DIRETORIA ADMINISTRATIVA E FINANCEIRA

GERÊNCIA DE SUPRIMENTOS E GESTÃO DE CONTRATOS

CONSULTA PÚBLICA Nº 2024/08

Objeto: Registro de preços para eventual aquisição de solução de segurança de Controle de Acesso à Rede (*Network Access Control* – NAC), com 5.000 (cinco mil) licenças para a funcionalidade de autenticação, autorização e gestão de contas temporárias; 1.000 (mil) licenças para a funcionalidade de classificação automática de dispositivos e 300 (trezentas) licenças para a funcionalidade de postura de admissão, com garantia, implementação e suporte técnico pelo período de 36 meses, prorrogável de forma sucessiva até o limite de 60 (sessenta) meses.

BB TECNOLOGIA E SERVIÇOS S.A.
GERÊNCIA DE SUPRIMENTOS E GESTÃO DE CONTRATOS
Consulta Pública

A BB TECNOLOGIA E SERVIÇOS S.A., por intermédio da Diretoria Administrativa e Financeira / Gerência de Suprimentos e Gestão de Contratos, torna pública a realização da Consulta Pública, na forma abaixo e de acordo com o Regulamento de Licitações e Contratos da BB Tecnologia e Serviços S.A., publicado em sua página eletrônica (www.bbts.com.br) em 01.02.2018 e os termos deste Edital, cuja minuta padrão foi aprovada pelo Parecer Jurídico nº º 2022/1206 de 23.02.2022.

1. Consulta Pública

1.1. A BB TECNOLOGIA E SERVIÇOS S.A. buscando identificar possíveis alternativas para aquisição de solução de segurança de Controle de Acesso à Rede (*Network Access Control* – NAC), com 5.000 (cinco mil) licenças para a funcionalidade de autenticação, autorização e gestão de contas temporárias; 1.000 (mil) licenças para a funcionalidade de classificação automática de dispositivos e 300 (trezentas) licenças para a funcionalidade de postura de admissão, com garantia, implementação e suporte técnico pelo período de 36 meses, informa que promoverá Consulta Pública, durante a qual serão tratados eventuais questionamentos e/ou solicitações de esclarecimentos decorrentes das informações constantes no Anexo 1.

1.2. Ressaltamos tratar-se de procedimento preliminar, cujo objetivo é o refinamento e ajustes na especificação da solução desejada, objetivando afastar eventuais inconsistências, bem como exigências incompatíveis com o objeto em questão, e a prospecção de soluções que atendam às necessidades da BBTS.

1.3. A BB TECNOLOGIA E SERVIÇOS S.A. se reserva o direito de, por ocasião da instauração do respectivo certame licitatório, independente das respostas e/ou argumentos porventura apresentados e motivada por razões de natureza técnica ou estratégica, alterar as especificações técnicas e demais condições objeto desta Consulta.

1.4. Eventuais respostas a esta Consulta Pública não constituirão uma oferta ou compromisso para contratar com a BB TECNOLOGIA E SERVIÇOS S.A. Os fornecedores que não participarem desta deste procedimento não estarão excluídos de um futuro processo licitatório.

1.5. A aceitação de uma proposta não compromete a BB Tecnologia e Serviços S. A. com a adjudicação de um contrato com qualquer fornecedor, mesmo que todos os requisitos estabelecidos nesta Consulta sejam cumpridos, nem limita o direito de negociar em nosso interesse.

1.6. O fornecedor não deve cobrar qualquer valor, mesmo que a título de compensação de despesas, pela submissão de respostas, demonstrações, discussões ou por qualquer outro motivo decorrente desta Consulta. O fornecedor é responsável por todo e qualquer custo ou despesa decorrentes do cumprimento desta Consulta.

1.7. A BB TECNOLOGIA E SERVIÇOS S.A. não assumirá o compromisso de acatar as sugestões apresentadas.

2. Confidencialidade

2.1. Fornecedores, seus empregados e representantes, sem prévio consentimento por escrito, não poderão:

a) Fazer declarações, anúncios, divulgações ou qualquer publicidade envolvendo o uso do nome, abreviaturas e símbolos relacionados a BB Tecnologia e Serviços S.A.;

b) Divulgar direta ou indiretamente que qualquer produto do fornecedor ou das empresas que representa foi aprovado, homologado ou endossado pela BB Tecnologia e Serviços S.A.;

c) Referir-se à existência desta Consulta em *press releases*, avisos ou em qualquer material publicitário distribuído ao público.

3. Cronograma

Etapa	Data
Recebimento de dúvidas	até 18h do dia 02/02/2024
Esclarecimentos de dúvidas	até 18h do dia 09/02/2024
Recebimento de propostas	até 18h do dia 21/02/2024

4. Contato

4.1. Toda comunicação sobre este processo da Consulta Pública, inclusive o encaminhamento propostas, de eventuais questionamentos e/ ou solicitações de esclarecimentos citados no item 2, deverão ser realizadas pelo e-mail: licitacoes@bbts.com.br.

4.2. As mensagens deverão conter o número desta Consulta Pública, a identificação da empresa, o nome do responsável e telefone para contato. Os esclarecimentos às dúvidas serão divulgados por esta mesma via e publicados no site www.bbts.com.br.

Brasília, 26 de janeiro de 2024

Italo Augusto Dias de Souza

Assinado de forma digital por Italo Augusto Dias de Souza
Dados: 2024.01.26 19:17:12 -03'00'

ÍTALO AUGUSTO DIAS DE SOUZA
Autoridade Competente

ANEXO 1

ESPECIFICAÇÕES TÉCNICAS

1. Objeto: Registro de preços para eventual aquisição de solução de segurança de Controle de Acesso à Rede (*Network Access Control* – NAC), com 5.000 (cinco mil) licenças para a funcionalidade de autenticação, autorização e gestão de contas temporárias; 1.000 (mil) licenças para a funcionalidade de classificação automática de dispositivos e 300 (trezentas) licenças para a funcionalidade de postura de admissão, com garantia, implementação e suporte técnico pelo período de 36 meses, prorrogável de forma sucessiva até o limite de 60 (sessenta) meses.

2. Especificações técnicas:

2.1. A solução deve atender a todas as funcionalidades exigidas nesse descritivo técnico, atendendo as seguintes funcionalidades para o quantitativo apresentado:

2.2. 5.000 (cinco mil) licenças para a funcionalidade de Autenticação, Autorização e Gestão de contas temporárias;

2.3. 1.000 (mil) licenças para a funcionalidade de Classificação automática de dispositivos.

2.4. 300 (trezentas) licenças para a funcionalidade de Postura de Admissão. Todos os serviços necessários para funcionamento da solução devem estar inclusos no licenciamento.

2.5. O licenciamento deve ser do tipo perpétuo.

2.6. O licenciamento deve-se realizar de forma global. Todos os appliances/softwares consomem licenças de um servidor centralizado.

2.7. A licença será contabilizada por dispositivo conectado, independentemente do modo de acesso. Exemplo: Guest, Suplicante 802.1x, MAC etc.

2.8. Os servidores deveram ser do formato Appliance Virtual, este deve ser projetado especificamente para a tarefa que compõem as atividades técnicas relativas a serviços de NAC.

2.9. Os acessos administrativos devem ser autenticados e criptografados.

2.10. A garantia, implementação e suporte técnico devem ser de total cobertura do fornecedor; atendendo as exigências da descrição técnica.

3. Servidor da Solução de NAC

3.1 A solução deve ser fornecida em *appliance* virtual compatível com VMWARE ESXI 7.0 ou superior.

3.2 A solução deve suportar mecanismo de alta disponibilidade para as funções de administração e monitoração;

3.3 A solução deve suportar mecanismo de redundância para as funções de autenticação;

3.4 A solução deve suportar arquitetura distribuída de seus serviços;

3.5 A solução deve permitir a instalação de servidores de gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover;

3.6 A solução deve permitir escalabilidade horizontal, ou seja, suportar a inclusão de novos dispositivos com a simples adição de novos appliances virtuais, sem causarem impacto na disponibilidade da solução.

3.7 A solução deve possuir recursos nativos para a replicação do banco de dados entre os servidores de gerenciamento;

3.8 A solução deve suportar os serviços de autenticação para até 3.000 usuários simultâneos em único appliance dedicado para autenticação e serviços;

3.9 A solução deve ser dimensionada para suportar no mínimo 10.000 diferentes endpoints em uma mesma implementação;

3.10 A solução deve possuir recursos para a criação e agendamento periódicos de backups da base de dados.

3.11 A solução deve permitir exportar o backup, através de atividade manual e programada via agendamento de tarefas

3.12 A solução deve permitir atualização remota da versão do software agente instalado, quando houver, quando a ferramenta for atualizada ou quando o usuário se conectar à rede.

3.13 As atualizações das configurações deverão ser realizadas sem a utilização de login scripts, agendamentos, tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução.

3.14 A solução deve integrar com softwares de SIEM e com os softwares de Análise de Vulnerabilidades, atendendo, no mínimo, uma das seguintes *Request for Comments* - RFCs: RFC 3164, RFC 5424 ou RFC 5426.

3.15 Em caso de contingência operacional (caso algum dos componentes centrais da solução venha a falhar), a parte restante da solução deve assumir o processamento do(s) componente(s) afetado(s) em 100% (cem por cento) sem perda de desempenho.

3.16 A solução deve permitir o sincronismo de tempo via NTP (*Network Time Protocol*).

4. Gerenciamento e Administração

4.1 A solução deve ser administrável remotamente por meio de interface gráfica (GUI) e/ou console de gerenciamento, utilizando canais autenticados e criptografados.

4.2 A solução deve conter mecanismo de comunicação em tempo real entre servidor e clientes, para entrega de configurações e políticas.

4.3 A solução deve admitir integração com MS-AD (Microsoft Active Diretor) para um único login do usuário (Single Sign On = SSO)

4.4 A solução deve possuir integração com LDAP e Open LDAP, para a importação da estrutura organizacional.

4.5 A solução deve aplicar regras diferenciadas baseando em diferentes topologias e segmentação lógica da rede.

4.6 A solução deve aplicar regras diferenciadas por grupos de usuários e máquinas.

4.7 Possuir contas administrativas que permitam a segregação de funções de monitoramento e administração.

4.8 A solução deve ter capacidade de segregação de perfis de acesso, permitindo diferentes níveis de acesso à console de gerenciamento, onde cada perfil possa ter permissões específicas associadas à sua função.

