o modelo de demonstração da solução (*hands on*) para repasse de conhecimento para a equipe técnica da CONTRATANTE, demonstrando as principais funcionalidades e a operação do produto;

2.6.3. utilizar fabricante ou técnico certificado pelo fabricante para repasse de conhecimento;

2.6.4. considerar o ambiente da CONTRATANTE;

2.6.5. considerar a definição da CONTRATAÇÃO de repasse *on-line* (ao vivo) e gravado; e

2.6.6. durante o repasse deverá permitir a interação entre as equipes técnicas de CONTRATANTE e CONTRATADA de forma *on-line* para esclarecimento de dúvidas.

2.7. A CONTRATANTE e a CONTRATADA são pessoas jurídicas totalmente distintas e independentes, não configurando este contrato nenhuma forma de sociedade, pelo que os profissionais terceirizados designados pela CONTRATADA para a prestação dos serviços objeto deste contrato atuarão sem qualquer subordinação laboral à CONTRATANTE, não ensejando nenhum vínculo ou relação de trabalho com a CONTRATANTE.

3. CLÁUSULA TERCEIRA – CONDIÇÕES PARA O SUPORTE TÉCNICO

3.1. Os atendimentos do Suporte Técnico devem ser prestados durante a vigência do contrato, sob demanda e ativo, deverão ser executados por profissional com Certificado de Capacitação Oficial do Fabricante, para cada item de (serviço e/ou *software*) que deverá emitir relatórios, sob demanda da CONTRATANTE, a respeito de eventuais incidentes específicos/apurações especiais;

3.2. Será dado início a abertura do chamado para o suporte técnico através dos canais: e-mail (_____) telefone (_____) ou Portal (_____), a ser gerenciado por um canal único de contato técnico para a centralização dos chamados e controles de SLA. O primeiro atendimento é para identificação e classificação de nível de chamado, sobre a sua severidade, que poderá ser URGENTE, ALTA, NORMAL ou BAIXA e passa-se, a contar os prazos de atendimento após esta classificação.

3.3. A disponibilidade do serviço de suporte deve observar o seguinte:

3.3.1. regime de funcionamento 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana e trezentos e sessenta e cinco dias por ano);

3.3.2. não possuir restrição ou limitação de número de abertura de incidentes;

3.3.3. atendimento na língua portuguesa, por telefone, e-mail, *web*, *whatsapp* e/ou videoconferência, com prioridade em caso de "*bugs*" e dúvidas de configuração;

3.3.4. acesso a materiais de apoio à configuração e uso específicos e exclusivos, elaborados pela CONTRATADA;

3.3.5. deverá incluir a resolução de incidentes e apoio operacional por meio de acesso remoto (VNC ou similar).

3.4. Para os chamados ocasionados por falha da solução que não possam ser resolvidos remotamente, a CONTRATADA deverá disponibilizar pronto atendimento presencial, sem ônus, na sede da CONTRATANTE.

3.5. Os atendimentos para manutenção que importem em riscos ao sistema ou aos processos de negócio relacionados deverão ser executados independentemente do horário comercial. Contudo, deverão ser agendados e autorizados previamente pela CONTRATANTE.

3.6. Para os casos em que o problema identificado demande correções na ferramenta, a serem feitas pelo fabricante, deverá ser fornecida solução de contorno, com o restabelecimento do funcionamento da ferramenta e posterior disponibilização da correção, sem prejuízo do Acordo de Nível de Serviço (ANS), os quais findam com a implementação da solução definitiva.

3.7. A CONTRATADA será acionada pela CONTRATANTE prioritariamente através de sistema de gerenciamento de chamados provido pela CONTRATADA, onde cada chamado deverá conter informações sobre classificação, criticidade, descrição detalhada da situação reportada, prazo de solução, dentre

outras informações pertinentes. A CONTRATANTE também acionará a CONTRATADA através de e-mails ou ligações telefônicas, sendo que, nestes casos, a CONTRATADA deverá registrar o chamado no sistema de gerenciamento de chamados e enviá-lo para a CONTRATANTE para controle e acompanhamento.

3.7.1. Um chamado só poderá ser considerado completamente concluído quando o mesmo for aceito e aprovado pela CONTRATANTE responsável pela sua abertura. A não observância de tais condições pela CONTRATADA poderá ser entendido como falta grave com vistas a distorcer a medição dos Níveis Mínimos de Serviço (NMS).

4. CLÁUSULA QUARTA – CONDIÇÕES DO ACORDO DE NÍVEL DE SERVIÇO – ANS

4.1. O intervalo de tempo para início de atendimento do chamado, de acordo com a severidade, deverá observar os critérios seguintes:

Prazo de Atendimento de Chamados	
Severidade	**Atendimento**
Urgente (1)	4 (quatro) horas
Alta (2)	12 (doze) horas
Normal (3)	1 (um) dia
Baixa (4)	3 (três) dias

4.2. A severidade é descrita da seguinte forma em um rol não taxativo:

Severidade	**Descrição**	
Urgente (1)	Interrupção de serviço crítico.	Um serviço crítico em ambiente de produção está indisponível e nenhuma solução de contingência está disponível.
		Um serviço crítico em ambiente de produção, está parado ou não responde e não está sendo possível estabilizá-lo ou reiniciá-lo.
		Mais de 30% (trinta por cento) dos serviços suportados pela solução são afetados.
Alta (2)	Funcionalidades principais.	Uma ou mais funcionalidades estão severamente prejudicadas.
		O uso da ferramenta pode continuar de forma restrita, apesar da produtividade em longo prazo poder ser afetada.
		Possíveis problemas críticos antes de uma atualização.
		Existe solução de contorno temporária para o problema.

Normal (3)	Funcionalidades menores.	Uma ou mais funcionalidades não críticas não estão funcionando, existindo solução de contorno disponível.
		Funcionamento de alguns componentes prejudicados, permitindo que os serviços sejam prestados.
		Possíveis problemas não críticos antes de uma atualização.
Baixa (4)	Perguntas gerais de utilização.	Questões referentes à aparência da solução, incluindo erros na documentação.

4.3. A CONTRATANTE avaliará os serviços prestados pela CONTRATADA por meio da utilização de indicadores de desempenho, que são critérios objetivos e mensuráveis estabelecidos entre CONTRATANTE e CONTRATADA, no intuito de aferir aspectos de qualidade relacionados aos serviços realizados.

4.4. Prazo de Início de Atendimento de Chamados: corresponde ao prazo, em horas corridas, que a CONTRATADA possui para iniciar as demandas solicitadas pela CONTRATANTE, seja através de e-mails, ligações telefônicas e/ou, prioritariamente, através de sistema de gerenciamento de chamados provido pela CONTRATADA, até a entrega à CONTRATANTE.

4.5. Por chamado entende-se qualquer incidente, requisição, problema ou mudança relacionados aos serviços prestados pela CONTRATADA.

4.6. Para medir o desempenho da CONTRATADA quanto ao início de atendimento dos chamados, foi definido o índice de 95%, a ser aferido mensalmente, sendo calculado considerando a quantidade de chamados iniciados dentro do prazo acordado sobre a quantidade total de chamados abertos, conforme fórmula:

$$\text{Indicador de Início de Atendimento (\%)} = \frac{\text{Qtde Chamados Iniciados no Prazo}}{\text{Qtde Chamados Abertos}} * 100$$

4.7. O nível de disponibilidade da Solução será medido através do indicador “Nível de Disponibilidade Atingido” (NDA). O desempenho esperado para esse indicador será de 98%. O índice NDA será aferido mensalmente, conforme fórmula abaixo:

$$\text{NDA (\%)} = \frac{DT + IJ}{DP} * 100$$

Onde:

- **DT (Disponibilidade Total)** - corresponde ao período total em que a solução se manteve disponível para os usuários executarem os serviços de negócio da CONTRATANTE.

- **IJ (Indisponibilidade Justificada)** - corresponde às indisponibilidades causadas por fatores fora da capacidade de gestão da CONTRATADA, como problemas de infraestrutura da CONTRATANTE. Este indicador também considera janelas de mudança previamente acordadas entre CONTRATADA e CONTRATANTE, devidamente autorizadas pela CONTRATANTE, ou seja, períodos para aplicação de qualquer mudança no sistema ou na infraestrutura que o suporta, fora do horário comercial; e

- **DP (Disponibilidade Prevista) -** corresponde ao período em que o sistema deve estar disponível para os usuários executarem os serviços de negócio da CONTRATANTE, considerando o período de 24 horas por dia e 7 dias por semana.

4.7.1. A medição da DT será composta por monitoramento realizado pela CONTRATANTE, podendo ser validada pela CONTRATADA a qualquer tempo.

4.7.2. O cálculo do NDA considera somente as indisponibilidades causadas por falhas na aplicação, no código, nas consultas ao banco de dados, nas integrações, nas customizações ou em qualquer item de sistema ou não, que estejam dentro da capacidade de gestão da CONTRATADA. É responsabilidade da CONTRATADA justificar os casos em que a indisponibilidade for causada por razões alheias à sua capacidade de gestão.