4.9 Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

4.10 Possuir interface para construção de regras customizadas de classificação de dispositivo com suporte a operadores lógicos.

4.11 Possuir uma base de regras e categorias pré-configuradas.

4.12 Permitir gerenciar, configurar e alterar regras e políticas através de interface gráfica web.

4.13 Possuir Dashboard para rápida visualização das informações sumarizadas com métricas das últimas 24 horas:

a) Número de dispositivos ativos
b) Número de visitantes ativos
c) Tempo médio para remediar os dispositivos
d) Porcentagem dos dispositivos em conformidade
e) Número de dispositivos descobertos

4.14 Deve disponibilizar informações de performance, CPU, Memória de cada componente da solução.

4.15 Deve disponibilizar o total de falhas de autenticação das últimas 24 horas e a principal razão.

4.16 Deve possuir tela de monitoração contínua das autenticações em tempo real com visualização imediata das seguintes informações:

a) Data e horário;
b) Link com os detalhes avançados da autenticação;
c) Status da autenticação;
d) Nome do usuário/dispositivo;
e) Endereço MAC;
f) Endereço IP;
g) NAD;
h) Interface;
i) Perfil de Autorização concedido;
j) Resultado da classificação do dispositivo – Categoria;
k) Status de Postura, conformidade;
l) Razão em caso de falha;
m) Protocolo de autenticação

4.17 Deve ser capaz de gerar relatórios com as informações referentes ao resultado da verificação da postura da máquina;

4.18 Toda a comunicação entre o dispositivo de gerenciamento de políticas e o dispositivo gerenciado deve ser criptografada através da utilização do SSL (Secure Socket Layer);

5. Autenticação

5.1 Deve Suportar protocolos EAP (autenticação extensível), PAP (autenticação de senha) e CHAP (autenticação de handshake de desafio);

5.2 A solução deve implementar autenticação de dispositivos e usuários utilizando o padrão IEEE802.1X suportando pelo menos os seguintes métodos EAP, EAP-TLS, TEAP

5.3 Deve permitir a autenticação dos usuários/dispositivos nas seguintes bases de dados:

a) Local do tipo usuário;
b) Local do tipo dispositivo;

c) Externa via RADIUS;

d) Externa via LDAP;

e) Externa via Windows Active Directory;

f) Certificado Digital;

5.4 A solução deve permitir a integração com a base de usuários do AD (Active Directory) para login único do usuário (Sign Sign On). As credenciais do usuário utilizadas no momento de autenticação do Windows deverão ser utilizadas na autenticação do usuário na solução de controle de acesso de forma automática sem que o usuário tenha que entrar com as credenciais novamente;

5.5 A solução deve oferecer autenticação de usuários através de portal web seguro HTTPS com redirecionamento automático;

5.6 A solução deve implementar autenticação específica para dispositivos do tipo *MAC Address* conforme método MAB (Mac Authentication Bypass);

5.7 A solução deve possuir uma base de dados interna para registro de dispositivos do tipo *MAC Address* podendo esta base ser preenchida automaticamente pelo mecanismo de descoberta automático de dispositivo;

5.8 A solução deve implementar validação de certificados digitais atendendo as seguintes caraterísticas.

a) Suportar o cadastramento de pelo menos duas CA (Certificate Authority) externos;

b) Suportar consulta periódica da lista de revogados CRL (Certificate Revogation List) via HTTP;

c) Suportar o protocolo OCSP para verificação do estado do certificado;

5.9 A solução deve implementar mecanismo flexível de regras que permita selecionar a base de dados onde será autenticado o usuário/dispositivos com base nos atributos RADIUS existentes na solicitação enviada pelo NAD (Network Access Device) e tipo de protocolo permitindo pelo menos a seguinte combinação de regras.

5.10 Deve prover servidor Radius com suporte aos métodos EAP.

5.11 Deve implementar autenticação Radius baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes;

5.12 Deve implementar Radius CoA Proxy.

5.13 Deve implementar base de dados interna centralizada para registro dos endereços MAC dos dispositivos que serão autenticados por esta funcionalidade.

5.14 Deve permitir a carga de um arquivo contendo uma lista de endereços MAC permitidos a partir de um único ponto de cadastramento.

5.15 Deve identificar dispositivos de redes que não são capazes de realizar autenticação, como catracas, câmeras de vigilância, detectores de fumaça, impressoras etc. 2de criar políticas de acesso a rede para esses dispositivos através do endereço MAC da interface de rede.

5.16 O servidor deve conter mecanismo de comunicação em tempo de terminado pelo administrador entre o cliente e servidor, para consulta de novas configurações e políticas.

5.17 Deve suportar redirecionamentos dos logs para um servidor de Syslog da CONTRATANTE.

5.18 Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado.

5.19 Deve permitir interoperabilidade com mínimo 3 fabricantes de tecnologia MDM (Mobile Device Management) do mercado.

5.20 Deve suportar implementar validação de certificados digitais atendendo as seguintes caraterísticas:

a) Deve suportar o cadastramento de CA (Certificate Authority) externos;

b) Deve suportar consulta periódica da lista de revogados CRL (Certificate Revogation List) via HTTP;

5.21 Deve suportar o protocolo OCSP (Online Certificate Status Protocol) para verificação do estado do certificado;

5.22 A solução deve integrar de forma transparente com os dispositivos de segurança, switches, roteadores e pontos de acesso wireless, no mínimo, dos seguintes fabricantes: Cisco, Huawei, HPE, Juniper.

6. Autorização

6.1 A solução deve possuir as funcionalidades de:

6.1.1 Implementar atribuição de VLAN;

6.1.2 Implementar atribuição de ACL do tipo Downloadable no mínimo nos seguintes protocolos TCP, ICMP, IP;

6.1.3 Implementar atribuição de ACL do tipo named;

6.1.4 Implementar atribuição de ACL do tipo “filter-id”;

6.1.5 Implementar atribuição de ACL do tipo Redirecionamento Web;

6.1.6 Implementar atribuição de TAG de segurança “SGT” conforme descrito no padrão IEEE802.1AE;

6.1.7 Implementar atribuição de política MacSec conforme padrão IEEE802.1AE;

6.1.8 Implementar atribuição do domínio de voz para telefones IP (Voice Domain);

6.1.9 Implementar atribuição do parâmetro de re-autenticação 802.1X;

6.1.10 Implementar atribuição do parâmetro “SmartPort”;

6.1.11 Permitir a customização de atributos de autorização;

6.1.12 Permitir a criação de perfis de usuários;

6.2 Deve permitir autorização de acesso condicional com base nos seguintes fatores:

a) Atributos LDAP do usuário autenticado;

b) Grupo de Active Directory do usuário autenticado;

c) Conteúdo do certificado digital (CN, OU);

d) Horário de conexão;

e) Localização;

6.3 Deve Implementar o protocolo RADIUS Change of Authorization (CoA);

7. Gestão de contas temporárias – Visitantes/Consultores

7.1 O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo (internet);

7.2 Deve implementar um portal web seguro SSL para criação de contas temporárias do tipo “visitante” com autenticação de autorizadores em base externa do tipo Active Directory, LDAP, e adicionar base local (podemos criar localmente) e atribuição de privilégio ao autorizador de acordo com seu perfil;

7.3 Deve realizar a autenticação dos autorizadores em base externa do tipo Open LDAP e atribuir o privilégio ao autorizador de acordo com perfil do usuário;

7.4 Deve permitir que as contas de usuários visitantes sejam gerenciadas internamente pela solução, não havendo necessidade de integração com o Open LDAP da CONTRATANTE;

7.5 Deve permitir a criação de perfil de contas temporárias podendo atribuir privilégio de acesso a rede distintos atendendo no mínimo os seguintes privilégios:

a) Perfil Visitante – Somente acesso HTTP/HTTPS para Internet;

b) Perfil Consultor – Somente acesso HTTP/HTTPS para Internet e Intranet;

7.6 Deve permitir a criação de “Periodicidade” declarando:

a) A conta temporária tem validade de X dia a partir de sua criação;

c) A conta temporária tem validade de X dia a partir do primeiro login;

e) O autorizador determinará o início e fim de cada conta de acordo com seu privilégio de autorizador;

f) Deve permitir a criação de perfis de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

7.7 Deve permitir a criação de perfis de acesso para as credenciais temporárias com diferentes privilégios de acesso à rede;

7.8 Deve permitir a criação de grupos de autorizadores com privilégios distintos de criação de contas temporárias especificando os seguintes privilégios por grupo:

a) Criar conta individual;

b) Criar contas aleatórias;

c) Importar contas de arquivo .csv;

d) Enviar credencial via Email;

e) Enviar credencial via SMS;

f) Ver a senha da conta de visitante;

g) Imprimir detalhes da conta visitante;

h) Ver e editar as contas criadas por todos os grupos de autorizadores;

i) Ver e editar as contas criadas pelo mesmo grupo de autorizadores;

j) Ver e editar as contas criadas pelo próprio autorizador;

k) Suspender contas criadas por todos os grupos de autorizadores;

l) Suspender contas criadas pelo mesmo grupo de autorizadores;

m) Duração máxima da conta visitante;

n) Especificar o Perfil de acesso a rede que será atribuído a conta visitante;

o) Especificar o Perfil de Tempo que será atribuído ao visitante;

7.9 Deve permitir a customização do formulário de criação de contas temporárias a ser preenchido pelo autorizador especificando quais campos são obrigatórios e quais campos são opcionais bem como permitir a criação de novos campos:

a) Nome;

b) Sobrenome;

c) Email;

d) Empresa;

e) Campo Customizado;

7.10 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

7.11 Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias;

7.12 Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres, quantos caracteres especiais e quantos números serão utilizados para compor a senha temporária;

7.13 Deve implementar um portal web seguro SSL a ser apresentado automaticamente aos usuários temporários (visitante/consultor) durante a sua conexão com a rede (hotspot);

7.14 Deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes.

7.15 Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através do portal web, sem a necessidade de um autorizador;

7.16 Deve implementar as seguintes funções no Portal Web (hotspot):

a) Permitir a troca de senha do usuário visitante diretamente pelo portal seguro;

b) Deve permitir configurar o número máximo de dias decorridos antes de exigir a troca da senha do usuário visitante;

c) Determinar o número máximo de erros de login antes de bloquear a conta;

d) Deve permitir configurar o número máximo de erros de login antes de bloquear a conta do usuário visitante;

e) Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;

f) Exigir somente no primeiro login o aceito do “Termo de uso aceitável de rede”;

g) Customização da página de “Termo de uso aceitável de rede”;

7.17 Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email ou impressão local;

8. Classificação automática de dispositivos

8.1 Deve implementar funcionalidades de Classificação Automática de Dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso;

8.2 Deve permitir a atualização das categorias de Classificação de Dispositivos, pelo fabricante;

8.3 Deve permitir que o administrador cadastre manualmente um determinado dispositivo em uma categoria.

8.4 Deve possuir base de regras e categorias de dispositivos pré-configurada;

8.5 Deve suportar mecanismo de atualização das regras e categorias pré configuradas

8.6 Deve implementar mecanismo de descobrimento automático e transparente de dispositivos que se conectam a rede wireless e wired classificando-os nas seguintes categorias:

a) Tablet
b) Impressora
c) Telefone IP
d) Workstation

8.7 Deve implementar os seguintes mecanismos para coleta de informações do dispositivo a ser utilizada na construção das regras de classificação.

a) Coleta do tráfego DHCP e HTTP enviado pelo dispositivo;
b) Coleta dos atributos RADIUS referente a sessão 802.1X do dispositivo;
c) Consulta SNMP ao switch de acesso ou controlador wireless;
d) Consulta DNS para resolução de nome;
e) Iniciar checagem de portas tcp contra o dispositivo “PortScan”;

8.8 Deve possuir interface para construção de regras customizadas de classificação de dispositivo com suporte a operadores lógicos;

8.9 Deve permitir a criação de regras e categorias customizadas;

8.10 Deve possuir uma base de regras e categorias pré-configuradas;

8.11 Deve suportar mecanismo de atualização das regras e categorias pré-configuradas;

8.12 Deve permitir que a classificação do dispositivo descoberto seja utilizada como parâmetro de autorização nas regras de admissão de dispositivos;

8.13 Deve permitir que o administrador cadastre manualmente um determinado dispositivo numa categoria;

8.14 Deve permitir a criação de regras para diferenciação de dispositivos corporativos e pessoais, possibilitando a adoção de políticas de “BYOD (Bring Your Own Device)”;

9. Postura de Admissão

9.1 Deve permitir bloquear a comunicação ponto a ponto entre máquinas que estiverem em conformidade (postura) com as políticas de controle de acesso à rede e máquinas que não estiverem em conformidade com as políticas do controle de acesso à rede;

9.2 Deve implementar funcionalidades de avaliação de postura de segurança (NAC/NAP) nos dispositivos clientes com sistema operacional Windows, Linux e MacOS;

9.3 A solução deve permitir a verificação da postura da estação de através das seguintes formas:

9.4 Agente Instalado: Agente a ser instalado na estação do usuário responsável para coleta das informações referentes a postura. O agente deve ser responsável somente pela verificação da postura da estação. Todo o controle de nível de acesso à rede, controle de tempo concedido e controle de banda deverão ser feitos através do Dispositivo de Aplicação de Políticas;

9.5 Agente Temporário (Java ou ActiveX): Agente web a ser carregando na estação no momento de verificação da postura para coleta das informações referentes a postura. O agente deve ser responsável somente pela verificação da postura da estação. Todo o controle de nível de acesso à rede, controle de tempo concedido e controle de banda deverão ser feitos através do Dispositivo de Aplicação de Políticas;

9.6 A solução deve implementar o bloqueio de acesso à rede, das máquinas que não estiverem em conformidade com as políticas do controle de acesso.

9.7 Deve permitir a avaliação de postura de segurança através de agente instalado permanente ou agente temporário;

9.8 A solução deve efetuar as verificações de conformidade das máquinas que acessem a rede corporativa de forma a permitir, bloquear ou redirecionar as conexões de acordo com as políticas de segurança implementadas.

9.9 A solução deve tomar ações como ativar ou desativar a porta do switch e trocar de VLAN após identificar uma inconformidade com a política de segurança no(s) host(s) da rede coorporativa;

9.10 O Agente (Instalado ou Temporário) deve permitir a verificação dos seguintes itens:

9.11 Sistema Operacional Instalado;

9.12 Verificação do Service Pack Instalado;

9.13 Chaves do Registro do Windows;

9.14 Arquivos existentes na estação do usuário;

9.15 Status dos serviços que estão rodando na máquina;

9.16 Existência de Software Antivírus e AntiSpyware Instalado;

9.17 Data da última atualização do Antivírus;

9.18 Status do software Antivírus (Habilitado ou Desabilitado) ;

9.19 Verificação do Hotfix do Windows Instalado

9.20 Os agentes devem permitir a verificação dos seguintes itens: atualizações do sistema operacional, estado e atualizações dos softwares de firewall, anti-virus, anti-spyware;

9.21 A solução deve permitir a verificação da última versão de antivírus fornecida. A solução deve ser capaz de verificar qual é a última assinatura disponível e a sua respectiva data.

9.22 A solução deve a possuir base de dados atualizada periodicamente com as informações de assinaturas de antivírus, Antispyware e Hotfixes de sistemas operacionais;

9.23 Deve implementar relatórios com as informações referentes aos resultados da verificação de postura dos dispositivos clientes;

9.24 Deve efetuar as verificações de conformidade(postura) dos dispositivos que acessem a rede corporativa de forma a permitir, bloquear ou redirecionar as conexões de acordo com as políticas de segurança implementadas;

9.25 A solução deve permitir a entrega de agente temporário para checagem de conformidade de máquinas não gerenciadas ou de terceiros que acessem a rede;

9.26 A solução deve permitir herança de políticas nos grupos.

9.27 A solução deve permitir a configuração de políticas distintas para usuários “on-line” (quando o usuário está dentro e/ou comunicando-se remotamente com a rede coorporativa) e “offline” (quando o usuário está fora e/ou desconectado da rede corporativa);

9.28 Deve permitir o controle do acesso de usuários que se conectem na rede corporativa interna via LAN, WLAN e VPN;

9.29 Deve implementar funcionalidades de Classificação Automática de Dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso;

9.30 Deve implementar autenticação via portal web para os usuários da rede wireless que não puderem se autenticar via 802.1X. Utilizar os recursos do padrão IEEE 802.1x, compatíveis com esse padrão, de forma integrada, por intermédio de um appliance que realize validação/autenticação em conformidade com o referido padrão em redes locais – LAN;

9.31 Deve auditar periodicamente, em intervalos de tempo definidos pelo administrador, se o computador possui antivírus, firewall, antispyware e patches instalados, ativos e atualizados.

9.32 Deve iniciar a auto-remediação do computador que falhou a auditoria, ou seja, corrigir os pontos nos quais a verificação especificada pelo administrador falhou.

10. Isolamento e Quarentena

10.1 O isolamento e Quarentena dos usuários deverão ser feitos através do dispositivo de aplicação de políticas. Não serão aceitas soluções onde o controle esteja baseado em a gente ou manipulação do endereço via DHCP.

10.2 Deve permitir o isolamento das estações mesmo que não possua agente instalado.

10.3 Deve permitir o Isolamento das estações mesmo que tenha endereço IP estático configurado;

10.4 Deve implementar mecanismo de isolamento ou quarentena dos dispositivos que estiverem em desacordo com as políticas de segurança;

11. Remediação

11.1 Caso o usuário não esteja de acordo com os requisitos de segurança da estação a solução deve prover mecanismos de atualização das seguintes formas:

11.2 Manual: O agente instalado deve guiar o usuário no processo de atualização da estação (provendo links para os patches, atualização) a fim de que a estação fique de acordo com as políticas de segurança;

11.3 Automático: O agente instalado deve realizar todo o processo de forma automática;

11.4 Deve suportar a configuração das seguintes formas de remediação:

a) Distribuição de Link Web;

c) Integração comSystemcenter e Wsus;

d) Integração com Antivírus e Antipyware;

Deve prover integração com o servidor SystemCenter e WSUS para instalação de patches de segurança Windows

12. Relatórios e Monitoramento

12.1 A solução deve oferecer alertas na console de gerência e enviar via SMTP/e-mail.

12.2 A solução deve possibilitar aos administradores do sistema a geração de relatórios customizados exportáveis nos formatos PDF, CSV e/ou TXT.

12.3 A solução deve fornecer funcionalidades de relatórios gráficos, com as seguintes informações:

a. Tipos de dispositivos;

b. FABRICANTE do dispositivo;

c. Sistema Operacional;

d. Endereço IP associado;

e. Informação detalhada dos usuários;

f. políticas em uso;

g Regras de Controle de Acesso.

12.4 A interface gráfica da solução deve prover as informações em tempo real.

12.5 A solução deve gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de logs devem conter a identificação do evento, data e hora, identificação do usuário e endereço IP do dispositivo.

12.6 A solução deve ser capaz de gerar e armazenar registros de logs com informações sobre falhas e erros ocorridos na console de gerenciamento, nos dispositivos e nos portais de autosserviço.

12.7 Centralizar os logs dos componentes da solução em um único ponto, ou permitir a exportação dos logs via syslog.

12.8 Possuir ferramenta para acompanhamento de eventos e estatística de logs.

12.9 Os acessos à administração e configuração, bem como as alterações realizadas durante o acesso, devem ser registrados em log, informando no mínimo: hora, data, IP de origem e usuário.

12.10 A solução deve permitir escalabilidade horizontal, ou seja, suportar a inclusão de novos dispositivos com a simples adição de novos Appliances Virtuais na infraestrutura tecnológica da rede corporativa.