4.8. O monitoramento estabelecido pela CONTRATANTE poderá conter testes automatizados que irão medir:

4.8.1. acesso ao sistema;

4.8.2. processo de *login*;

4.8.3. execução de *scripts* ou *jobs*;

4.8.4. execução de funcionalidades no sistema;

4.8.5. conformidade de requisitos não funcionais; ou

4.8.6. qualquer teste necessário para mensurar a real disponibilidade da solução e de seus processos de negócio.

5. CLÁUSULA QUINTA – PREÇO

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

5.2. As despesas decorrentes deste contrato correrão por conta dos recursos próprios da POUPEX, consignados na conta orçamentária. Centro de custo: _____. Conta contábil/orçamentaria _____.

5.3. Nos preços fixados nesta cláusula estão compreendidos todos os custos e despesas que, direta ou indiretamente, decorram do cumprimento pleno e integral do objeto deste contrato, tais como e sem se limitar a: telefone, fax, transporte, passagens e diárias, hospedagem, deslocamento, alimentação, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, *softwares*, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.

6. CLÁUSULA SEXTA – FORMA E CONDIÇÕES DE PAGAMENTO

6.1. A CONTRATANTE pagará à CONTRATADA pela prestação dos serviços objeto deste contrato, conforme o quadro abaixo, mediante a Atesto na Nota Fiscal, apresentada com 10 (dez) dias de antecedência do vencimento.

Item	Descrição	Qtd.	Valor Unitário	Valor Total
1.	Subscrição de licenciamento de solução de proteção da camada de DNS	2.000		

2.	Serviço de suporte técnico da solução	2.000		
3.	Serviço de implantação da solução	1		
4.	Repasse de conhecimento	1		
5.	Operação assistida	1		
			TOTAL	

6.2. A Nota Fiscal (NFe/DANFE) deverá ser preenchida com os dados da CONTRATANTE informados a seguir:

Razão Social: ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO – POUPEX

CNPJ: 00.655.522/0001-21

Inscrição municipal ou CF/DF: 07.451.631/001-57

End.: Avenida Duque de Caxias, s/n.º, Parte A, Setor Militar Urbano – SMU

Cidade: Brasília/DF

CEP: 70630-902

6.3. A CONTRATANTE obriga-se a efetuar as retenções tributárias incidentes nos percentuais e alíquotas determinados por Leis e Decretos, para as quais a CONTRATADA deverá destacar na Nota Fiscal os respectivos valores das retenções cabíveis.

6.4. Não serão efetuados os recolhimentos referentes ao IRPJ, CSLL, PIS e COFINS, quando a Declaração de Optante pelo SIMPLES Nacional for apresentada junto com a Nota Fiscal. Neste caso, o documento original da Declaração deverá ser enviado pelos Correios para o endereço do item 6.2.

6.5. Para que o pagamento seja realizado por meio de depósito bancário, as informações abaixo devem estar atualizadas, vinculadas ao CNPJ da CONTRATADA, ou de alguma de suas filiais, desde que devidamente registrado na nota fiscal.

Nome do Favorecido – (RAZÃO SOCIAL DA CONTRATADA)

CNPJ – 00.000.000/0000-00

Número do Banco - 000

Nome do Banco - BANCO FULANO S/A

Número da Agência Bancária – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Número da Conta Corrente – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Modalidade de Conta – CONTA CORRENTE/CONTA POUPANÇA

6.6. Na impossibilidade de o pagamento ser realizado por conta corrente, poderá ser emitido o Boleto Bancário pela CONTRATADA, fazendo-se referência à Nota Fiscal emitida.

6.7. O pagamento será liquidado em até 10 (dez) dias úteis após a entrada da nota fiscal na Gerência de Compras e Contratos - GECOC, desde que o serviço esteja devidamente prestado mediante a apresentação do respectivo Termo de Aceite.

6.7.1. A nota fiscal juntamente com o arquivo XML somente serão recebidos no e-mail corporativo pagamento.gecoc@poupex.com.br, até o dia 20 do mês de sua emissão, para que as retenções sejam processadas pela CONTRATANTE até o último dia útil do mesmo mês. Caso não seja possível à CONTRATADA encaminhar as referidas Notas Fiscais nesse prazo, essas deverão ser emitidas com data do

1º (primeiro) dia do mês subsequente.

6.7.2. Todos os campos da Nota Fiscal deverão ser corretamente preenchidos, sem exceção, sob pena de devolução da Nota. A Nota Fiscal emitida com irregularidades (rasuras, dados incompletos, vencimento em desacordo, etc.) será devolvida com as informações que motivaram a rejeição para nova emissão, e será iniciada a contagem de novo prazo para pagamento após as correções pertinentes.

6.8. O custo das tarifas bancárias deverá ser suportado pela CONTRATADA nos casos em que os dados bancários informados estejam em desacordo com o CNPJ da CONTRATADA, ou que apresentem alguma inconsistência que motivaram a rejeição do pagamento.

6.9. Será considerada inválida qualquer forma de cobrança realizada em desacordo com o previsto nesta cláusula.

6.10. O não pagamento de quaisquer valores devidos pela CONTRATANTE no prazo acima mencionado implicará a incidência dos seguintes encargos moratórios, até a data do efetivo pagamento:

6.10.1. Juros de mora de 1% (um por cento) ao mês, calculados “pro rata die”; e

6.10.2. Multa de 2% (dois por cento) sobre o parcelamento em atraso.

7. CLÁUSULA SÉTIMA - PRAZO

7.1. O prazo para a execução dos serviços será de 12 (doze) meses, contados a partir da data de assinatura deste contrato, podendo ser prorrogado por igual(is) e sucessivo(s) período(s), mediante assinatura de Termo(s) Aditivo(s), até o limite de 60 (sessenta) meses, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea:

7.1.1. que os serviços tenham sido prestados regularmente;

7.1.2. a CONTRATADA não tenha sofrido qualquer punição de natureza pecuniária;

7.1.3. a CONTRATANTE ainda tenha interesse na realização do serviço;

7.1.4. o valor do contrato permaneça economicamente vantajoso para a CONTRATANTE; e

7.1.5. a CONTRATADA concorde com a prorrogação do contrato.

7.2. A CONTRATADA deverá, ainda, cumprir os seguintes prazos:

Item	Descrição	Prazos
1.	Assinatura do instrumento contratual	Em até 5 (cinco) dias úteis após a convocação da empresa vencedora.
2.	Planejamento da implantação	Em até 5 (cinco) dias úteis após assinatura do instrumento contratual.
3.	Entrega das licenças	Em até 5 (cinco) dias úteis a partir da entrega do planejamento da implantação.
4.	Implantação da solução	Em até 10 (dez) dias úteis a partir da entrega das licenças.
5.	Repasse de conhecimento	Em até 5 (cinco) dias úteis a partir da implantação da solução.
6.	Serviço de suporte técnico	A partir do recebimento definitivo das licenças e observando o período de vigência do instrumento contratual.
7.	Operação assistida	Em até 5 (cinco) dias úteis a partir da finalização do repasse de conhecimento.

8. CLÁUSULA OITAVA – REAJUSTE

8.1. O valor pactuado no item 5.1. poderá ser reajustado após 12 meses da assinatura deste contrato, desde que solicitado pela CONTRATADA por escrito, sendo calculado pela variação do IPCA/IBGE (Índice Nacional de Preços ao Consumidor Amplo), ou, em caso de sua extinção ou não divulgação, outro índice equivalente, que melhor se ajuste ao objeto do contrato, ou ainda, por acordo entre as partes.

8.2. A CONTRATADA, ao realizar a solicitação de reajuste, deverá encaminhar a memória de cálculo, com base no índice utilizado no item 8.1.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATADA

9.1. São obrigações da CONTRATADA:

9.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

9.1.2. realizar os serviços de acordo com os requisitos estabelecidos na Especificação Técnica da Solução, parte integrante deste contrato;

9.1.3. comunicar por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, prestando os esclarecimentos necessários;

9.1.4. fornecer todas as informações solicitadas, no prazo de 5 (cinco) dias úteis ou prazo determinado para atendimento de demandas legais;

9.1.5. não realizar instalação de *software*, alteração de configuração ou correção de erros dos ambientes computacionais preexistentes, assim como de qualquer outra infraestrutura da CONTRATANTE. Todavia, a CONTRATADA deverá auxiliar a equipe técnica da CONTRATANTE, da melhor forma possível, para que esta possa implementar o plano de ação a fim de que o objetivo de implantação da solução seja atendido com sucesso;

9.1.6. atender prontamente quaisquer orientações e exigências do fiscal técnico da CONTRATANTE, inerentes à execução do objeto contratual;

9.1.7. propiciar todos os meios e facilidades necessárias à fiscalização do instrumento contratual pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

9.1.8. administrar todo e qualquer assunto relativo aos seus profissionais;

9.1.9. disponibilizar à CONTRATANTE acesso aos relatórios ou *dashboards* de monitoramento do ambiente utilizado, visando melhorar a gestão de recursos;

9.1.10. informar de imediato à CONTRATANTE, quaisquer vulnerabilidades ou registros de incidente de segurança cibernética relacionados aos serviços prestados;

9.1.11. excluir os dados armazenados na solução / nuvem ao término do instrumento contratual, em até 10 dias corridos;

9.1.12. cumprir os prazos de ANS acordados para atendimento das demandas vinculadas ao instrumento contratual;

9.1.13. responsabilizar-se pela veracidade, idoneidade, suficiência e exatidão das informações fornecidas à CONTRATANTE;

9.1.14. manter a confidencialidade dos dados, informações e documentos aos quais venha a ter acesso em decorrência da prestação dos serviços contratados, sendo esta obrigação extensiva a seus sócios, diretores, mandatários, assim como todos os empregados envolvidos na contratação, conforme exigências previstas na Lei Geral de Proteção de Dados (LGPD).