13. Subcontratação:

13.1 Não será admitida a subcontratação total ou parcial do objeto do contrato.

14. Condições de Entrega:

14.1 A entrega das licenças de software deverá ser realizada em até 5 (cinco) dias úteis contados a partir do início da vigência do contrato, em horário comercial, mediante prévio entendimento e alinhamento com o Fiscal do serviço da BB Tecnologia e Serviços;

14.2 Durante a fase de implementação, a Contratada deverá realizar a passagem de conhecimento.

14.3 Todo o trâmite de entrega das licenças deve ser alinhado com o Fiscal do serviço e formalizado através do e-mail: ceris@bbts.com.br

14.4 Os ativos e softwares deverão ser entregues na BB TECNOLOGIA E SERVIÇOS no endereço: SEPN - Setor de Edifícios de Utilidade Norte - Quadra 508 Conjunto "C" Lote 07, Primeiro Subsolo - Asa Norte - CEP 70740-543

14.5 Os detalhes de aceite dos ativos e softwares estão previstos no item “Condições de Aceite”;

15. Informações de Faturamento:

- CNPJ de faturamento: 42.318.949/0013-18
- Endereço de faturamento: SEPN QD 508 CONJUNTO C LOTE, 07 - ASA NORTE, BRASÍLIA
- Inscrição Estadual: 0732200700203
- Inscrição Municipal: 0732200700203

16. Condições de Instalação, Implementação e/ou Customização:

16.1 Para a execução dos serviços de instalação, implementação e configuração, a CONTRATADA deverá alocar profissionais devidamente capacitados pelo respectivo fabricante da solução fornecida.

16.2 Os serviços de instalação, implementação e configuração deverão ser precedidos do efetivo levantamento do ambiente, documentação e planejamento detalhado, incluindo rollback e plano de contingência, submetidos à aprovação da CONTRATANTE.

16.3 A CONTRATADA deverá instalar, implementar e configurar a solução remotamente ou presencialmente.

16.4 Os produtos fornecidos, conforme projeto de implantação elaborado pela CONTRATADA e aprovado pela equipe técnica da CONTRATANTE, deverá apresentar documentação contendo as instruções passo-a-passo para a sua implementação.

16.5 Os produtos fornecidos serão instalados e configurados em conformidade com o padrão da Rede IP Multisserviços da CONTRATANTE.

16.6 A CONTRATADA deverá instalar, configurar os produtos fornecidos para permitir seu funcionamento nos Data Centers da CONTRATANTE. Estas ações deverão contemplar no mínimo, as seguintes atividades:

16.7 Análise preliminar da topologia e operação atual da rede IP Multisserviços da CONTRATANTE com vistas a seu aproveitamento na solução ofertada.

16.8 Completa instalação e configuração, e ajustes de toda a solução ofertada.

16.9 Implementação, com a coleta de evidências, dos controles de requisitos de segurança da CONTRATANTE, que forem possíveis de serem aplicados nos produtos fornecidos, componentes da solução contratada.

16.10 Acompanhamento e homologação do ambiente de produção.

16.11 Documentação detalhada de todos os passos da instalação, configuração e ajustes, no ambiente de produção, a qual deverá ser entregue em arquivo eletrônico no formato PDF, antes da emissão do termo de aceite técnico a ser expedido pela CONTRATANTE.

16.12 A critério da CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para a

CONTRATANTE, visando minimizar os transtornos aos usuários pela eventual indisponibilidade da rede.

16.13 A critério da CONTRATANTE, seguindo as recomendações do fabricante da solução, a integração com os controladores de domínio da BBTS poderá utilizar ADFS ou SSO, ou outra recomendada, tendo em vista a realização de monitoramento em tempo real para políticas de bloqueio da atividade, da conta ou duplo fator de autenticação.

16.14 Os trabalhos serão coordenados e acompanhados pelos analistas e técnicos da CONTRATANTE, devendo haver repasse de conhecimento durante a execução dos serviços.

16.15 A CONTRATADA deverá dispor de um profissional com o papel de gerente de projetos para gerenciar todas as atividades do projeto, utilizando as boas práticas previstas no PMBOK 6ª edição ou posterior;

16.16 O gerente de projetos da CONTRATADA deverá orquestrar e estar presente nas reuniões obrigatórias;

16.17 O gerente de projetos deve buscar refinar o objetivo do projeto bem como traçar caminhos para alcançá-lo com o máximo de eficiência e eficácia possível;

16.18 São atividades previstas pelo gerente de projetos, porém não limitadas a elas:

16.19 Alinhar os objetivos, escopo e entregáveis do Projeto;

16.20 Definir a Matriz de Responsabilidades;

16.21 Elaborar cronograma que permita o acompanhamento da evolução do serviço;

16.22 Conduzir a definição do Plano de Comunicação;

16.23 Alinhar outras abordagens: como Premissas, Exclusões e Restrições;

16.24 Definir a periodicidade das reuniões obrigatórias e técnicas do Projeto;

16.25 Alocar os recursos envolvidos na implementação pela CONTRATADA;

16.26 Coordenar todas as estratégias desde o planejamento da migração até o encerramento do projeto.

16.27 O Encerramento do Projeto se dará com o aceite final pela BB Tecnologia e Serviços de acordo com as condições destas especificações técnicas;

16.28 A CONTRATADA deverá em até 05 (cinco) dias após a assinatura do Contrato, realizar o envio para o Fiscal de Serviços, da documentação no formato PDF, com a comprovação de que o(s) profissional(is) que atuarão na instalação dos produtos, previstos neste edital, possuam:

16.28.1 Vínculo do contrato social, ou registro na carteira profissional, ou ficha de empregado, ou contrato de trabalho, ou contrato de prestação de serviços com a CONTRATADA;

16.28.2 Possuam formação superior em ciência da computação, sistemas de informação, redes ou semelhante, desde que voltada para área de TI, através de envio em

formato .PDF dos respectivos certificados, declarações ou diplomas de conclusão emitido pela respectiva entidade de ensino legalmente reconhecida pelo MEC;

16.28.3 Possuam a certificação técnica do fabricante: Principais fabricantes de segurança cibernética

16.29 A CONTRATADA deverá manter todas as qualificações exigidas durante toda a duração do contrato.

16.30 Ao final do entregável será o documento Plano de Implantação da solução;

16.31 A CONTRATADA deverá garantir que as atividades de Implantação causem o mínimo de disrupção nos serviços da BBTS, estando a postos caso haja a necessidade de reversão (rollback);

16.32 Ao término da Implantação, a CONTRATADA deverá confeccionar a documentação que contenha detalhes dos componentes, conexões e configurações implementadas, além do resumo detalhado das atividades realizadas para refletir o desenho final executado para servir de base para a manutenção da solução Implementada;

16.33 Após o término da implementação a CONTRATADA deverá fornecer 01 (um) recurso como suporte consultivo remoto de até 05 (cinco) dias úteis, começando no próximo dia útil após a conclusão da implantação;

16.34 O entregável é o documento Desenho da Solução Implementada;

17. Condições de Aceite:

17.1 A BBTS irá realizar o aceite: após a entrega de ativos, softwares e a implantação da solução

17.2 A CONTRATADA deverá realizar a implementações em até 30 (trinta) dias corridos.

17.3 Caso a CONTRATADA não realize a entrega dentro do prazo estipulado, sem justificativa plausível, poderá ser aplicada multa conforme previsto.

17.4 A BBTS disporá de um período de até 30 (trinta) dias corridos para avaliação das quantidades, validação e correspondência aos itens discriminados no contrato;

17.5 Caso seja verificado que as especificações contratadas/pactuadas não atendem ou os ativos não estejam em perfeito funcionamento, poderá a BBTS rejeitá-los, integralmente ou em parte, obrigando-se a CONTRATADA a providenciar a substituição dos equipamentos não aceitos no prazo de até 30 (trinta) dias corridos;

17.6 Caso sejam satisfeitas todas as condições, a BBTS, por meio do Fiscal de Serviços, emitirá o respectivo “Aceite de Recebimento de ativos”, no prazo máximo de 10 (dez) dias úteis;

17.7 O aceite será realizado pelo Fiscal do Serviço através de e-mail com título “Aceite de Recebimento de Ativos – Contrato DGCO nº “XXXX”, a ser enviado para a CONTRATADA e contendo o texto: “A BB Tecnologia e Serviços (BBTS) confirma a entrega

e atesta o aceite do recebimento dos ativos e softwares referentes ao contrato DGCO nº "XXXX", com a empresa, de acordo com os quantitativos e especificações contratadas.";

17.8 A CONTRATADA deverá realizar a Implantação do objeto, em até 30 (trinta) dias corridos após o aceite de recebimento dos ativos e licenças;

17.9 O encerramento da migração é a condição para a BBTS atestar o término da implementação e se dará com o aceite final;

17.10 O aceite final será o resultado das avaliações técnicas sobre a migração em si, do aceite de entrega de todos os documentos (entregáveis), além do aceite da realização das sessões de passagem de conhecimento (validação de que todas as sessões foram realizadas);

17.11 Caso sejam satisfeitas todas as condições, a BBTS, por meio do Fiscal de Serviços, emitirá o respectivo "Aceite da Implementação", no prazo máximo de 20 (vinte) dias corridos após o recebimento dos entregáveis.

17.12 O aceite final será realizado pelo Fiscal do Serviço através de e-mail a ser enviado para a CONTRATADA.

17.13 Caso não sejam satisfeitas todas as condições, onde a CONTRATADA não cumpriu o prazo de até 30 (trinta) dias para a implementação, serão aplicadas as devidas multas de acordo com as

18. Condições de Garantia e Assistência Técnica, Manutenção e Suporte Técnico:

18.1 Todos os ativos e licenças deverão possuir garantia, por período de 36 (trinta e seis) meses, contada a partir da data da implementação, compreende atualização, manutenção e suporte técnico, que consiste em: Evolução/upgrade do produto, repassando à BBTS quaisquer atualização, melhoria ou correção introduzida nos produtos que componham a solução, bem como a catalogação de novas versões (*releases*), que contenham, além de outras, as funções dos produtos em questão.

18.2 Manutenção da solução, assim entendida a correção de erros de funcionamento ou desempenho inconsistente com as especificações técnicas dos produtos.

18.3 Atuação na resolução de problemas de atualização da solução, upgrade, salvamento e restauração.

18.4 Fornecimento de qualquer informação relativa ao funcionamento da solução, dirimindo as dúvidas ou problemas operacionais na sua utilização.

18.5 Assegurar a total disponibilidade e manter a solução em perfeitas condições de uso.

18.6 Em caso de alteração de versão de quaisquer softwares fornecidos na solução integrada que implique em deformação ou inabilitação das funcionalidades, o proponente

executará as alterações necessárias ao atendimento dos requisitos descritos neste documento, sem qualquer custo adicional para o Banco do Brasil.

18.7 A BBTS se reserva no direito de efetuar conexão da solução a produtos de outros fornecedores, seja hardware ou software, desde que tal iniciativa não implique incompatibilidade com a solução. A efetivação de tal medida não poderá, sob qualquer hipótese, servir como justificativa para desobrigação da prestação da garantia.

18.8 O proponente concederá à BBTS, durante o período de sua vigência, garantia integral “on-site” e/ou remoto, que deve contemplar o atendimento no formato 24x7x4, compreendendo resposta do fornecedor em até 04 (quatro) horas; disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias da semana, inclusive com atendimentos nos feriados, a contar da data da implementação, da solução, contra qualquer defeito que a solução venha a apresentar, mesmo após ocorrida sua aceitação/aprovação pelo Banco, observadas as condições a seguir:

18.9 A garantia “*on-site*” indicada no item anterior será acionada em casos que não forem possíveis a resolução de forma remota.

18.10 Deverá ser efetuada manutenção corretiva sempre que a solução apresentar falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado.

18.11 As manutenções corretivas serão de responsabilidade do proponente, sem custos adicionais à BBTS.

18.12 O proponente deve garantir à BBTS o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários, e efetuar downloads das atualizações do software, atualização de listas e informações de *threat intelligence* ou documentação do software que compõem a solução.

18.13 O proponente deverá fornecer quaisquer atualizações e/ou correções de software em até 48 (quarenta e oito) horas após sua disponibilidade no mercado, ficando a critério da BBTS a implantação da atualização.

19. Homologação:

19.1 Até 30 (trinta) dias após a entrega das licenças, conforme descrito abaixo:

19.2 Avaliação: BBTS em até 15 (quinze) dias corridos a partir da entrega;

19.3 Se correção: Contratada em 10 (dez) dias corridos a partir do indicativo BBTS;

19.4 Reavaliação: BBTS em 5 (cinco) dias corridos a partir do reenvio.

20. Condições de Pagamento:

20.1 O pagamento será creditado, conforme cronograma abaixo, após o aceite das licenças/serviço, em conta corrente mantida preferencialmente no Banco do Brasil S.A.,

em nome da CONTRATADA, em até 30 dias corridos, a contar da emissão da Nota fiscal de cada etapa, acompanhada do Documento Auxiliar da Nota Fiscal Eletrônica, relativo aos municípios em que o documento é exigido

ETAPA	DETALHAMENTO DO PAGAMENTO	PERCENTUAL
Etapa 01 - Entrega	Pagamento realizado após emissão do termo de aceite de entrega.	40%
Etapa 02 - Instação	Pagamento realizado após emissão do termo de aceite de instalação.	40%
Etapa 03 - Implantação	Pagamento realizado após emissão do termo de aceite de implantação.	20%
Etapa 04 - Garantia	Garantia 36 (trinta e seis) meses. Pagamento realizado após a emissão do termo de aceite de implantação.	100%

21. Multa:

21.1 Para efeito de aplicação de multas referentes ao descumprimento de obrigações contratuais, às infrações serão atribuídos graus, conforme as tabelas 1 e 2 a seguir:

TABELA 1	
GRAU	CORRESPONDÊNCIA
1	0,2% sobre o valor contratado
2	0,5% sobre o valor contratado

TABELA 2		
ITEM	DESCRIÇÃO DA OCORRÊNCIA	GRAU
1	Executar serviço incompleto ou de caráter paliativo, ou deixar de providenciar recomposição complementar; por ocorrência, cumulativamente não superior a 10%.	1
2	Deixar de disponibilizar condições necessárias à realização das implementações previstas no contrato; por ocorrência, cumulativamente não superior a 5%.	1
3	Deixar de cumprir prazos de entregas individuais, de implementação ou entrega dos documentos referenciados no item 16.3.2, sem justificativa aceitável, cumulativamente não superior a 10%.	1
4	Deixar de cumprir prazos de entrega dos documentos do item 17.10, em sua totalidade, sem justificativa aceitável, até o término do prazo previsto no item 17. (Condições de aceite).	2
5	Deixar de cumprir prazo de entrega dos ativos e softwares, sem justificativa aceitável, dentro do prazo previsto no item 14 (Condições de	2

	entrega).	
6	Deixar de entregar os ativos e softwares com especificação em conformidade, ou em mal funcionamento, sem justificativa aceitável, dentro dos prazos previstos no item 17 (Condições de aceite).	2
7	Deixar de cumprir prazo de conclusão de implementação, prevista no item 17 (Condições de aceite).	2

22. Acordo de Nível de Serviço:

22.1 A prestação dos serviços de suporte técnico, manutenção e atualização deverá compreender, no mínimo, as seguintes atividades:

22.2 O atendimento ao chamado expresso da CONTRATANTE, visando o restabelecimento do funcionamento da solução de software contratada, quando da ocorrência de quaisquer falhas ou problemas de ordem técnica;

22.3 Correções de problemas relatados pela CONTRATANTE (manutenção corretiva) e correções de problemas realizadas pela CONTRATADA (manutenções evolutivas);

22.4 Serviço de esclarecimento de dúvidas relativas à utilização, configuração e parametrização das soluções objeto desta contratação;

Severidade	Escopo
1	Um problema que tenha um impacto crítico na capacidade da CONTRATANTE em manter sua SOLUÇÃO ativa. Um número significativo de usuários do sistema e/ou da rede é incapaz de executar adequadamente as suas tarefas: **IMPACTO ALTISSIMO** – solução inoperante ou severamente degradada.
2	Um problema que tenha um impacto na capacidade da CONTRATANTE em manter sua SOLUÇÃO ativa, cuja severidade seja significativa, porém não crítica, e que possa ser de natureza repetitiva. O funcionamento do sistema, da rede ou do produto é afetado, mas o desempenho não foi severamente degradado. **IMPACTO ALTO** - que possivelmente coloque em risco um ambiente de produção - a solução continua operante, mas apresenta graves restrições.
3	Um problema que não cause impacto na capacidade da CONTRATANTE em manter sua SOLUÇÃO ativa. **IMPACTO BAIXO** – problemas ou dúvidas que criem restrições à operação da solução.
4	Um problema que **NÃO CAUSE IMPACTO** na capacidade da CONTRATANTE em manter sua SOLUÇÃO ativa. Não é um problema e sim suporte para ajustes ou otimizações. Problemas ou dúvidas que não afetem a operação da solução.

22.5 Fornecimento de versões de software atualizadas e manutenção corretiva dos sistemas, compreendendo o diagnóstico e identificação de problemas, correção de erros, de defeitos (bugs), de falhas comprovadas de segurança ou de mau funcionamento sobre qualquer funcionalidade ou decorrente de qualquer customização efetuada pela CONTRATADA durante a vigência do contrato;

22.6 Fornecimento dos patches e novas versões de software integrantes das soluções, objeto deste termo, sem custo adicional para a CONTRATANTE, tão logo se tornem disponíveis, num prazo máximo de 60 (sessenta) dias.

22.7 A cada atualização realizada, a CONTRATANTE deverá ser notificada por e-mail e disponibilizar no site, de forma relevante a ser identificada de imediato e deverão ser disponibilizados os manuais técnicos originais e documentos comprobatórios do licenciamento da nova versão/pat;

22.8 Garantia, à CONTRATANTE, de pleno acesso aos sites do fabricante da solução, objeto deste termo, com direito a consultas a quaisquer bases de conhecimento disponíveis para usuários e com direito a download de quaisquer atualizações regulares de software ou documentação, correções de versões, novas funcionalidades e aperfeiçoamentos das licenças de software a que tem direito, provendo informações, assistência e orientação para:

22.9 Instalação, desinstalação, configuração e atualização de software;

22.10 Aplicação de correções (patches);

22.11 Diagnósticos, avaliações e resolução de problemas;

22.12 Demais atividades relacionadas à correta operação e funcionamento dos sistemas;

22.13 Realização dos atendimentos observando a classificação dos problemas reportados, de acordo com os níveis de severidade, com a seguinte classificação;

ITEM	DESCRIÇÃO DA OCORRÊNCIA	GRAU
1	Deixar de atender evento de severidade 1, (em conformidade com o Item 22.15 e seus subitens). Problema que cause IMPACTO ALTISSIMO – solução inoperante ou severamente degradada, por ocorrência, cumulativamente não superior a 10%.	0,5 % do valor do contrato.
2	Deixar de atender evento de severidade 2, (em conformidade com o Item 22.19 e seus subitens). Problema que cause IMPACTO ALTO - que possivelmente coloque em risco um ambiente de produção - a solução continua operante, mas apresenta graves restrições., cumulativamente não superior a 10%.	0,4 % do valor do contrato.
3	Deixar de atender evento de severidade 3, (em conformidade com o Item 22.23). Problema que cause IMPACTO BAIXO – problemas ou dúvidas que criem restrições à operação da solução., por ocorrência, cumulativamente não superior a 10%.	0,3 % do valor do contrato.
4	Deixar de atender evento de severidade 4, (em conformidade com o Item 22.26). Problema que NÃO CAUSE IMPACTO na capacidade da CONTRATANTE em manter sua SOLUÇÃO ativa, por ocorrência, cumulativamente não superior a 10%.	0,2 % do valor do contrato.