9.1.15. refazer, sem ônus para a CONTRATANTE, os serviços executados em desacordo com as características e especificações exigidas neste contrato e constantes da Proposta Comercial da CONTRATADA;

9.1.16. não designar, para a prestação dos serviços objeto deste contrato, familiar de dirigente ou de empregado da CONTRATANTE ou da Fundação Habitacional do Exército – FHE;

9.1.16.1. considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

9.1.17. não se pronunciar em nome da CONTRATANTE, inclusive junto a órgãos de imprensa, sobre nenhum assunto relativo à atividade da mesma, guardar sigilo absoluto quanto a toda informação obtida da CONTRATANTE em decorrência do presente contrato, bem como não divulgar ou reproduzir quaisquer documentos, instrumentos normativos e materiais encaminhados pela CONTRATANTE;

9.1.18. não transferir, por qualquer forma, os direitos e obrigações que o presente contrato lhe atribui, salvo com a expressa anuência da CONTRATANTE, manifestada por escrito e por quem detenha poderes para tanto;

9.1.19. pagar todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre o objeto deste contrato. Fica, desde logo, convencionado que a CONTRATANTE poderá descontar, de qualquer crédito da CONTRATADA, a importância correspondente a eventuais pagamentos dessa natureza, que venha a efetuar por imposição legal;

9.1.20. cumprir todas as leis e instrumentos normativos reguladores da sua atividade empresarial, bem como satisfazer, às suas expensas, todas as exigências legais decorrentes da execução do presente contrato; e

9.1.21. assumir inteira responsabilidade por todos e quaisquer danos provocados à CONTRATANTE, decorrente de atos comissivos e omissivos, praticados por seus sócios, associados, integrantes não sócios, empregados, prestadores de serviços, representantes e prepostos, durante a execução do contrato. Os danos causados à CONTRATANTE serão suportados pela CONTRATADA, sem prejuízo das demais responsabilidades legalmente imputáveis.

9.2. a CONTRATADA é, para todos os fins e efeitos jurídicos, única e exclusiva responsável por seus empregados, prepostos e/ou prestadores de serviços, afastada a CONTRATANTE, em todas as hipóteses, de qualquer responsabilidade fiscal, trabalhista, comercial, civil, penal, administrativa e previdenciária pelos contratos firmados pela CONTRATADA. Desde já, a CONTRATADA obriga-se a excluir a CONTRATANTE de toda demanda judicial promovida por seu empregado, preposto e/ou seu contratado para prestação de serviços objeto deste contrato, isentando a CONTRATANTE de todo e qualquer ônus, responsabilidade e/ou vínculo para com estes;

9.2.1. caso seja mantida a presença da CONTRATANTE em eventuais reclamações trabalhistas ou quaisquer outras ações, administrativas ou judiciais, que tenham como fundamento matérias objeto do presente contrato, a CONTRATADA obriga-se, desde logo e sem qualquer discussão, a ressarcir a CONTRATANTE de todos os valores despendidos e de adiantar pagamentos a serem efetuados em razão de eventuais condenações, no prazo de 24 (vinte e quatro) horas, contados da solicitação nesse sentido, sob pena de multa de 10% (dez por cento) sobre o valor da condenação ou do valor efetivamente pago, em conformidade com o art. 408, do Código Civil.

10. CLÁUSULA DÉCIMA - OBRIGAÇÕES DA CONTRATANTE

10.1. São obrigações da CONTRATANTE:

10.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

10.1.2. fornecer infraestrutura e informações necessárias para implantação da solução e equipe técnica para acompanhamento das atividades, devendo garantir o sigilo das informações;

10.1.3. receber o objeto fornecido pela CONTRATADA, desde que em conformidade com a proposta aceita, emitindo o Termo de Recebimento dos serviços;

10.1.4. permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, caso necessário, o acesso remoto da CONTRATANTE, respeitadas as normas de segurança vigente;

10.1.5. prover as informações necessárias para que a CONTRATADA possa dar andamento às suas atividades, devendo observar o sigilo das informações;

10.1.6. notificar a CONTRATADA, por escrito, sobre ou a respeito de quaisquer irregularidades encontradas nas execuções de serviços fixando-lhe prazos para as correções;

10.1.7. proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços dentro das condições estabelecidas neste contrato; e

10.1.8. efetuar o pagamento de sua responsabilidade na data prevista, desde que cumpridos todos os procedimentos administrativos de responsabilidade da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA – SERVIÇOS EM NUVEM

11.1. Em consonância com a Resolução BACEN nº 4.893, de 2021, no tocante à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a CONTRATADA deverá, no mínimo:

11.1.1. permitir o acesso da CONTRATANTE aos dados e às informações a serem processados ou armazenados;

11.1.2. garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados;

11.1.3. permitir o acesso da CONTRATANTE aos relatórios relativos aos procedimentos e aos controles utilizados para mitigação de vulnerabilidades na liberação de novas versões, segurança cibernética e continuidade do serviço, elaborados por empresa de auditoria especializada independente contratada pela CONTRATADA;

11.1.4. apresentar relatório que comprove a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;

11.1.5. apresentar formalização da existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

11.1.6. apresentar evidências que comprovem:

11.1.6.1.adoção de medidas de segurança para a transmissão e armazenamento dos dados; e

11.1.6.2.manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes.

11.1.7. adotar mecanismos de controle para:

11.1.7.1.definição de processos, testes e trilhas de auditoria;

11.1.7.2.definição de métricas e indicadores adequados; e

11.1.7.3.identificação e a correção de eventuais deficiências.

11.1.8. Em caso de extinção do contrato a CONTRATADA deverá:

11.1.8.1.realizar transferência dos dados armazenados ao novo prestador de serviços ou à CONTRATANTE; e

11.1.8.2.realizar exclusão dos dados armazenados, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

11.2. Para facilitar o entendimento, adotamos a seguinte classificação de serviços em nuvem:

11.2.1. IaaS – Infraestrutura como Serviço;

11.2.2. PaaS- Plataforma como Serviço;

11.2.3. SaaS- *Software* como Serviço; e

11.2.4. Não se aplica.

12. CLÁUSULA DÉCIMA SEGUNDA – DA RESPONSABILIDADE SOCIAL E AMBIENTAL

12.1. Em cumprimento às diretrizes da Política de Responsabilidade Socioambiental da CONTRATANTE, a CONTRATADA se compromete a:

12.1.1. não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal na execução de suas atividades, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

12.1.2. não empregar menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre, e nem menores de 16 (dezesseis) anos, salvo na condição de jovem aprendiz;

12.1.3. não permitir a prática ou a manutenção de atos discriminatórios que limitem o acesso a relação de emprego, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

12.1.4. buscar prevenir e erradicar práticas danosas ao meio ambiente, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos à produção, consumo e destinação dos resíduos sólidos de maneira sustentável, implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

12.1.5. comprovada a não observância dos preceitos acima, a CONTRATANTE notificará a CONTRATADA para a respectiva regularização. O não atendimento da notificação sujeitará a CONTRATADA às penalidades previstas contratualmente e, até mesmo, impossibilitar a renovação do pacto sem prejuízo das cominações legais.

13. CLÁUSULA DÉCIMA TERCEIRA – DA PROTEÇÃO DOS DADOS E DAS INFORMAÇÕES DA CONTRATANTE E DE TERCEIROS

13.1. As Partes reconhecem e declaram que, havendo qualquer hipótese de tratamento de dados em decorrência da presente relação contratual, se comprometem a cumprir as disposições da Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados), assim como as demais regras de proteção de dados aplicáveis ao caso.

13.2. A CONTRATADA se obriga a tratar os dados pessoais a que tiver acesso em razão desta relação unicamente para os fins necessários à execução do objeto descrito na Cláusula Primeira deste instrumento e pelo tempo de vigência do contrato, observadas as demais disposições contratuais e de acordo com a Lei nº 13.709, de 2018.

13.3. A CONTRATADA assegura que qualquer pessoa, física ou jurídica, cujo acesso aos dados pessoais e informações da CONTRATANTE se dê por ocasião deste instrumento, estará vinculada por obrigações contratuais de proteção equivalentes às previstas nesta Cláusula Décima Terceira.