22.14 Glosas a serem aplicadas de acordo com o nível de severidade;

22.15 Para os problemas classificados como de severidade 1 (um), a assistência técnica será prestada em regime 24x7x365 (on-site), com atendimento em até 2 (duas) horas corridas após o registro do chamado;

22.16 A solução de contingência não poderá ultrapassar 8 (oito) horas corridas, após o registro do chamado;

22.17 Caso haja necessidade de troca do equipamento ou peça, esta deverá ser feita em no máximo 24 (vinte e quatro) horas corridas, contadas a partir da abertura do chamado;

22.18 A solução definitiva não poderá ultrapassar 10 (dez) dias corridos após o registro do chamado;

22.19 Para os problemas classificados como severidade 2 (dois), a assistência técnica será prestada em regime 24x7x365 (remota ou on-site), com atendimento em até 2 (duas) horas corridas após o registro do chamado;

22.20 Caso o problema não tenha sido contingenciado após 6 (seis) horas corridas, a partir do registro do chamado, a assistência técnica deverá ser on-site e a solução de contingência não poderá ultrapassar 10 (dez) horas corridas, após o registro do chamado;

22.21 Caso haja necessidade de troca do equipamento ou peça, esta deverá ser feita em no máximo 72 (setenta e duas) horas corridas, contadas a partir da abertura do chamado;

22.22 A solução definitiva não poderá ultrapassar 15 (quinze) dias corridos após o registro do chamado;

22.23 Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 4 (quatro) horas após o registro do chamado;

22.24 A PROPONENTE terá, no máximo, 40 (quarenta) horas, após o registro do chamado, para implantar uma solução de contingência;

22.25 A solução definitiva não poderá ultrapassar 30 (trinta) dias corridos após o registro do chamado.

22.26 Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (quatro) horas após o registro do chamado;

22.27 A PROPONENTE terá, no máximo, 15 dias corridos para responder ao chamado e solucionar, após o seu registro;

22.28 Demais problemas de hardware, a solução definitiva não poderá ultrapassar 45 (quarenta e cinco) dias corridos e para software, 6 (seis) meses;

22.29 O descumprimento de qualquer um dos indicadores supracitados acarretará a aplicação de multa, previstas no Item 21, e de acordo com a legislação em vigor;

22.30 A Tabela a seguir apresenta os prazos máximos, contados a partir abertura do chamado, a serem atendidos pela CONTRATADA para cada grau de severidade;

Severidade	**Atendimento**			
	Regime	**Prazo**	**Solução de Contingência**	**Solução Definitiva**
1	**24x7x365 (on-site)**	Até 2 (duas) horas corridas*	Até 8 (oito) horas corridas*	Até 10 (dez) dias corridos*
2	**24x7x365 (remoto ou on-site)**	Até 2 (duas) horas corridas*	Até 10 (dez) horas corridas*	Até 15 (quinze) dias corridos*
3	**Horário comercial 8x5 (remoto)**	Até 4 (quatro) horas*	Até 40 (quarenta) horas*	Até 30 (trinta) dias corridos*
4	**Horário comercial 8x5 (remoto)**	Até 4 (quatro) horas*	Suporte / Resposta ao chamado: Até 15 (quinze) dias corridos*	
(*) prazo após o registro do chamado				

22.31 A CONTRATADA deverá permitir acesso da CONTRATANTE a sua central de atendimento ou à central de atendimento do fabricante no Brasil, com disponibilização de número fixo no Brasil e endereço de e-mail ou ferramenta de acesso WEB para registro de chamados e respectivo acompanhamento, na modalidade 24x7x365, envolvendo todos os recursos do ambiente que será objeto do contrato com resolução de problemas, via telefone ou via ferramenta WEB. O registro dos chamados deverá possuir, pelo menos, as seguintes informações: data, hora, descrição da demanda, número da ordem de serviço, identificação do solicitante e do atendente;

22.32 Os prazos para atendimento dos serviços de suporte técnico serão interrompidos somente se ficar caracterizado que se trata de falha de laboratório (bug), sendo necessário o encaminhamento da falha ao laboratório do fabricante e o acompanhamento de sua solução. Neste caso, a empresa deverá estabelecer uma solução de contorno para a falha até que a solução definitiva seja adotada, principalmente se for referente a problemas de severidade 1 e 2;

22.33 Entende-se por término do reparo do sistema a disponibilidade do mesmo para uso em perfeitas condições de funcionamento no local onde está instalado. Porém, o chamado somente poderá ser fechado após a equipe técnica da CONTRATANTE declarar que o ambiente está em perfeito funcionamento e deverá haver a possibilidade de reabertura dos chamados fechados indevidamente.

22.34 Comunicação, por escrito, à CONTRATANTE, de condições inadequadas de funcionamento ou má utilização a que estejam submetidos os sistemas objeto desta especificação, fazendo constar a causa de inadequação e a ação devida para a correção;

22.35 Responsabilidade pelas ações executadas ou recomendadas por analistas e profissionais do quadro da empresa bem como pelos efeitos provenientes da execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função da execução dessas atividades;

22.36 Orientação e esclarecimento à equipe técnica da CONTRATANTE, sobre os assuntos pertinentes ao objeto deste termo, principalmente nos casos em que a CONTRATADA executar manutenções na ferramenta;

22.37 Emissão de relatório de serviços de suporte, em meio eletrônico, quando demandado pela CONTRATANTE, em que constem informações referentes ao número e descrição do chamado técnico, data e hora da abertura do chamado e dos andamentos, data e hora do término do atendimento e descrição da solução. Por meio desse relatório verificar-se-á o cumprimento do SLA e das demais obrigações contratuais para posterior desembolso físico financeiro, que ocorrerá após aprovação do fiscal do contrato BBTS.

23. Vigência:

23.1 As licenças serão adquiridas em caráter permanente. A garantia terá vigência de 36 (trinta e seis) meses, prorrogável até o limite de 60 (sessenta) meses.

24. Repactuação de preço/Reajuste:

24.1 O preço estipulado para as licenças será fixo e reajustável.

24.2 O preço estipulado para a garantia poderá ser repactuado mediante acordo entre as partes, de conforme previsto na legislação vigente, adotando-se como parâmetros básicos a qualidade e os preços de mercado para a prestação dos serviços objeto deste Contrato.

24.3 Será admitida a repactuação dos preços dos serviços contratados, desde que seja observado o interregno mínimo de um ano.

25. Matriz de risco:

CATEGORIA DO RISCO	DESCRIÇÃO	CONSEQUÊNCIA	ALOCAÇÃO DO RISCO
Risco atinente ao Tempo da Execução	Atraso na execução do objeto contratual por culpa do Contratado.	Aumento do custo do produto e/ou do serviço.	Contratada
	Fatos retardadores ou impeditivos da execução do contrato próprios do risco ordinário da atividade empresarial ou da execução.	Aumento do custo do produto e/ou do serviço.	Contratada
	Fatos retardadores ou impeditivos da execução do contrato que não estejam na sua álea ordinária, tais como fatos do príncipe.	Aumento do custo do produto e/ou do serviço.	Contratante

Risco da Atividade Empresarial	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária.	Aumento ou diminuição do lucro do Contratado.	Contratada
	Variação da taxa de câmbio.	Aumento ou diminuição do custo do produto e/ou do serviço.	Contratada
	Violação de dados pessoais de TERCEIROS identificados e identificáveis por falha de segurança técnica e administrativa.	Sujeito às penalidades contratuais por infringência à Lei Geral de Proteção de Dados.	Contratada
	Violação de dados pessoais de terceiros identificados e identificáveis por descumprimento das orientações do Contratante.	Sujeito às penalidades contratuais por infringência à Lei Geral de Proteção de Dados.	Contratada
	Violação de dados pessoais de terceiros identificados e identificáveis por descumprimento das normas de proteção de dados.	Sujeito às penalidades contratuais por infringência à Lei Geral de Proteção de Dados.	Contratada

	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra.	Aumento do custo do produto e/ou do serviço.	Contratante

26. Qualificação Econômico-Financeira:

26.1 A qualificação econômico-financeira da CONTRATADA será avaliada de acordo com os seguintes critérios:

26.1.1 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da legislação em vigor, acompanhado do demonstrativo das contas de lucros e prejuízos que comprovem sua boa situação financeira.

26.1.2 A comprovação da boa situação financeira da CONTRATADA será baseada também na obtenção de Índices de Liquidez Geral (LG), de Solvência Geral (SG) e de Liquidez Corrente (LC) resultantes da aplicação das fórmulas abaixo, sendo considerada habilitada a empresa que apresentar resultado maior que 1, em todos os índices aqui mencionados:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

26.1.3 Caso o fornecedor que não atinja os índices econômico-financeiros, será aceito alternativamente a comprovação de patrimônio líquido igual ou superior a 10% (dez por cento) do valor estimado da contratação, por meio da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, apresentados na forma da lei, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrados há mais de 3 (três) meses da data da apresentação da proposta.

27. Qualificação Técnica:

27.1 A qualificação técnica da CONTRATADA será avaliada de acordo com os seguintes critérios:

27.2 Apresentar para fins de qualificação técnica no mínimo 01 (um) atestado(s) e/ou declaração(ões) de capacidade técnica comprovando que executa/executou, serviço compatível em características, quantidades e prazos ao indicado no projeto básico, sendo aceito o somatório de atestado, sendo admitida a apresentação de atestados referentes a períodos sucessivos não contínuos, não havendo obrigatoriedade de a soma dos períodos serem ininterruptos.

27.3 A CONTRATADA deve disponibilizar, se solicitadas, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia simples do contrato que deu suporte à contratação, cópia das notas fiscais, endereço atual da CONTRATANTE e local em que foram prestados os serviços.

28. *Due Diligence*:

28.1 Considerando que a BB TECNOLOGIA E SERVIÇOS S.A. implementou a gestão de risco de fornecedores por meio de Due Diligence, e que a referida ferramenta permite aumentar a segurança nas contratações e na gestão, fica a CONTRATADA, ciente de que, a critério da BB Tecnologia e Serviços, poderá efetuar o Background Check (Análise Reputacional) e solicitar que a CONTRATADA preencha, assine e encaminhe o FQ415-042- Questionário de Due Diligence (anexo V) com as devidas evidências, no prazo máximo de 03 (três) dias úteis, contados da solicitação do envio, observando que a entrega do questionário respondido e suas evidências é fato determinante para a assinatura do contrato.

29. Pesquisa de Pessoas Expostas Politicamente (PEP)

29.1 Considerando que a BB TECNOLOGIA E SERVIÇOS S.A. implementou a gestão de risco de fornecedores para aumentar a segurança nas contratações e na gestão, fica a CONTRATADA, ciente de que, a critério da BB Tecnologia e Serviços, poderá ser realizada pesquisa de Pessoas Expostas Politicamente.

30. Garantia Financeira da Execução Contratual:

30.1 Será exigida garantia de 5% (cinco por cento) sobre o valor contratado, nos termos do artigo 70 da Lei nº 13.303/16.

30.2 A garantia deverá ser válida durante todo o período de vigência do contrato, estendendo-se por mais 3 (três) meses após o término desse período.

ANEXO 2 – MODELO DE PROPOSTA COMERCIAL

Planilha de Preços					
LOTE ÚNICO					
	ITENS	**1**	**2**	**3**	**4**
EMPRESA	**DESCRIÇÃO**	**Valor para 5.000 (cinco) mil licenças para a funcionalidade de autenticação, autorização e gestão de contas temporárias.**	**Valor para 1.000 (mil) licenças para a funcionalidade de classificação automática de dispositivos**	**Valor para 300 (trezentas) licenças para a funcionalidade de postura de admissão.**	**Valor da garantia 36(trinta e seis) meses.**
xxxxxxx	**Valor unitário**				
	Valor total do item				
Valor total da proposta					

ANEXO 3 – QUESTIONÁRIO DE DUE DILIGENCE

1. **Informações Cadastrais**

1.1. Razão social:

1.2. Nome fantasia:

1.3. CNPJ:

1.4. Endereço:

1.5. CEP:

1.6. E-mail:

1.7. Website:

1.8. Telefone:

1.8.1 Telefone 1:

1.8.2 Telefone 2:

1.8.3 Telefone Celular:

1.9. Porte da Empresa:

□ Microempresa – Faturamento menor ou igual a R$ 360 mil.

□ Pequena empresa – Faturamento maior que R$ 360 mil e menor ou igual a R$ 4,8 milhões.

□ Média empresa – Faturamento maior que R$ 4,8 milhões e menor ou igual a R$ 300 milhões.

□ Grande empresa – Faturamento maior que R$ 300 milhões.

1.10. Ramo principal de atividade da empresa:

□ Comercial

□ Industrial

□ Prestação de Serviço

1.11. Informar número de Empregados:

2. Eixo Gestão

b. A empresa possui Código de Ética, Guia de Conduta ou documentos correlatos que descrevem as condutas éticas que devam ser observadas pelos integrantes da Alta Administração, empregados próprios e/ou terceirizados?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

c. A empresa possui alguma política formal ou programa de responsabilidade empresarial que inclua aspectos ambientais, sociais e de saúde e segurança do colaborador?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

d. A empresa divulga publicamente relatório anual sobre sua atuação referente aos eixos financeiros, ambientais e sociais?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

e. Qual o faturamento da empresa nos últimos 3 anos?

2018:_____ 2019:_____ 2020: _____

f. A empresa possui algum certificado do sistema gestão? (ISO 9.001, 14.001, 16.001, 27.001, 37.001, OHSAS 18.001, entre outros)?

□ Sim □ Não

Nota – Requer a apresentação de evidência (s).

g. A empresa promove ações de capacitação do público interno em questões relacionadas a gestão ambiental, diversidade, assédio, direitos humanos, anticorrupção, etc.?

□ Sim □ Não

Nota – Requer a apresentação de evidência (s).

1. Eixo Social (Direitos Humanos)

h. A empresa possui compromisso formal com os Direitos Humanos?

□ Sim □ Não

Nota 1 - Considerar compromissos relacionados: à erradicação do trabalho infantil, erradicação do trabalho forçado ou compulsório, combate à prática de discriminação em todas suas formas, prevenção do assédio moral e do sexual, valorização da diversidade, respeito à livre associação sindical e direito à negociação coletiva.

Nota 2: Requer apresentação de evidência (s).

i. A sua empresa responde ou respondeu, nos últimos 3 anos, processo judicial ou administrativo decorrente de práticas envolvendo trabalho forçado ou compulsório e/ou trabalho infantil, em suas próprias operações ou em sua cadeia de suprimentos?

□ Sim □ Não

Nota: Se positivo, apresentar evidência (s) com o número do processo e instância.

j. A sua empresa responde ou respondeu, nos últimos 3 anos, processo judicial ou administrativo decorrente de práticas envolvendo assédio moral ou sexual e/ou discriminação em suas próprias operações ou em sua cadeia de suprimentos?

□ Sim □ Não

Nota: Se positivo, apresentar evidência (s) com o número do processo e instância.

k. A sua empresa promove o engajamento do público interno, incluindo trabalhadores terceirizados, no combate a qualquer prática de discriminação em matéria de emprego e ocupação?

□ Sim □ Não

Nota - Se positivo, apresentar evidência (s). Considerar iniciativas ou procedimentos relacionados: à seleção e contratação, promoção, acesso a treinamento, sensibilização dos funcionários diretos e trabalhadores terceirizados para o tema.

l. A empresa avalia a satisfação dos funcionários e implementa ações de melhoria contínua?

□ Sim □ Não

Nota 1 - Em caso de resposta positiva, considerar que pelo menos um dos temas seguintes são atendidos: Clima organizacional (exposição a estresse, ambiente harmônico, cooperação entre funcionários, etc.); Carga de trabalho (horas trabalhadas, metas de produção e outros tipos de demandas); Remuneração compatível com a carga de trabalho; Benefícios.

Nota 2 - Requer apresentação de evidência (s).

m. A empresa tem políticas de melhoria da qualidade de vida dos funcionários?

□ Sim □ Não

Nota 1 - Em caso de resposta positiva, considerar que pelo menos um dos temas seguintes são atendidos: Incentiva ações para a alimentação saudável, academia, ginástica laboral e outras atividades que promovam o bem estar e uma vida mais saudável (física e psíquica); Conscientiza, informa e estimula seus funcionários quanto a um estilo de vida saudável; Acompanha a situação de seus funcionários quanto a aspectos relacionados à sua qualidade de vida e estrutura programas que incentivem progressos em relação ao tema; Possui programas que incentivem a redução de horas-extras e equilíbrio entre carga horária disponível e demanda de trabalho.

Nota 2 - Requer apresentação de evidência (s).

n. A empresa busca, por meio de práticas cotidianas, construir um relacionamento com a comunidade local visando seu desenvolvimento?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s).

o. A empresa tem política de diversidade publicamente disponível que inclua fatores de diversidade como gênero, cor, etnia, orientação sexual, país de origem ou nacionalidade?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s).

p. Nos quadros da empresa tem mulheres ocupando cargo de gerência e/ou diretoria?

□ Sim. Quantas? _____ □ Não

q. Nos quadros da empresa tem negros ocupando cargo de gerência e/ou diretoria?

□ Sim. Quantos? _____ □ Não

r. Na empresa existe diferença na remuneração entre pessoas de gêneros diferentes ocupantes de cargos de gerência e/ou diretoria?

□ Sim. Percentual médio da diferença_____ □ Não

s. Na empresa, as funcionárias que retornam de licença-maternidade permanecem por no mínimo 12 meses após o retorno?

□ Sim □ Não.

t. Nos quadros da empresa tem pessoas com deficiência (PcD)?

□ Sim. Quantas? ___□ Não

u. A empresa adota medidas visando promover a empregabilidade de pessoas com deficiência(PcD)?

□ Sim □ Não

Nota 1 - Considerar uma ou mais das seguintes medidas: investimento em meios de acessibilidade; investimento em tecnologias adequadas para a realização do trabalho; capacitação profissional; sensibilização e conscientização de seus funcionários para a recepção e boa convivência profissional.

Nota 2 - Se positivo, requer a apresentação de evidência (s).

v. A empresa disponibiliza plano de saúde para os funcionários?

□ Sim □ Não

w. Qual o tempo médio de trabalho dos funcionários da empresa?

□ De 1 a 5 anos

□ De 5 a 10 anos

□ Acima 10 anos

1. Eixo Ambiental

x. O monitoramento e a mitigação dos riscos socioambientais fazem parte da estratégia da empresa?

□ Sim □ Não

y. A alta direção patrocina/acompanha as ações/estratégias ambientais?

□ Sim □ Não

z. A empresa possui licença (s) ambiental (is) para o funcionamento? (Licença de Operação - LO ou equivalente)?

□ Sim □ Não □ Não se aplica

Nota 1 - Caso seja aplicado à atividade da empresa a necessidade da licença ambiental.

Nota 2 – Requer a apresentação de evidência (s).

aa. A empresa possui passivos ambientais?

□ Sim □ Não

bb. A empresa foi autuada, multada ou notificada nos últimos 10 anos por motivo de crime ou descumprimento da legislação ambiental?

□ Sim □ Não

Nota 2: Se positiva apresentar evidência com o número do processo e órgão para verificação.

cc. A empresa possui procedimentos estruturados para logística reversa, em conformidade com a Lei nº 12.305/2010?

□ Sim □ Não □ Não se aplica

dd. A empresa possui programa de Coleta seletiva implementado?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s).

ee. A empresa emite relatório de emissão de GEE (Gases do efeito estufa) relacionados a sua atividade?

□ Sim □ Não □ Não se aplica

Nota - Requer a apresentação de evidência (s).

ff. A empresa possui política ambiental para redução da emissão de GEE (Gases do efeito estufa)?

□ Sim □ Não □ Não se aplica

Nota - Requer a apresentação de evidência (s).

4.10 A empresa tem conhecimento da procedência dos insumos utilizados no seu processo produtivo e/ou prestação de serviço?

□ Sim □ Não

4.11 A empresa possui programa de geração distribuída ou faz uso de outra matriz energética além da convencional?

□ Sim Qual?_____ □ Não

4.12 A empresa possui ações/metas para redução do consumo de energia elétrica e água?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s).

1. Eixo Integridade

1.1. Nome, cargo e percentual de participação (quando aplicável) de seus proprietários, sócios controladores, conselheiros e diretores:

Nome	CPF	Cargo	% Participação (quando plicável)

5.1.1 Percentual de participação societária da sua empresa em outras pessoas jurídicas na condição de controladora, controlada, coligada ou consorciada, bem como a razão social e o CNPJ das mesmas.

□ Não se aplica

Razão Social	CNPJ	% Participação	Relacionamento Societário

1.2. A empresa ou sociedades controladoras, controladas, coligadas ou consorciadas estão localizadas ou realizam operações comerciais e financeiras nos seguintes locais:

Angola, Argentina, Bolívia, China, Colômbia, Gabão, México, Nigéria, Paraguai, Tanzânia, Venezuela, Ilhas Cayman, Cingapura, Mônaco, Panamá, Ilhas Virgens Britânicas, Nicarágua.