13.4. A CONTRATANTE irá analisar a liberação dos acessos da CONTRATADA às suas dependências, equipamentos, *softwares* e sistemas que forem necessários ao cumprimento do objeto contratual, devendo esta obedecer às normas e políticas de segurança adotadas pela POUPEX.

13.5. A CONTRATADA compromete-se a utilizar recursos de segurança da informação e de tecnologia em versões comprovadamente seguras e atualizadas, adotando mecanismos de detecção e prevenção de ataques cibernéticos.

13.6. A CONTRATADA, além de adotar medidas de segurança, técnicas e administrativas de proteção de dados, integridade e confidencialidade, compromete-se a não utilizar, compartilhar ou comercializar quaisquer elementos de dados pessoais (sejam eles físicos ou lógicos), que se originem, sejam criados ou que passem a ser acessados a partir da assinatura do presente contrato, sendo igualmente vedada a utilização desses dados após o encerramento deste instrumento.

13.7. A CONTRATADA deverá informar, quando solicitado, as medidas de segurança, técnicas e administrativas empregadas com o objetivo de proteger os dados pessoais de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, acesso não autorizado ou qualquer outra forma de tratamento inadequado ou ilícito.

13.8. A CONTRATADA autoriza a CONTRATANTE a realizar avaliações dos controles de segurança de dados, quando for o caso, comprometendo-se a acatar as recomendações que visem a proteger os dados e/ou informações da CONTRATANTE.

13.9. Caso os dados ou informações a que a CONTRATADA venha a ter acesso em razão deste instrumento sejam, de qualquer forma, acessados ou obtidos por pessoa não autorizada, ou caso sejam objeto de fraude, perda ou destruição, a CONTRATADA deverá notificar imediatamente a CONTRATANTE, informando o ocorrido assim que dele tiver ciência.

13.10. Na hipótese de a CONTRATADA violar e/ou divulgar tais dados e/ou informações sem as devidas autorizações, inclusive por meio de atos de seus sócios, integrantes não sócios, empregados, prepostos, prestadores de serviços e/ou terceiros que por meio dela obtiverem o acesso aos respectivos dados e informações, ficará sujeita às penalidades legais, bem como ao pagamento de perdas e danos apurados em processo próprio.

13.11. Sem prejuízo da apuração de perdas e danos, a violação à legislação de proteção de dados ou às previsões desta Cláusula Décima Terceira pela CONTRATADA ou por quaisquer de seus subcontratados poderá ensejar a rescisão contratual, além da possibilidade de incidência de multa equivalente a 5 (cinco) vezes o valor do presente contrato.

13.12. A CONTRATADA reembolsará a CONTRATANTE nos custos incorridos para remediar os danos causados por uma violação de dados.

13.13. Sem expressa autorização da CONTRATANTE, é vedado à CONTRATADA a cessão, a transferência, ou a subcontratação, total ou parcial, dos serviços prestados.

13.14. É igualmente vedado à CONTRATADA armazenar ou realizar transferência internacional de dados e informações a que vier a ter acesso sem expressa autorização da CONTRATANTE.

13.15. Na ocasião do encerramento deste instrumento contratual, serão realizados os seguintes procedimentos:

13.15.1. transferência dos dados e informações à nova prestadora de serviços ou à CONTRATANTE, a critério da última; e

13.15.2. exclusão, pela CONTRATADA, de todos os dados e informações recebidos, após sua transferência e confirmação da integridade e da disponibilidade por parte da CONTRATANTE.

13.15.3. na eventual hipótese de subcontratação, a qual somente se dará por expressa autorização da CONTRATANTE, a CONTRATADA deverá se certificar de que houve a exclusão de todos os dados e informações a que a SUBCONTRATADA teve acesso, enviando à CONTRATANTE os devidos comprovantes de exclusão.

14. CLÁUSULA DÉCIMA QUARTA – CONFIDENCIALIDADE

14.1. A CONTRATADA obriga-se a manter o sigilo sobre as informações fornecidas ou obtidas junto à CONTRATANTE, sejam estas classificadas como “informações confidenciais”, ou não, abrangendo inclusive informações cadastrais, comerciais ou outras obtidas em decorrência da presente contratação, que são de propriedade exclusiva da CONTRATANTE, respondendo a CONTRATADA pelo pagamento das perdas e danos apurados em processo próprio, quando ocorrer a violação ou a divulgação das mesmas, inclusive por atos de seus empregados, prepostos, prestadores de serviços ou terceiros que as obtiverem junto à CONTRATADA.

14.1.1. O referido sigilo se estende mesmo após o término do compromisso contratual, por tempo indeterminado.

14.1.2. A CONTRATANTE tornará disponível à CONTRATADA as informações públicas e não-públicas sobre suas contas, bens, propriedades, direitos, obrigações, negócios e operações, além de outras, doravante referidas, em conjunto, como as “INFORMAÇÕES”.

14.1.3. Serão consideradas como informações públicas aquelas de caráter oficial que forem publicamente divulgadas pela CONTRATANTE.

14.2. As Partes se obrigam, por si, suas controladas, coligadas, seus empregados, administradores, prepostos, terceiros de sua confiança e por seus representantes legais a:

14.2.1. manter confidencialidade sobre todas as INFORMAÇÕES e a não as transmitir nem as revelar a terceiros;

14.2.2. não discutir, perante terceiros, nem usar, divulgar, revelar ou dispor das INFORMAÇÕES para outra finalidade que não aquelas relacionadas à avaliação de seus interesses recíprocos em negociar com a outra parte, cumprindo-lhes adotar cautelas e precauções adequadas no sentido de impedir o uso indevido das INFORMAÇÕES por qualquer pessoa que a estas venha a ter acesso; e

14.2.3. guardar e manter confidencialidade sobre todas as cópias, reproduções, sumários, análises ou comunicados referentes às INFORMAÇÕES ou nestas baseadas, devendo devolvê-los à CONTRATANTE, quando solicitado.

14.3. A parte que estiver recebendo as INFORMAÇÕES ou qualquer outro dado referente às atividades desenvolvidas pela outra parte se obriga e se compromete a protegê-los, a fim de que não sejam revelados a terceiros não autorizados. Todavia, essa obrigação não se aplica às INFORMAÇÕES e/ou dados que:

14.3.1. já forem do domínio público à época em que tiverem sido revelados;

14.3.2. passarem a ser de domínio público, após sua revelação, sem que a divulgação seja efetuada em violação ao disposto neste Acordo;

14.3.3. já forem notoriamente do conhecimento da parte recipiente antes de lhe terem sido revelados; ou

14.3.4. forem legalmente revelados à parte recipiente por terceiros que não os tiverem recebido sob a vigência de uma obrigação de confidencialidade.

15. CLÁUSULA DÉCIMA QUINTA – FISCALIZAÇÃO E GESTÃO DO CONTRATO

15.1. A execução do contrato será acompanhada e fiscalizada pelos seguintes representantes, abaixo CREDENCIADOS.

CONTRATANTE
Gestor do contrato:
Nome: XXXXXXX – CPF: XXXXXXXXXXX – UTA/Telefone: XXXXXXXXXX
Fiscal do Contrato:
Nome: XXXXXXX – CPF: XXXXXXXXXXX – UTA/Telefone: XXXXXXXXXX
CONTRATADA
Preposto:
Nome: XXXXXXX – CPF: XXXXXXXXXXX –Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX
Responsável Técnico:
Nome: XXXXXXX – CPF: XXXXXXXXXXX –Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX

15.2. As alterações dos representantes acima nomeados como Gestores, Fiscais, Prepostos e Responsáveis técnicos, poderão ser realizadas por meio de simples APOSTILAMENTO, sendo estabelecido novo CREDENCIAMENTO.

15.3. O representante da CONTRATANTE denominado Gestor do Contrato, atuará com o apoio do fiscal técnico e fiscal administrativo do Contrato, credenciados neste instrumento.

15.4. O Gestor, juntamente com os fiscais, deverá acompanhar a prestação dos serviços, registrar as ocorrências e determinar as medidas necessárias ao fiel cumprimento do contrato, bem como atestar, no todo ou em parte, a realização dos serviços objeto deste Contrato.

15.5. O atesto dos serviços prestados pela CONTRATANTE para pagamento das notas fiscais não exime a plena responsabilidade da CONTRATADA em garantir o cumprimento total e satisfatório do contrato em conformidade com as especificações estabelecidas quando da contratação.

15.6. O descumprimento total ou parcial das responsabilidades assumidas pela CONTRATADA, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste contrato.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES CONTRATUAIS

16.1. As alterações das obrigações estabelecidas neste contrato deverão ser formalizadas por meio da lavratura de Termo Aditivo, mediante acordo entre as partes, e em conformidade com os preços e condições vigentes.

16.2. Na hipótese de alteração das condições econômicas fundamentais prevalecentes na assinatura deste contrato, as partes ajustarão as cláusulas que assegurarão a recuperação dos valores ora contratados, objetivando a manutenção do equilíbrio econômico-financeiro do contrato.

16.3. A CONTRATADA deverá comunicar à CONTRATANTE quaisquer alterações em seu Contrato Social, razão ou denominação social, objeto, CNPJ e outros e ainda seus dados bancários, endereços, telefones, fax, e demais dados que, porventura, venham interferir na alteração da habilitação e qualificação exigidas para a execução das obrigações contratuais.

17. CLÁUSULA DÉCIMA SÉTIMA – RESILIÇÃO DO CONTRATO

17.1. Independentemente de justificativa e sem que caiba qualquer indenização à outra parte, este contrato poderá ser denunciado a qualquer tempo, pela CONTRATANTE ou pela CONTRATADA, mediante comunicação feita por escrito e com antecedência mínima de 30 (trinta) dias.

18. CLÁUSULA DÉCIMA OITAVA – PENALIDADES

18.1. O inadimplemento total ou parcial das obrigações contratuais dá, à CONTRATANTE, o direito de aplicar as seguintes penalidades:

18.1.1. advertência, em casos de inexecução total ou parcial do contrato, conforme a gravidade;

18.1.2. Multa de:

18.1.2.1. até 5% (cinco por cento) sobre o valor total do contrato, em caso de inexecução parcial da obrigação assumida, sem prejuízo à eventual indenização suplementar, nos termos da segunda parte do parágrafo único do artigo 416 do Código Civil;

18.1.2.2. até 10% (dez por cento) sobre o valor total do contrato, em caso de inexecução total da obrigação assumida;

18.1.2.3. 0,5% (cinco décimos por cento) ao dia sobre o valor total do contrato, no caso da não correção de serviços que estejam em desacordo com o contrato e com a proposta técnica da CONTRATADA, imediatamente após a notificação da CONTRATANTE;

18.1.3. Rescisão unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais;

18.1.4. Os casos de descumprimento dos indicadores de percentuais mínimos aceitáveis, conforme definidos neste contrato, serão enquadrados como inexecução parcial do contrato;

18.1.5. Será considerado como inexecução total do contrato, podendo incorrer rescisão contratual, as situações a partir de 3 (três) enquadramentos parciais consecutivos.

18.1.6. Em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstâncias do caso específico.

18.1.7. As multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades.

18.1.8. Não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves.

18.2. Sendo rescindido o presente contrato, o pagamento devido será proporcional aos serviços prestados até a data da resolução.

18.3. Para se ressarcir de eventuais prejuízos causados pela CONTRATADA e do valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar esses valores do pagamento.

18.4. Caso o procedimento previsto no item anterior não baste para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará a cobrança judicial e ou a competente ação para reparação de danos, independentemente de prévia notificação (judicial ou extrajudicial), à CONTRATADA.

18.5. No processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

19. CLÁUSULA DÉCIMA NONA – VIGÊNCIA

19.1. O presente contrato terá vigência desde a data de sua assinatura e vigorará até ___ de _____ de 20__.

20. CLÁUSULA VIGÉSIMA – CONDIÇÕES GERAIS

20.1. Este contrato e a Proposta Técnica e Comercial constituem a totalidade do acordo entre os signatários com relação às matérias aqui previstas e superam, substituem e revogam os entendimentos, negociações e acordos anteriores.

20.2. Em caso de divergências entre a proposta da CONTRATADA e este instrumento fica desde já acordado que prevalecerão as condições estabelecidas neste contrato.

20.3. Não valerá como precedente, novação, ou renúncia aos direitos que a lei e o presente instrumento asseguram a CONTRATANTE, sua tolerância a eventuais descumprimentos de cláusulas, seus itens e subitens, pela CONTRATADA.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – FORO

21.1. As partes elegem o Foro da Circunscrição Judiciária de Brasília/DF para dirimir quaisquer questões oriundas do presente contrato, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

E por estarem justos e acertados, assinam o presente contrato em duas vias de igual teor, perante duas testemunhas que também subscrevem.

Brasília-DF, de de 2023.

CONTRATANTE	CONTRATADA

TESTEMUNHAS:

Nome:	Nome:
CPF:	CPF:

APÊNDICE I

Nº	CARACTERÍSTICAS TÉCNICAS	REQUISITO	RESPOSTA DO FORNECEDOR
1.1	A solução deve implementar a função de DNS Recursivo, ou seja, ser capaz de resolver nomes para IP de forma recursiva utilizando o protocolo DNS sem a necessidade de alterações de código, drivers, pilhas TCP/IP ou substituição do cliente padrão presente nos sistemas operacionais.	OBRIGATÓRIO	
1.1.1.	A solução deve operar exclusivamente sobre o protocolo DNS, não sendo aceitas soluções que oferecem segurança a apenas determinados protocolos ou aplicações como, por exemplo, HTTP(S) e FTP	OBRIGATÓRIO	
1.2	Deve possuir licenciamento válido, garantia e suporte técnico do fabricante por 12 (doze) meses;	OBRIGATÓRIO	
1.3	A solução deverá ser ofertada em nuvem, e deve ser entregue com todos os licenciamentos e subscrições necessários para seu funcionamento.	OBRIGATÓRIO	
1.3.1.	A solução deve implementar mecanismos de alta disponibilidade que não exijam reconfigurações de *appliances* e agentes e intervenções manuais na solução;	OBRIGATÓRIO	
1.3.1.1.	A comunicação do agente com a nuvem deve ser autenticada e criptografada;	OBRIGATÓRIO	
1.3.1.2.	Os serviços em nuvem devem estar localizados em pelo menos 02 (dois) continentes, contendo pelo menos 02 (dois) Datacenters no Brasil localizados em cidades diferentes;	DESEJÁVEL	
1.3.1.3.	Para integração da infraestrutura da CONTRATANTE diretamente com a solução em nuvem, a implantação da solução deve ser através da configuração de DNS *Forwarder* nos servidores internos de DNS da CONTRATANTE, qualquer que seja o sistema operacional ou solução de servidores de DNS, incluindo servidores Windows, Linux, roteadores, firewalls, switches ou outros equipamentos;	OBRIGATÓRIO	
1.3.1.4.	A solução na nuvem deve operar sem a necessidade de instalação de *software* ou componentes na infraestrutura interna da CONTRATANTE, exceto:	OBRIGATÓRIO	
1.3.1.4.1	Instalação de máquinas virtuais na rede da CONTRATANTE (rede corporativa interna ou tenant na nuvem) para receber as requisições DNS e permitir a	OBRIGATÓRIO	

	identificação de cada dispositivo. Neste caso, a CONTRATANTE fornecerá a infraestrutura para operação das máquinas virtuais;		
1.3.14.2	Instalação de agentes nos dispositivos (computadores e dispositivos móveis);	OBRIGATÓRIO	
1.4	O sistema deve suportar pelo menos 100 (cem) bilhões de requisições DNS por dia;	OBRIGATÓRIO	
1.5	A solução deve permitir identificar em cada requisição de resolução de nomes o IP interno (privado) da estação, servidor e qualquer outro dispositivo conectado a LAN ou WLAN;	OBRIGATÓRIO	
1.6	1.6. A solução deve permitir visualizar o IP interno (privado) de uma estação mesmo quando esta estação estiver utilizando NAT (Network Address Translation);	OBRIGATÓRIO	
1.6.1	É admitido o uso de agente na estação do usuário para esta identificação;	OBRIGATÓRIO	
1.7	Se a solução necessitar o uso de agentes, estes devem ser licenciados para todos os usuários da CONTRATANTE;	OBRIGATÓRIO	
1.7.1	Os agentes devem ser compatíveis com sistemas operacionais Windows 7, 8/8.1 e 10 e superiores e Mac OS X 10.11 e superiores;	OBRIGATÓRIO	
1.8	As informações sobre resoluções de consultas DNS não devem permanecer armazenadas ou em cache nos appliances e nos agentes das estações;	OBRIGATÓRIO	
1.9	A solução deve ser capaz de encaminhar resoluções de domínios customizados para servidores internos da CONTRATANTE, incluindo domínios internos e consulta reversa de DNS;	OBRIGATÓRIO	
1.10	O fabricante da solução deve possuir centro de inteligência contra ameaças em escala global, com mecanismo dinâmico de reputação de domínios, operando 24x7, todos os dias do ano, conectado a diversas fontes de informações sobre atividades e comportamentos na Internet, incidentes de segurança, capaz de realizar análises de malwares, ransomwares e outros agentes maliciosos com atualizações constantes de proteção;	OBRIGATÓRIO	
1.11	A solução deve ser efetiva e permanecer ativa em todo momento, independentemente da conectividade do cliente;	OBRIGATÓRIO	
1.12	Os dispositivos remotos (fora do ambiente da CONTRATANTE) devem poder utilizar o serviço sem que	OBRIGATÓRIO	

	haja necessidade de conectividade com a rede interna da CONTRATANTE;		
1.13	A solução de filtro de DNS deverá funcionar para os dispositivos remotos em qualquer combinação de configuração a seguir: com dispositivos conectados via VPN ou não e operando em split tunneling ou não.	OBRIGATÓRIO	
1.14	Deve permitir no mínimo duas maneiras de funcionamento:		
1.14.1	Por meio de agente instalado no dispositivo;	OBRIGATÓRIO	
1.14.2	Configuração de servidor DNS utilizado pelo dispositivo;	OBRIGATÓRIO	
1.15	Deve possuir inteligência de ameaças atualizada de forma contínua em escala global (Internet) e customizada, criando um mecanismo dinâmico de reputação além de recursos padronizados de forma estática;	OBRIGATÓRIO	
1.16	Dever causar impacto mínimo de performance para o usuário e no endpoint;	OBRIGATÓRIO	
1.17	Deve operar nativamente e permitir o uso de uma política geral de segurança na camada DNS;	OBRIGATÓRIO	
1.18	Deve integrar de forma simples no sistema de DNS atual do ambiente de produção, especificamente substituindo as referências de servidores recursivos externos em uso;	OBRIGATÓRIO	
1.19	Deve permitir proteger todas as plataformas cliente e servidor do ambiente que utilizem comunicação internet através de resolução DNS;	OBRIGATÓRIO	
1.20	Deve implementar proteção dos dispositivos quando forem iniciadas conexões para IPs identificados como maliciosos, mesmo quando não houver resolução de nomes;	OBRIGATÓRIO	
1.20.1	Essa proteção deve permanecer quando o usuário estiver dentro e fora da rede corporativa, sem impacto para as demais políticas de segurança configuradas para o local do usuário;	OBRIGATÓRIO	
1.20.2	É admitido o uso de agente instalado nas estações;	DESEJÁVEL	
1.20.3	Não serão aceitas soluções que fazem o redirecionamento de todo o tráfego do usuário;	OBRIGATÓRIO	
1.20.4	A atualização da lista de IPs suspeitos deve ser automática;	OBRIGATÓRIO	
1.20.5	A lista de IPs suspeitos não deve ser armazenada em disco, devendo ser mantida em memória;	OBRIGATÓRIO	
1.21	Suportar todos os tipos de dispositivos, estações de	OBRIGATÓRIO	

	trabalho, servidores, dispositivos móveis, sensores e outros dispositivos IoT, appliances e outros, gerenciados e não gerenciados, que se comunicam com a Internet e utilizam o protocolo DNS;		
1.22	Deve disponibilizar em uma única console recursos de visibilidade, prevenção e contenção de infecções malware no ambiente local e usuários remotos;	OBRIGATÓRIO	
1.23	Deve implementar a prevenção (bloqueio) de malware avançado em diversos vetores de ataque, abrangendo no mínimo e-mail e acesso Web;	OBRIGATÓRIO	
1.24	Deve bloquear tráfego de Comando e Controle (C&C, C2, CallBack, PhoneHome) para evitar exfiltração de dados e outros mecanismos de controle remoto implementados por malware e botnets;	OBRIGATÓRIO	
1.25	Deve possuir a capacidade de estabelecer reputação, tagging e inteligência de domínios por mecanismos preditivos e dinâmicos, utilização de modelagem estatística, Aprendizado de Máquina (Machine Learning) e aproveitamento automático de utilização de domínios globalmente;	OBRIGATÓRIO	
1.26	Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas e domínios por modelos automáticos de co-ocorrência em escala global (concorrência de acessos);	OBRIGATÓRIO	
1.27	A solução deve utilizar e correlacionar informações relacionadas aos domínios incluindo, pelo menos, IPs para onde aquele domínio resolve, outros domínios que resolvem para os mesmos IPs, usuários que registraram aquele domínio e outros domínios, Autonomous Systems que detêm os IPs relacionados e histórico de alterações da resolução do domínio;	OBRIGATÓRIO	
1.28	A solução deve ser capaz de reconhecer padrões de ataques para proteção contra domínios maliciosos novos ou desconhecidos;	OBRIGATÓRIO	
1.29	Deve realizar a detecção e prevenção de DGA's (Domain Generation Algorithm) em tempo real, permitindo a obtenção de inteligência e elementos de correlação com outras infraestruturas globais em uso no contexto observado;	OBRIGATÓRIO	
1.30	Deve suportar o uso de API programável e documentada para consulta, integração e complemento de inteligência de ameaças com sistemas externos;	OBRIGATÓRIO	
1.31	Não deve conflitar com nenhum sistema antivírus local	OBRIGATÓRIO	

	ou posicionado em gateway;		
1.32	Quando a consulta de resolução de domínio for para domínios seguros, o serviço deve ser transparente para o usuário final, resolvendo o domínio para a resposta correspondente;	OBRIGATÓRIO	
1.33	O mecanismo de proteção proativo e automático atuante na monitoração em tempo real da solução durante as pesquisas DNS não pode ser um elemento tipo add-on, ou seja, deve ser uma funcionalidade núcleo da solução, que não dependa de repasse de ações de bloqueio para sistemas externos como firewalls, IPS ou proxy no controle de acesso;	OBRIGATÓRIO	
1.34	A solução deve incorporar a capacidade de controle de acesso por categorias implementado em nível DNS mesmo quando não relacionadas à segurança;	OBRIGATÓRIO	
1.35	Deve permitir a criação de políticas de segurança com base nos endereços IP públicos utilizados pelos servidores de DNS locais;	OBRIGATÓRIO	
1.36	Deve permitir a definição de listas personalizadas de acesso, para permitir (whitelisting) e para bloqueio (blacklisting), incluindo a capacidade de fazer o upload delas;	OBRIGATÓRIO	
1.37	Deve permitir a criação de objetos para identificação de redes internas a partir dos IPs privados;	OBRIGATÓRIO	
1.38	Deve permitir a criação de objetos para identificação de redes a partir do IP público;	OBRIGATÓRIO	
1.38.1	Deve permitir estabelecer configurações que viabilizem a monitoração, prevenção e controle em redes remotas onde o endereçamento Internet mude em intervalos de tempo (dinâmico);	OBRIGATÓRIO	
1.39	Deve permitir a criação de políticas atribuídas a objetos de redes de IPs privados e públicos;	OBRIGATÓRIO	
1.40	Deve permitir a criação de múltiplas políticas de segurança com diferentes critérios de seleção com base no IP interno, IP público, usuário, grupo de usuário, estação de trabalho, segmento de rede;	OBRIGATÓRIO	
1.41	As políticas de segurança devem fornecer, pelo menos, as seguintes funcionalidades:		
1.41.1	Opção de bloqueio de domínios relacionados com artefatos maliciosos e domínios comprometidos, independente da aplicação, protocolo ou porta utilizada pela aplicação;	OBRIGATÓRIO	
1.41.2	Opção de bloqueio de domínios de serviços de DDNS	OBRIGATÓRIO	

	(Dynamic DNS);		
1.41.3	Opção de bloqueio de domínios recentemente ativados;	OBRIGATÓRIO	
1.41.4	Opção de bloqueio de domínios potencialmente nocivos que apresentam comportamento suspeito e possam estar relacionados a ameaças;	OBRIGATÓRIO	
1.41.5	Opção de bloqueio de domínios utilizados para túneis sobre o protocolo DNS (DNS Tunneling VPN);	OBRIGATÓRIO	
1.41.6	Opção de bloqueio de domínios relacionados a botnets e redes de Comando e Controle (C2), independente da aplicação, protocolo ou porta da aplicação;	OBRIGATÓRIO	
1.41.7	Opção de bloqueio de domínios relacionados com phishing ou fraudes para obter dados pessoais ou financeiros;	OBRIGATÓRIO	
1.41.8	Opção de bloqueio de domínios com base na classificação da categoria do domínio;	OBRIGATÓRIO	
1.41.8.1	Deve suportar, no mínimo, as seguintes categorias: Command & Control callbacks, Malware, Phishing, Cryptomining, Pornography, Gambling, Illegal Activities, Terrorism, Proxy/Anonymizer, Personal VPN ou equivalentes.	OBRIGATÓRIO	
1.41.9	Opção de bloqueio de domínios utilizados para mineração de criptomoedas;	OBRIGATÓRIO	
1.41.10	Opção de bloqueio de aplicativos incluindo, pelo menos, os aplicativos Anonymizers, Amazon Drive, Dropbox, Box, Google Drive, Mega, Microsoft OneDrive, BitTorrent, Amazon Video, Google Play Movies, Google Play Music, HBO Now, Netflix, Spotify, YouTube e Twitch;	OBRIGATÓRIO	
1.41.11	Opção de permissão de aplicativos que foram bloqueados por determinadas categorias, incluindo, pelo menos, os aplicativos listados no item anterior;	OBRIGATÓRIO	
1.41.12	Permitir a criação de listas brancas (whitelist) e listas negras (blacklist) globais de domínios, ou seja, aplicada a todas as políticas, e específicos por política de segurança;	OBRIGATÓRIO	
1.41.13	Permitir que políticas de segurança funcionem em modo restrito permitindo somente acessos a domínios de uma lista branca;	OBRIGATÓRIO	
1.42	As alterações de configuração das políticas de segurança devem ser efetivadas imediatamente, sem necessidade de atualização de bases ou assinaturas nos	OBRIGATÓRIO	

	agentes;		
1.43	O bloqueio aos domínios maliciosos deve ser implementado através da resposta da consulta DNS para um IP seguro;	OBRIGATÓRIO	
1.44	A solução deve permitir o controle de acesso baseado em políticas que incorporem identidades como elementos de decisão de contexto de acesso, incluindo os decorrentes de capacidade de integração com Microsoft Active Directory como:	OBRIGATÓRIO	
1.44.1	Usuários;	OBRIGATÓRIO	
1.44.2	Grupos;	OBRIGATÓRIO	
1.44.3	Sistemas/endpoints;	OBRIGATÓRIO	
1.44.4	Redes, IP's, CIDR;	OBRIGATÓRIO	
1.45	A solução não deve depender de listas locais, feeds, antivírus ou proxies para:		
1.45.1	Manutenção e automação do conteúdo das categorias de segurança padrão;	OBRIGATÓRIO	
1.45.2	Prover visibilidade e detecção de condições de "Fast Fluxing" (redes utilizadas por várias botnets para esconder os domínios utilizados para baixar malware ou hospedar sites web com phishing) de infraestruturas e domínios suspeitos, maliciosos e dinâmicos;	OBRIGATÓRIO	
1.45.3	Prover visibilidade e prevenção de exposição contra ataques incorporando "Domain-Shadowing" (processo de criação de subdomínios por proprietários de domínio usando credenciais) e cadeias de acesso aos portais de distribuição de malware e ataques;	OBRIGATÓRIO	
1.46	A solução deve ser acessível para usuários localizados na rede local da CONTRATANTE e remotamente, de qualquer local conectado à Internet, sendo admitida a instalação de agentes nas estações de trabalho remotas;	OBRIGATÓRIO	
1.46.1	Deve ser fornecida, sem ônus adicional para a CONTRATANTE, toda a infraestrutura incluindo hardware, *software*, licenças e assinaturas e demais componentes em alta disponibilidade necessários para o uso da solução por usuários remotos;	OBRIGATÓRIO	
1.46.2	A comunicação do agente com a nuvem deve ser autenticada e criptografada;	OBRIGATÓRIO	
1.47	A utilização da solução por usuários localizados na rede LAN ou WLAN não deve exigir a instalação de agentes;	OBRIGATÓRIO	

1.48	Deve ser licenciado para todos os usuários corporativos, independentemente do local de trabalho;	OBRIGATÓRIO	
1.49	Deve permitir a personalização de múltiplas páginas de bloqueio de acesso e uso em distintas políticas de forma simultânea;	OBRIGATÓRIO	
1.50	Caso o usuário esteja utilizando um navegador web através de HTTP e HTTPS, a solução deve exibir uma página indicado o motivo do bloqueio;	OBRIGATÓRIO	
1.50.1	Deve permitir a definição de um texto que deve ser apresentado na página de bloqueio;	OBRIGATÓRIO	
1.50.2	Permitir a criação de páginas personalizadas diferenciadas por tipo de bloqueio, incluindo bloqueios por categoria, lista negra, phishing e política de segurança;	OBRIGATÓRIO	
1.50.3	Permitir a configuração de uma URL para redirecionamento do usuário;	OBRIGATÓRIO	
1.50.4	Permitir a configuração de um formulário para contato com o administrador;	OBRIGATÓRIO	
1.50.5	Para acesso utilizando HTTPS, a solução deve disponibilizar o certificado utilizado para criptografia da sessão ou permitir a importação de um certificado e a chave privada correspondente;	OBRIGATÓRIO	
1.51	Todas as configurações do serviço devem ser realizadas através de ferramenta gráfica a partir de um portal com acesso via web utilizando protocolo seguro (HTTPS);	OBRIGATÓRIO	
1.52	Permitir o acesso simultâneo de múltiplos administradores;	OBRIGATÓRIO	
1.53	Permitir a criação de administradores com perfis de acesso total, somente leitura e somente geração de relatórios;	OBRIGATÓRIO	
1.54	Deve permitir que condições de bloqueio sejam tratadas de forma diferente, incluindo recursos de by-pass configurável por usuários e códigos com tempos de duração preestabelecidos para contextos específicos de acesso e categorias;	OBRIGATÓRIO	
1.55	Deve permitir integração para SSO (Single Sign-On) através do padrão aberto SAML (Security Assertion Markup Language) para autenticação com provedores SAML, como Okta, PingID, Onelogin e outros, por definição de metadata, devendo suportar adicionalmente, pelo menos, ADFS (Active Directory Federation Services).	OBRIGATÓRIO	

1.56	Deve permitir a utilização de mecanismo para implementar dois fatores de autenticação para acesso a console de gerenciamento através de SMS ou aplicativo para dispositivos móveis compatível com Android e iOS;	OBRIGATÓRIO	
1.56.1	O aplicativo deve estar disponível para download por todos os usuários da CONTRATANTE;	OBRIGATÓRIO	
1.57	Não deve conflitar com nenhum sistema sandbox posicionado como endpoint em segmentos de rede ou plataforma gateway;	OBRIGATÓRIO	
1.58	Não deve precisar de um mecanismo de firewall para bloqueio de exposição a ameaças em tempo real;	OBRIGATÓRIO	
1.59	Não deve precisar realizar nenhum tipo de inspeção profunda no tráfego internet para permitir o bloqueio de acesso a infraestruturas dinâmicas suspeitas, realizando a distribuição de ameaças ou comprometidas em tempo real;	OBRIGATÓRIO	
1.60	Não deve precisar de integração com proxy para bloqueio de ameaças em tempo real;	OBRIGATÓRIO	
1.61	Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo;	OBRIGATÓRIO	
1.62	Não deve ser uma solução para substituição de infraestrutura de DNS interno, serviço DHCP ou firewall;	OBRIGATÓRIO	
1.63	Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas pela monitoração automática de endereçamento IP e suas respectivas ASN incluindo atribuição DNS e correlação WHOIS automática;	OBRIGATÓRIO	
1.64	Deve nativamente e automaticamente permitir a monitoração através de uma modelagem contínua que quantifica, estabelece ranking e identifica padrões de utilização de infraestruturas, estabelecendo critérios de detecção e correlação com campanhas e mecanismos direcionados de ataques;	OBRIGATÓRIO	
1.65	A solução deve possuir um mecanismo automático de roteamento por Anycast em escala global;	OBRIGATÓRIO	
1.66	A solução deve permitir páginas de bloqueio customizáveis, configuração de Bypass ou Sinkhole;	OBRIGATÓRIO	
1.67	Deve permitir um mecanismo de busca de inteligência para domínios, IP’s, HASH, incluindo a automação destas por uso de API’s;	OBRIGATÓRIO	

1.68	Não serão aceitas soluções IPAM (IP Address Management);	OBRIGATÓRIO	
1.69	Deve permitir implementar um mecanismo de integração com RSA NetWitness;	DESEJÁVEL	
1.70	Deve permitir proteger sistemas dentro e fora do perímetro de segurança;	OBRIGATÓRIO	
1.71	Deve ser capaz de alimentar inteligência de ameaças a plataformas SIEM (Security Information and Event Management);	OBRIGATÓRIO	
1.72	Deve ser capaz de monitorar a atividade de rede em tempo real;	OBRIGATÓRIO	
1.73	Deve ser capaz de monitorar a utilização de serviços em nuvem (Cloud Services) para identificar riscos e desenvolver atividades de conformidade de forma automática;	OBRIGATÓRIO	
1.74	Deve permitir a identificação de ataques direcionados;	OBRIGATÓRIO	
1.75	Deve permitir a comparação do tráfego DNS local e utilização de um domínio contra os padrões globais de tráfego;	OBRIGATÓRIO	
1.76	Deve permitir a visualização de informações além de endereços IP ou DNS, como o relacionamento inteiro com a ASN (Autonomous System Number);	OBRIGATÓRIO	
1.77	Deve permitir exportar logs DNS para um repositório terceiro para análise posterior;	OBRIGATÓRIO	
1.78	Deve permitir, nativamente, o uso de inteligência gerada por tecnologia de virtualização de artefatos, sejam suspeitos ou maliciosos, incorporando-o diretamente no processo de defesa proativa em nível DNS de forma automática;	OBRIGATÓRIO	
1.79	Permitir a criação de usuários com autorização de transpor o bloqueio por categoria de conteúdo e lista de domínios, sem a necessidade de reconfigurar os servidores DNS destes usuários;	OBRIGATÓRIO	
1.79.1	Permitir a criação de códigos temporários com autorização de transpor o bloqueio por categoria de conteúdo e lista de domínios, sem a necessidade de reconfigurar os servidores DNS destes usuários;	OBRIGATÓRIO	
1.80	Deve permitir o uso de uma API programável e documentada para:	OBRIGATÓRIO	
1.80.1	Automação de envios, pesquisas (query) em históricos e processo de análise;	OBRIGATÓRIO	

1.80.2	Automação na utilização de inteligência de ameaças para segurança de DNS, incluindo domínios, IP, URL e hashes de arquivos;	OBRIGATÓRIO	
1.81	Deve permitir consolidar, em uma única interface e de forma automática, a correlação de reputação de inteligência DNS de forma individualizada por domínios em escala global com resultados de análise dinâmica e estática de artefatos e indicadores comportamentais para ameaças malware (incluindo Advanced Persistent Threats) em escala global.	OBRIGATÓRIO	
Nº	**FUNCIONALIDADE DE RELATÓRIOS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR**
2.1	Possuir relatório de informações gerais contendo, pelo menos, as seguintes informações:		
2.1.1	Gráfico com total de requisições de resolução de domínios realizadas ao longo do tempo;	OBRIGATÓRIO	
2.1.2	Gráfico com total de requisições de resolução de domínios que foram bloqueadas por critérios de segurança, categoria e listas ao longo do tempo;	OBRIGATÓRIO	
2.1.3	Gráfico com total de requisições de resolução de domínios que foram bloqueadas por critérios de segurança, incluindo malwares, phishings, botnets e outros ao longo do tempo;	OBRIGATÓRIO	
2.1.4	Listagem dos, pelo menos, 10 destinos mais solicitados que foram bloqueados e suas quantidades de resoluções;	OBRIGATÓRIO	
2.1.5	Listagem dos clientes com mais solicitações e suas quantidades de resoluções;	OBRIGATÓRIO	
2.1.6	Listagem dos motivos de bloqueio, com as suas quantidades;	OBRIGATÓRIO	
2.1.7	Permitir escolher os períodos destes dados considerando, pelo menos, as janelas de tempo das últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.2	Possuir relatório gráfico com o total de requisições de resolução de domínios ao longo de um período;	OBRIGATÓRIO	
2.2.1	Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.2.2	Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;	OBRIGATÓRIO	
2.3	Possuir relatório com sumário das requisições	OBRIGATÓRIO	

	informando os bloqueios por critérios de segurança, categorias, listas de bloqueio e as resoluções que foram permitidas normalmente;		
2.3.1	Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;	OBRIGATÓRIO	
2.4	Possuir relatório gráfico do volume de requisições de resolução de domínios informando os bloqueios por critérios de segurança, categorias e listas de bloqueio;	OBRIGATÓRIO	
2.4.1	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.5	Possuir relatório com listagem dos domínios resolvidos, informando a data e hora da requisição, o cliente, o destino, o IP privado, IP público, tipo de requisição DNS e a resposta;	OBRIGATÓRIO	
2.5.1	Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.5.2	Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;	OBRIGATÓRIO	
2.5.3	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.5.4	Permitir a filtragem por critério de segurança;	OBRIGATÓRIO	
2.5.5	Permitir a filtragem por respostas bloqueadas e permitidas;	OBRIGATÓRIO	
2.5.6	Permitir o download do resultado em formato CSV;	OBRIGATÓRIO	
2.6	Possuir relatório com listagem dos domínios mais solicitados, apresentando a classificação da categoria do domínio e o volume de requisições;	OBRIGATÓRIO	
2.6.1	Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.6.2	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.6.3	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.6.4	Permitir a busca e filtragem por IP;	OBRIGATÓRIO	
2.6.5	Permitir a filtragem por critérios de ameaça e risco dos domínios;	OBRIGATÓRIO	
2.7	Possuir relatório com listagem de categorias de domínios mais solicitados, apresentando o volume de	OBRIGATÓRIO	

	requisições;		
2.7.1	Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.7.2	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.7.3	Permitir a filtragem para resoluções bloqueadas e permitidas;	OBRIGATÓRIO	
2.8	Possuir relatório com listagem de origens, incluindo segmentos de rede, IPs públicos, agentes e outros, por quantidade de solicitações, apresentando o volume de requisições;	OBRIGATÓRIO	
2.8.1	Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.8.2	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.8.3	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.8.4	Permitir a filtragem por critérios de ameaça e risco dos domínios;	OBRIGATÓRIO	
2.9	Possuir relatório por cliente apresentando gráfico da quantidade de solicitações ao longo do tempo com resoluções bloqueadas e permitidas, listagem dos domínios mais acessados, das categorias de riscos e ameaças e das últimas resoluções de nomes realizadas;	OBRIGATÓRIO	
2.9.1	Deve exibir o IP público utilizado para resolução;	OBRIGATÓRIO	
2.9.2	Deve exibir o IP privado do cliente;	OBRIGATÓRIO	
2.9.3	Permitir filtros de, pelo menos, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.10	Possuir relatório por domínio apresentando gráfico da quantidade de solicitações ao longo do tempo com resoluções bloqueadas e permitidas e comparação com o volume de resoluções feitas por outros usuários do serviço no contexto global para aquele domínio, listagem dos clientes que mais solicitaram resolução, das últimas resoluções de nomes realizadas;	OBRIGATÓRIO	
2.10.1	Deve exibir o IP público utilizado para resolução;	OBRIGATÓRIO	
2.10.2	Deve exibir o IP privado do cliente;	OBRIGATÓRIO	
2.10.3	Permitir filtros de, pelo menos, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	

2.11	Possuir relatório de domínios agrupados por serviços online disponíveis na Internet incluindo, por exemplo, porém, não se limitando a, Office 365, Dropbox, Salesforce, LinkedIn, Google Docs, Reddit, Facebook, Gmail e outros;	OBRIGATÓRIO	
2.11.1	Deve informar a classificação do serviço;	OBRIGATÓRIO	
2.11.2	Deve informar o volume de solicitações de resoluções realizadas e a quantidade bloqueada;	OBRIGATÓRIO	
2.11.3	Deve informar o volume de clientes que fizeram requisições;	OBRIGATÓRIO	
2.11.4	Deve informar a data da primeira requisição e a última data;	OBRIGATÓRIO	
2.11.5	Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias.	OBRIGATÓRIO	
2.11.6	Permitir a filtragem por cliente que solicitou a resolução;	OBRIGATÓRIO	
2.11.7	Permitir a filtragem por categoria do domínio;	OBRIGATÓRIO	
2.11.8	Permitir a busca por um serviço;	OBRIGATÓRIO	
2.12	Possuir relatório de aplicações online identificadas informando o nome da aplicação, o fornecedor da aplicação, a categoria da aplicação e as quantidades de aplicações da mesma categoria;	OBRIGATÓRIO	
2.13	Possuir ferramenta de extração de relatórios permitindo busca a partir de:		
2.13.1	Tipo de resposta: permitida, bloqueada, lista de bloqueio ou de permissão;	OBRIGATÓRIO	
2.13.2	Tipo do cliente: estação de trabalho, usuário, agente, dispositivos de rede, rede ou local;	OBRIGATÓRIO	
2.13.3	Categoria da ameaça;	OBRIGATÓRIO	
2.13.4	Categoria do domínio;	OBRIGATÓRIO	
2.13.5	Permitir a exclusão de domínios que resolvem para CDNs;	OBRIGATÓRIO	
2.14	Deve armazenar todos os registros de acesso por pelo menos 30 dias e permitir seu download em formato CSV;	OBRIGATÓRIO	
2.15	Deve permitir o agendamento para geração e envio automático de relatórios de, pelo menos, os seguintes tipos:		
2.15.1	Listagem das resoluções realizadas, permitindo a filtragem por cliente, domínio, IP de cliente, permissão ou bloqueio, categoria do domínio e risco e ameaça do	OBRIGATÓRIO	

	domínio;		
2.15.2	Listagem de eventos de segurança incluindo malware, botnet e outras ameaças e riscos, permitindo a filtragem por cliente, domínio, IP de cliente e risco e ameaça do domínio;	OBRIGATÓRIO	
2.15.3	Listagem dos serviços agrupados por domínio, permitindo a filtragem pelo serviço, cliente e a categoria;	OBRIGATÓRIO	
2.15.4	Listagem do volume de requisições, indicando permissão ou bloqueio, permitindo filtragem por cliente;	OBRIGATÓRIO	
2.15.5	Gráfico do volume total, permitindo filtragem por cliente;	OBRIGATÓRIO	
2.15.6	Listagem dos domínios mais resolvidos, permitindo filtragem por cliente, permissão ou bloqueio, domínio, categoria e riscos e ameaça do domínio;	OBRIGATÓRIO	
2.15.7	Listagem das categorias mais resolvidas, permitindo filtragem por cliente, permissão ou bloqueio;	OBRIGATÓRIO	
2.15.8	Listagem dos clientes que mais fazem requisições de resolução, permitindo filtragem por cliente, categoria e riscos e ameaça do domínio;	OBRIGATÓRIO	
2.15.9	Relatório executivo gráfico com o resumo das ameaças bloqueadas, eventos de segurança mais recorrentes e serviços mais acessados;	OBRIGATÓRIO	
2.15.10	Entende-se por cliente qualquer origem da requisição de resolução de nomes, podendo ser um usuário, estação de trabalho, agente, IP público, rede com IP privado ou local, conforme configurações das funcionalidades de segurança	OBRIGATÓRIO	