□ Sim □ Não

1.3. A sua empresa é membro de alguma iniciativa nacional ou internacional de combate à corrupção?

□ Sim. Qual? _____ □ Não

1.4. Algum integrante da Alta Administração[1] ou seus familiares[2] (até terceiro grau) ocupa ou é candidato a cargo eletivo ou cargo de confiança na administração pública?

□ Sim □ Não

1.4.1. Em caso afirmativo, forneça os detalhes abaixo:

Nome	Grau de Parentesco	Nome do Órgão/Entidade	Cargo	Período

[1] Ocupantes de cargo ou membros de colegiados posicionados hierarquicamente acima da linha gerencial média. Ex.: Membros do Conselho de Administração e da Diretoria Executiva, Sócios, Presidente, Vice-presidente, Diretor e/ou Gerente Executivo.

[2] Primeiro grau: pai, mãe e filhos; Segundo grau: irmãos, avós e netos; Terceiro grau: tios, sobrinhos, bisavós e bisnetos

1.5. Algum integrante da Alta Administração ou seus familiares (até terceiro grau) mantém negócios pessoais ou relacionamento próximo com algum agente público?

□ Sim □ Não

1.5.1. Em caso afirmativo, forneça os detalhes abaixo:

Nome	Nome do Órgão/Entidade	Cargo	Grau de Parentesco	Nome do empregado ou membro	Cargo do empregado ou membro

1.6. Algum integrante da Alta Administração é familiar (até terceiro grau) de algum empregado da BB Tecnologia e Serviços que ocupe função gerencial ou de algum membro da Diretoria Executiva ou Conselho de Administração da BBTS ou de funcionário que trabalhe diretamente com o processo de compra e contratação da BBTS?

□ Sim □ Não

1.6.1. Em caso afirmativo, forneça os detalhes abaixo:

Nome	Grau de Parentesco	Nome do empregado ou membro	Cargo do empregado ou membro

1.7. A sua empresa possui regras específicas formalizadas para visitas e demais interações com entes públicos, com foco na Prevenção e Combate à Corrupção?

□ Sim □ Não

Nota – Se positivo fornecer evidência (s).

1.8. Algum integrante da Alta Administração da sua empresa já foi preso, acusado, investigado (mesmo que em curso), processado ou condenado por fraude ou corrupção nos últimos 10 anos?

□ Sim □ Não

Nota – Se positivo fornecer evidência (s).

1.9. A empresa, controladoras, controladas, coligadas ou consorciadas já foram acusadas, investigadas (mesmo que em curso), processadas ou condenadas por fraude ou corrupção nos últimos 10 anos?

□ Sim □ Não

Nota – Se positivo fornecer evidência (s).

1.10. A empresa, controladora, controlada, coligada ou consorciada já entregou, ofertou, autorizou, acordou ou prometeu qualquer tipo de pagamento ou benefício a qualquer autoridade governamental nacional ou estrangeira, para angariar ou manter negócios, ou mesmo obter qualquer vantagem comercial, nos últimos 10 anos?

□ Sim □ Não

Nota – Se positivo fornecer evidência (s).

1.11. Algum integrante da Alta Administração, empregado, agente ou terceiro representando a sua empresa já entregou, ofertou, autorizou, acordou ou prometeu qualquer tipo de pagamento ou benefício a qualquer autoridade governamental nacional ou estrangeira, para angariar ou manter negócios, ou mesmo obter qualquer vantagem comercial, nos últimos 10 anos?

□ Sim □ Não

Nota – Se positivo fornecer evidência (s).

1.12. A empresa, controladora, controlada, coligada ou consorciada esteve submetida à investigação ou avaliação externa relacionada à fraude e/ou corrupção por algum órgão ou

agência, nacional ou internacional (CGU, TCU, TCE, CVM, SEC, PF, etc.) nos últimos 10 anos?

□ Sim □ Não

Nota – Se positivo fornecer evidência (s).

1.13. A empresa conhece a legislação anticorrupção a qual está sujeita?

□ Sim □ Não

1.14. A empresa possui um Programa de Integridade estruturado com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira?

□ Sim □ Não

Nota 1 - Caso a resposta desta questão seja “Sim”, responder às Questões 5.15 e 5.16.

Nota 2 - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

1.15. A empresa possui uma estrutura hierárquica definida para coordenar e implantar o programa de integridade?

□ Sim □ Não

1.16. O Programa de Integridade é revisado periodicamente pela Alta Administração?

□ Sim. Qual periodicidade? ____ □ Não

1.17. A empresa possui unidade específica e independente para mapear e analisar os riscos aos quais está exposta e verificar o cumprimento da legislação pelos empregados?

□ Sim □ Não

1.18. A empresa possui mapeamento dos riscos de ocorrência de fraude e corrupção?

□ Sim □ Não

1.19. A empresa possui medidas para evitar atos de corrupção nas situações de risco identificadas?

□ Sim □ Não

1.20. A empresa possui política anticorrupção ou documento equivalente, amplamente distribuída para colaboradores, gestores, diretores e conselheiros?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.21. A empresa possui normativos internos que determinem a proibição de qualquer tipo de pagamento ou benefício a qualquer autoridade governamental nacional ou estrangeira, para obter ou manter negócios ou vantagem comercial?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.22. A empresa possui normativos internos que determinem a proibição ou restrição, quanto ao oferecimento de presentes, brindes e hospitalidade a agentes públicos, clientes e parceiros comerciais?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.23. A empresa possui normativos internos que disponham sobre doação e/ou contribuição a instituições de caridade, programas sociais ou a partidos políticos?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.24. A empresa possui normativos internos de *Due Diligence* para a avaliação da reputação, idoneidade e das práticas de combate à corrupção de terceiros, tais como: fornecedores, distribuidores, agentes, consultores, representantes comerciais e/ou parceiros operacionais?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.25. A empresa conhece os documentos da BB Tecnologia e Serviços, disponibilizados no site www.bbts.com.br, relacionados a Compliance, Ética e Integridade?

□ Sim □ Não

https://www.bbts.com.br/index.php/canal-do-fornecedor-etica-integridade

1.25.1. Se afirmativo, informar quais documentos disponibilizados pela BBTS (www.bbts.com.br) sua empresa tem conhecimento:

□ Política de Relacionamento com Fornecedores

□ Código de Ética e Normas de Conduta

□ Política de Prevenção e Combate à Corrupção, Lavagem de Dinheiro e ao Financiamento do Terrorismo

□ Programa de Compliance

1.26. A empresa oferece e/ou recomenda treinamentos periódicos sobre Integridade e/ou sobre os aspectos da Lei Anticorrupção?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.26.1. Se afirmativo, informar para quais públicos a empresa oferece e/ou recomenda treinamentos e fornecer evidencias:

□ Conselheiros □ Diretores □ Colaboradores □ Fornecedores

1.27. A empresa oferece e/ou recomenda treinamentos periódicos sobre o seu Código de Ética, Normas de Conduta?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.27.1. Se afirmativo, informar para quais públicos a empresa oferece e/ou recomenda treinamentos e fornecer evidencias:

□ Conselheiros □ Diretores □ Colaboradores □ Fornecedores

1.28. A empresa dá conhecimento e solicita aos empregados, que se relacionam com a BB Tecnologia e Serviços, que respeitem os documentos da BBTS, disponibilizados no site www.bbts.com.br, relacionados a Compliance, Ética e Integridade?

□ Sim □ Não

https://www.bbts.com.br/index.php/canal-do-fornecedor-etica-integridade

1.29. A empresa possui canal de denúncias relacionado à corrupção e a outros desvios de conduta, abertos e amplamente divulgados a todos os empregados próprios e/ou terceirizados?

□ Sim □ Não

Nota 1 - Caso tenha canal de denúncia, responda à Questão 5.30.

Nota 2 - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.30. O canal de denúncia garante o anonimato evitando qualquer tipo de perseguição ou retaliação ao denunciante?

□ Sim □ Não

1.31. A empresa possui mecanismos de investigação de indícios de fraude e/ou corrupção e procedimentos que assegurem a interrupção/correção de irregularidade ou infração detectadas e a tempestiva remediação dos danos gerados?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.32. A empresa possui normativos internos que disponham sobre o monitoramento da efetividade e da eficiência do programa de integridade anticorrupção da sua empresa?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

1.33. A empresa utiliza os serviços de terceiros, tais como agentes, consultores, representantes comerciais e/ou outros tipos de intermediários, sejam pessoas físicas ou jurídicas, com o objetivo de angariar novos negócios?

□ Sim □ Não

1.33.1. Se afirmativo, informar o nome e/ou razão social dos agentes, consultores, representantes comerciais e/ou outros tipos de intermediários, sejam pessoas físicas ou jurídicas

Nome/Razão Social	CPF/CNPJ

1.34. A empresa realiza avaliação prévia de requisito de integridade, para mitigar o risco de estabelecer relação de negócios com fornecedores, parceiros e demais terceiros, eventualmente envolvidos em ato de corrupção?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s).

1.35. A empresa divulga o seu programa de integridade aos seus fornecedores, distribuidores, representantes comerciais, intermediários e/ou outros tipos de parceiros de negócios?

□ Sim □ Não

1.36. A empresa solicita que seus fornecedores, distribuidores, representantes comerciais, intermediários e/ou outros tipos de parceiros de negócios declarem pleno conhecimento sobre os principais aspectos do seu programa de integridade?

□ Sim □ Não

Nota - Requer a apresentação de evidência (s).

1.37. Nos contratos firmados há previsão de cláusulas que obrigue a contraparte a respeitar

□ Programa de Integridade

□ Código de Ética/Norma de Conduta

□ Lei 12.846/2013 – Lei Anticorrupção

Nota 1 - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

Nota 2 – Pode ser marcado mais de uma alternativa

2. Declaração de veracidade das informações

2.1. Declaro e atesto para os devidos fins que este formulário foi preenchido por pessoa com poderes outorgados para representar a empresa e que as informações fornecidas acima, bem como os documentos disponibilizados são verdadeiros e não ocultaram quaisquer dados. Se em algum momento as informações ou documentos apresentados neste questionário não representarem mais a realidade, comprometemo-nos a comunicar imediatamente à BB Tecnologia e Serviços.

Local e data:

Assinatura:

Nome por extenso:

Cargo: