Projeto Básico – Aquisição de Solução de Software

1 Objeto:

1.1 Contratação de Solução de Segurança Multicamada e Multicanal para Proteção de Dispositivos e Detecção de Anomalias Web, para proteção do acesso às interfaces de canais web e mobile realizado pelos usuários do CONTRATANTE, tanto pessoas físicas quanto jurídicas, sejam eles clientes internos ou externos, de acordo com as condições e especificações técnicas descritas neste documento, compreendendo:

1.1.1 Cessão de direito de uso permanente do software, para quantidade ilimitada de usuários;

1.1.2 Serviços de instalação, customização, implementação, treinamento, garantia, compreendendo atualização, manutenção e suporte técnico;

1.1.3 Prestação de serviços de suporte técnico operacional, por 60 (sessenta) meses, contados do aceite da implementação.

1.2 A SOLUÇÃO e os serviços de suporte devem ser fornecidos única e exclusivamente pela PROPONENTE, sendo vedada a subcontratação dos serviços, exceto o uso de infraestrutura de terceiros para hospedagem e/ou distribuição da SOLUÇÃO, sendo obrigatórios o atendimento aos seguintes critérios:

1.2.1 A PROPONENTE assume todas as responsabilidades acerca da disponibilidade, segurança e integridade da infraestrutura de processamento e distribuição, sejam software ou hardware, bem como da SOLUÇÃO, hospedados e distribuídos por esta infraestrutura;

1.2.2 As funcionalidades técnicas objeto deste projeto básico serão providas por software fornecidos, mantidos e suportados pela própria PROPONENTE, de acordo com os demais critérios definidos neste projeto básico.

2 Detalhamento do Objeto:

2.1 A SOLUÇÃO deve ser apta a atender as especificações contidas neste documento em sua integralidade. Para tanto, deverá integrar-se aos processos, sistemas atuais e sistemas futuros do Banco do Brasil, além de contemplar os serviços de customização (se necessário) de manutenção, suporte técnico e transferência de tecnologia.

2.2 A SOLUÇÃO deve ser composta, no mínimo, pelas seguintes funcionalidades:

2.2.1 Proteção de Dispositivo (*Endpoint*): componente baseado em agente de software instalado no dispositivo do usuário, com capacidade de identificação do dispositivo, detecção, bloqueio e remoção de *malwares* (softwares maliciosos) e ameaças avançadas, para prover proteção contra ataques cibernéticos, principalmente dos tipos *DNS poison (*no dispositivo ou elemento de rede), *man-in-the-browser*, *man-in-the-middle*, *phishing*, *overlay*, *keylogging*, adulteração de informações de documentos, adulteração de dados de transação, captura de identidades e captura de credenciais;

2.2.2 Detecção de Anomalias Web: componente com capacidade de detecção de anomalias na navegação web, no acesso (login) e nas transações dos usuários, para detecção e prevenção, contra ataques cibernéticos, principalmente dos tipos *main-in-the-browser*, *phishing*, captura de identidade e captura de credenciais;

2.2.3 Gerenciador de Eventos: base centralizada de inteligência de segurança e de correlacionamento de eventos obtidos pelos componentes (item 2.2.1 e 2.2.2), para envio de alertas, *feeds* e consultas online de eventos de detecção e proteção, níveis de risco e informações sobre as detecções e proteções providas pela SOLUÇÃO, bem como para retroalimentação da base de inteligência;

2.2.4 Console de Gerenciamento: base centralizada com detalhamento dos eventos de detecção e proteção, agregação das informações para disponibilização de relatórios e estatísticas, com classificação e filtro dos dados, permitindo visualizações em diversos formatos (inclusive representação gráfica), além de prover parametrização e informações sobre os componentes de detecção e proteção.

3 Especificações Técnicas:

3.1 Requisitos Técnicos Funcionais

3.1.1 Requisitos do Componente de Proteção de Dispositivo (item 2.2.1)

3.1.1.1 Ser baseado em software, instalado e executado no dispositivo do usuário;

3.1.1.2 Ser capaz de executar suas funcionalidades em dispositivos do tipo computador pessoal, sejam desktop, notebooks ou assemelhados, com as seguintes características:

3.1.1.2.1 Sistemas operacionais de 32 e 64 bits da família Microsoft Windows, versões Windows XP (SP3), Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 10; assim como os novos que serão lançados e;

3.1.1.2.2 Ser compatível com, no mínimo, os seguintes navegadores:

3.1.1.2.2.1 Microsoft Internet Explorer (a partir da versão 9 e superiores, assim como as novas que serão lançadas);

3.1.1.2.2.2 Mozilla Firefox (a partir da versão 11 e superiores, assim como as novas que serão lançadas);

3.1.1.2.2.3 Google Chrome (a partir da versão 20 e superiores, assim como as novas que serão lançadas) e;

3.1.1.2.2.4 Opera (a partir da versão 11 e superiores, assim como as novas que serão lançadas).

3.1.1.2.3 Sistemas operacionais de 32 e 64 bits da família Apple, com a versões Mac OS X a partir da versão Leopard (10.5) e superiores, assim como os novos que serão lançados e;

3.1.1.2.4 Ser compatível com, no mínimo, os seguintes navegadores:

3.1.1.2.4.1 Apple Safari (a partir da versão 5 e superiores, assim como as novas que serão lançadas);

3.1.1.2.4.2 Mozilla Firefox (a partir da versão 11 e superiores, assim como as novas que serão lançadas).

3.1.1.2.5 Sistemas operacionais de 32 e 64bits das distribuições Linux e;

3.1.1.2.6 Ser compatível com, no mínimo, os seguintes navegadores:

3.1.1.2.6.1 Mozilla Firefox (a partir da versão 11, assim como as novas que serão lançadas);

3.1.1.2.6.2 Google Chrome (a partir da versão 20, assim como as novas que serão lançadas) e;

3.1.1.2.6.3 Opera (a partir da versão 11, assim como as novas que serão lançadas).

3.1.1.3 Ser capaz de executar suas funcionalidades em dispositivos do tipo *mobile*, seja *smartphones*, *tablets* ou assemelhados, rodando no mínimo os seguintes sistemas:

3.1.1.3.1 Sistemas operacionais das famílias Android OS – a partir da versão 2.3, assim como as novas que serão lançadas;

3.1.1.3.2 Sistemas operacionais das famílias Apple iOS – a partir da versão 7, assim como as novas que serão lançadas e;

3.1.1.3.3 Sistemas operacionais das famílias Windows Phone – a partir da versão 7.5 (*mango*), assim como as novas que serão lançadas.

3.1.1.4 Ser disponibilizado como pacotes de API - *Application Programming Interface* e/ou SDK - *Software Development Kit* (bibliotecas do kit de desenvolvimento), compatível com cada sistema operacional requerido para dispositivos do tipo *mobile*, seja *smartphones*, *tablets* ou assemelhados;

3.1.1.5 Permitir coletar arquivos e programas maliciosos e, quando aplicável, disponibilizar informações aos usuários sobre melhores práticas de segurança, analisando presença de softwares antivírus, versões de navegadores, versão de Java, atualizações do sistema operacional, entre outras, sugerindo atualizações sempre que recomendável;

3.1.1.6 Ser capaz de disponibilizar, a pedido da CONTRATANTE, software de instalação provido em pacote executável, compatível com cada sistema operacional, conforme item 3.1.1.2 e subitens, customizados para uso em ambientes corporativos, com ativação ou desativação de capacidades que permitam a execução do componente de proteção de dispositivo em ambientes com restrições de infraestrutura ou com imposição de políticas de segurança (como por exemplo: conectividade limitada, rede, *firewall*, *proxy*, restrições de técnicas de proteção, etc.);

3.1.1.7 O software de instalação deve, no mínimo, possuir as seguintes funcionalidades:

3.1.1.7.1 Ser único e implementado em um pacote executável, compatível com cada sistema operacional, conforme item 3.1.1.2 e subitens, para dispositivos do tipo computador pessoal, sejam *desktop*, *notebooks* ou assemelhados;

3.1.1.7.2 Possibilitar a exibição de logotipo e nome customizados da CONTRATANTE na interface de instalação para permitir ao usuário a associação direta da solução com a identidade visual da CONTRATANTE;

3.1.1.7.3 Ter processo de instalação transparente para o usuário e que não exija a reinicialização do dispositivo para ativação da SOLUÇÃO;

3.1.1.7.4 Executar um único processo de instalação para suportar todos os navegadores requeridos em um mesmo sistema operacional do dispositivo do usuário;

3.1.1.7.5 Exigir, para a execução do processo de instalação, que o usuário detenha poderes de administrador no sistema operacional do dispositivo;

3.1.1.7.6 Permitir a execução do processo de instalação em modo silencioso, inclusive quando o equipamento do usuário estiver em rede corporativa;

3.1.1.7.7 Permitir ao usuário, sem exigir o acionamento de suporte da PROPONENTE ou da CONTRATANTE, realizar com total autonomia a desinstalação do componente de proteção de dispositivo a qualquer momento sem prejuízos ao dispositivo, ao sistema operacional ou aos navegadores;

3.1.1.8 O software de instalação não deve:

3.1.1.8.1 Necessitar a instalação prévia de pacotes de software adicional (por exemplo: *Java Virtual Machine*, .NET *Framework*, Bibliotecas Visual C++, etc.) para execução completa do processo de instalação e ativação do componente de proteção de dispositivo;

3.1.1.8.2 Requerer nova instalação caso o usuário já possua o componente de proteção de dispositivo, mesmo que tenha sido instalado a partir de outra instituição financeira;

3.1.1.9 Suportar, no mínimo, os protocolos IPv4 e IPv6, para os eventos *login*, que consistem nos acessos dos clientes do BB às aplicações do Autoatendimento pela internet e mobile;

3.1.1.10 Possuir suporte aos idiomas abaixo, identificados pelo idioma do sistema operacional, configurado no dispositivo:

3.1.1.10.1 Português;

3.1.1.10.2 Inglês;

3.1.1.10.3 Espanhol;

3.1.1.10.4 Japonês.

3.1.1.11 Possuir mecanismo de atualizações, contínuas e transparentes, que não exija interação, intervenção do usuário e nem a reinicialização do sistema operacional;

3.1.1.12 Implementar mecanismos e técnicas de proteção com, no mínimo, as seguintes funcionalidades:

3.1.1.12.1 Estabelecer um ambiente virtual blindado entre o navegador do usuário-cliente e o servidor de páginas, através da integração do componente, implementado por software, de forma a garantir a proteção das transações dos clientes do Banco no Internet Banking e demais aplicações Web e ou Java, sem efetuar qualquer modificação nas configurações e arquivos existente no ambiente operacional do computador do cliente, com exceção nos casos de DNS poisoning;

3.1.1.12.2 Ser capaz de gerar código único para identificação de dispositivo, com proteção contra adulteração e que garanta que a identificação foi gerada

pelo próprio componente de proteção de dispositivo. Essa identificação deverá ter proteção eficiente contra clonagem e personificação;

3.1.1.12.3 Ser capaz de detectar, bloquear e/ou remover malwares e ameaças avançadas;

3.1.1.12.4 Possuir mecanismos de detecção de malware baseados em:

3.1.1.12.4.1 Assinaturas;

3.1.1.12.4.2 Análise de comportamentos de malwares e;

3.1.1.12.4.3 Inspeção de algoritmos.

3.1.1.12.5 Possuir heurística de detecção de sites falsos (phishing), inclusive com detecção baseada em padronagem visual;

3.1.1.12.6 Possuir mecanismo de proteção de navegador para bloquear acesso ao DOM (Document Object Model) do navegador a processos desconhecidos durante a navegação nos sites protegidos da CONTRATANTE;

3.1.1.12.7 Possuir mecanismo de proteção de navegador para bloquear alterações ou acesso aos processos e bibliotecas do navegador realizados por programas não permitidos;

3.1.1.12.8 Possuir mecanismo de proteção de navegador para iniciar proteção antes que quaisquer componentes ou extensões possam atuar no navegador;

3.1.1.12.9 Possuir mecanismo de proteção de navegador para bloquear os BHOs (Browser Help Objects) desconhecidos e os BHOs não assinados por um autor conhecido;

3.1.1.12.10 Possuir mecanismo de proteção de navegador para monitorar o acionamento de bibliotecas dinâmicas e bloquear a execução de módulos não autorizados e de módulos desconhecidos;

3.1.1.12.11 Ser capaz de bloquear captura de tela ou dados do usuário durante a navegação dos sites e o acesso a cookies de sites com informações protegidas;

3.1.1.12.12 Ser capaz de garantir que apenas os certificados informados pela CONTRATANTE sejam válidos na conexão com seus sites através de protocolo seguro (HTTPS);

3.1.1.12.13 Ser capaz de proteger contra ataques de envenenamento de DNS local (arquivo hosts) e nos elementos de rede (roteadores e modens Wifi, ADSL, etc) do usuário ou fornecidos pelo provedor de acesso a internet;

3.1.1.12.14 Ser capaz de criptografar teclas desde o driver do teclado até o navegador para prevenir ataques, principalmente, de keyloggers;

3.1.1.12.15 Detectar e alertar o usuário quando este navegar em sites maliciosos que tentem ou possam infectar o dispositivo;

3.1.1.12.16 Atuar no navegador protegendo o usuário mesmo que esteja navegando em modo anônimo;

3.1.1.12.17 Permitir coletar informações e artefatos automaticamente para análise, em caso de investigação de erros e para identificação de novas ameaças, sem exigir interação ou intervenção do usuário.

3.1.1.12.18 Permitir ao usuário alterar a configuração de conexão à internet do agente (conexão direta, detectar proxy automaticamente a partir das configurações do navegador, detectar proxy automaticamente a partir das configurações do sistema operacional e configurar proxy), independente da configuração do navegador, para ser usada tanto pelo mecanismo de atualização quanto de coleta de informações e artefatos;

3.1.1.12.19 Conter mecanismo que possa determinar elementos a serem bloqueados (Blacklist) ou liberados (Whitelist). Estes elementos devem ser:

3.1.1.12.19.1 Endereços de domínios e URLs;

3.1.1.12.19.2 Endereços IPs;

3.1.1.12.19.3 Arquivos e Programas;

3.1.1.12.19.4 Caminhos de arquivos.

3.1.1.12.20 Possuir mecanismos robustos de autoproteção, contra engenharia reversa, evitando ataques diretos à sua integridade e funcionamento.

3.1.2 Requisitos do Componente de Detecção de Anomalias Web

3.1.2.1 Executar as funções de detecção de anomalias web em qualquer software de navegação web compatível com, no mínimo com, as seguintes famílias e versões:

3.1.2.1.1 Item 3.1.1.2 e subitens retro;

3.1.2.1.2 Navegadores executando em dispositivos compatíveis com o sistema operacional Google Android OS a partir da versão 2.3 e as novas que serão lançadas;

3.1.2.1.3 Navegadores executando em dispositivos compatíveis no mínimo com o sistema operacional Apple iOS a partir da versão 4 e as novas que serão lançadas;

3.1.2.1.4 Navegadores executando em dispositivos compatíveis no mínimo com o sistema operacional Microsoft Windows Phone a partir da versão 7 e as novas que serão lançadas;

3.1.2.2 Ser capaz de realizar detecção determinística (dispositivo infectado ou não infectado;

3.1.2.3 Ser capaz gerar informações de detecção, principalmente, de ataques dos tipos *main-in-the-browser*, *phishing*, captura de identidade e captura de credenciais;

3.1.2.4 Considerar, para compor o perfil comportamental do usuário, no mínimo, as informações de dispositivo, navegador, navegação, identificação do usuário e transações realizadas pelo usuário;

3.1.2.5 Detectar, adicionalmente e no mínimo, os seguintes fatores de risco na interação do usuário:

3.1.2.5.1 Utilização de máquina virtual;

3.1.2.5.2 *Proxy*;

3.1.2.5.3 Inserção de URLs ao invés de fluxo normal de navegação;

3.1.2.5.4 Copiar e colar ao invés de digitação;

3.1.2.5.5 IP *velocity*;

3.1.2.5.6 Geolocalização suspeita;

3.1.2.5.7 Tentativas de falsificação de características do equipamento (*device spoofing*);

3.1.2.5.8 Dispositivo sendo operado remotamente;

3.1.2.5.9 Movimentos de mouse não usuais (automação).

3.1.3 Requisitos do Componente Gerenciador de Eventos

3.1.3.1 Possuir base global centralizada de informações de dispositivos envolvidos em ataques, para uso na detecção de *malwares* e ataques;

3.1.3.2 Enviar alertas, inclusive de desinstalação do componente de proteção de dispositivo, em tempo real, à CONTRATANTE;

3.1.3.3 Ser capaz de:

3.1.3.3.1 Manter histórico de eventos de detecção de *malware* e *phishing* obtidos pelos componentes de proteção de dispositivo e de detecção de anomalias web, armazenando a URL e suas características (IP, data do acesso, quantidade de acessos, etc.), no caso de *phishing*;

3.1.3.3.2 Correlacionar os eventos do item 3.1.3.3.1 com as detecções obtidas nos canais mobile e internet pelos componentes de proteção de dispositivo e de detecção de anomalias web;

3.1.3.3.3 Gerar índice de avaliação de risco, no acesso do usuário ou na execução de transação, disponibilizando para a CONTRATANTE para tratamento on-line do índice de risco.

3.1.3.4 Disponibilizar sistema de classificação por pontuação (*rating*) do estado geral dos equipamentos/computadores dos usuários finais, que leve em consideração o potencial de comprometimento da segurança (quanto maior o *rating*, maior o risco de fraude com a utilização do equipamento/computador).

3.1.4 Requisitos do Componente Console de Gerenciamento

3.1.4.1 Disponibilizar suas funcionalidades em interface web, com visualização textual e gráfica, com capacidade de exportar as informações para arquivo nos formatos PDF e CSV (texto separado por vírgula ou ponto-e-vírgula);

3.1.4.2 Disponibilizar opção para visualizar, no mínimo, as seguintes informações sobre a solução:

3.1.4.2.1 Quantidade de downloads do componente;

3.1.4.2.2 Quantidade de componentes instalados;

3.1.4.2.3 Quantidade de componentes desinstalados;

3.1.4.2.4 Status de Proteção (acessos protegidos X acessos totais);

3.1.4.2.5 Eventos de detecção de *malwares*, com a classificação por família;

3.1.4.2.6 URL de sites falsos (*phishing*) detectados e suas características (IP, data do acesso, quantidade de acessos, etc.);

3.1.4.2.7 Eventos de *malware* detectados pelo componente de detecção de anomalias Web, onde o agente não se encontra instalado no dispositivo;

3.1.4.2.8 Eventos de risco baseados em perfil de acesso do cliente.

3.1.4.3 Disponibilizar opção para consultar, no mínimo, as seguintes informações do componente de proteção de dispositivo instalado:

3.1.4.3.1 Data de instalação do componente;

3.1.4.3.2 Última comunicação com o componente;

3.1.4.3.3 Endereços IP associados ao dispositivo;

3.1.4.3.4 Versão atual do componente instalado;

3.1.4.3.5 Plataforma e versão do sistema operacional;

3.1.4.3.6 Identificadores de usuário associados ao dispositivo;

3.1.4.3.7 Status e histórico de infecções;

3.1.4.3.8 Histórico de atualizações do componente;

3.1.4.3.9 Processos em execução no equipamento;

3.1.4.3.10 Componentes não-padrão adicionados aos navegadores do dispositivo;

3.1.4.3.11 Informar, no mínimo, as seguintes ferramentas e funcionalidades e seu *status* (habilitado, atualizado ou desatualizado) quando aplicável ao ambiente do dispositivo:

3.1.4.3.11.1 Atualizações automáticas do sistema operacional;

3.1.4.3.11.2 Atualizações Java;

3.1.4.3.11.3 Atualizações Acrobat Reader;

3.1.4.3.11.4 Adobe Flash;

3.1.4.3.11.5 Navegador Padrão;

3.1.4.3.11.6 Antivírus;

3.1.4.3.11.7 Firewall.

3.1.4.4 Disponibilizar opção para visualizar as tendências de infecções ocorridas nos aplicativos protegidos da CONTRATANTE em comparação com as tendências por regiões e mundial;

3.1.4.5 Permitir à CONTRATANTE a parametrização dos intervalos e destinos dos *feeds* de eventos e alertas;

3.1.5 Arquitetura

3.1.6 A SOLUÇÃO deve atuar em múltiplas camadas e múltiplos canais, implementando, no mínimo:

3.1.6.1 Camada baseada em agente instalado para proteção de dispositivo do usuário e seu acesso aos aplicativos *web* e *mobile* disponibilizados pelo CONTRATANTE;

3.1.6.2 Camada baseada na detecção de anomalias na navegação, no acesso aos aplicativos *web* e *mobile*, independente de componente instalado;

3.1.6.3 Camada baseada na detecção de anomalias na execução de *logins* e na execução de transações no acesso aos aplicativos *web* e *mobile*, independente de componente instalado;

3.1.6.4 Camada de correlação de eventos e dados de risco, entre camadas, canais e entidades internas e externas, para retroalimentar as bases de inteligência da solução, aprimorando e incrementando a assertividade da solução na detecção e prevenção de ataques e provendo identificação de dispositivos e usuários historicamente comprometidos ou envolvidos em ataques.

3.1.6.5 A SOLUÇÃO deve atuar nos aplicativos abaixo (relação não exaustiva), web ou mobile, com acesso pelos canais web e mobile do CONTRATANTE, em endereços associados aos domínios e subdomínios registrados em DNS (Domain Name Service) em nome da CONTRATANTE, dentre os quais, mas não apenas, "*.bancobrasil.com.br", "*.bb.com.br", "*.bancodobrasil.com.br", usados, no mínimo e principalmente, pelos seguintes serviços aplicativos:

3.1.6.5.1 Online Banking Pessoa Física (Auto Atendimento Pessoa Física);

3.1.6.5.2 Online Banking Exterior (Auto Atendimento Internacional);

3.1.6.5.3 Office Banking Pessoa Jurídica (Auto Atendimento Pessoa Jurídica);

3.1.6.5.4 Office Banking Setor Público (Auto Atendimento Setor Público);

3.1.6.5.5 Office Banking Exterior (Treasure Management System);

3.1.6.5.6 Correspondentes Bancários (Coban);

3.1.6.5.7 Home Broker;

3.1.6.5.8 Tesouro Direto;

3.1.6.5.9 Emissão de segunda via de boleto;

3.1.6.5.10 Portal BB;

3.1.6.5.11 Aplicativos Transacionais BB.

3.1.6.6 A distribuição do software de instalação para download deve ser realizada por infraestrutura disponibilizada pela PROPONENTE ou sob sua responsabilidade, fora do ambiente da CONTRATANTE, com capacidade suficiente para atender a todos os usuários dos canais web e mobile da CONTRATANTE;

3.1.6.7 Admite-se a distribuição do software de instalação a partir de loja de software oficial (Apple Application Store, Google Play Store e Windows Phone Store), para download e instalação do componente de proteção de dispositivo em dispositivos do tipo *mobile*, sejam *smartphones*, *tablets* ou assemelhados;

3.1.7 Infraestrutura

3.1.7.1 A SOLUÇÃO não pode requerer, para seu pleno funcionamento ou instalação ou atualização, nenhum software executável adicional instalado e executando na infraestrutura de datacenter da CONTRATANTE;

3.1.7.2 A SOLUÇÃO não pode requerer, para seu pleno funcionamento ou instalação ou atualização, nenhum hardware adicional instalado e operando na infraestrutura da CONTRATANTE;

3.1.7.3 A SOLUÇÃO não pode requerer, para seu pleno funcionamento ou distribuição ou atualização, nenhuma capacidade adicional na infraestrutura de datacenter da CONTRATANTE;

3.1.7.4 A SOLUÇÃO não pode requerer, para seu pleno funcionamento ou instalação ou atualização, nenhum software executável adicional instalado e executando na infraestrutura de datacenter da CONTRATANTE;

3.1.7.5 A SOLUÇÃO não pode requerer, para seu pleno funcionamento ou instalação ou atualização, nenhum hardware adicional instalado e executado na infraestrutura da CONTRATANTE;

3.1.7.6 A SOLUÇÃO não pode requerer, para seu pleno funcionamento ou instalação ou atualização, nenhuma capacidade adicional na infraestrutura de datacenter da CONTRATANTE;

3.1.8 Integração

3.1.8.1 O componente gerenciador de eventos deve ser capaz de disponibilizar informações e eventos, no mínimo, pelos seguintes métodos:

3.1.8.1.1 API - *Application Programming Interface* - baseada em serviços web (REST/JSON) para consumo *on-line*;

3.1.8.1.2 Envio de mensagens dos eventos por email via protocolo SMTP - *Simple Mail Transfer Protocol*;

3.1.8.1.3 Envio da relação dos eventos por arquivo TXT/CVS através do protocolo SFTP - *Secure File Transfer Protocol*.

3.1.9 Segurança

3.1.9.1 O *login* de usuário para acesso à console de gerenciamento deverá ser autenticado com no mínimo dois fatores;

3.1.9.1.1 A autenticação por dois fatores pode ser implementada pelo uso de SSL/TLS mutuamente autenticado com uso de certificado digital (algo que o usuário possui) e confirmado pelo uso de senha (algo que o usuário conhece);

3.1.9.2 A PROPONENTE deve garantir que a infraestrutura disponibilizada para download e atualização dos softwares seja protegida contra ataques à infraestrutura tecnológica e que os pacotes de software a serem distribuídos aos usuários não sejam adulterados por terceiros;

3.1.9.3 Os pacotes executáveis do software de instalação devem ser assinados digitalmente pela PROPONENTE, no padrão exigido por cada sistema operacional, antes da distribuição para os usuários finais, para garantir a autenticidade da origem do software;

3.1.9.4 O software de instalação deve proteger a desinstalação do componente de proteção de dispositivo com validação de interação humana (por exemplo, com uso de captcha), para assegurar que o próprio usuário solicitou a desinstalação;

3.1.9.4.1 O código único para identificação de dispositivo gerado pelo componente de proteção de dispositivo deve ter proteção contra colisão que seja capaz de identificar o dispositivo como único em todo o universo de dispositivos protegidos e identificados pela componente de proteção de dispositivo;

3.1.9.5 A API de integração online do componente gerenciador de eventos deve ser protegida por SSL/TLS mutuamente autenticado (HTTPS).

3.1.10 Capacidade e Performance

3.1.10.1 A SOLUÇÃO deve ser capaz de atender, no mínimo, os seguintes conjuntos de usuários:

3.1.10.1.1 Clientes Pessoa Física em Canais Web:

3.1.10.1.1.1 Doze (12) milhões de usuários em potencial;

3.1.10.1.1.2 Um (01) milhão de usuários únicos diários;

3.1.10.1.1.3 Quatro (04) milhões de usuários únicos mensais.

3.1.10.1.2 Clientes Pessoa Física em Canais Mobile:

3.1.10.1.2.1 Cinco (05) milhões de usuários únicos mensais.

3.1.10.1.3 Clientes Pessoa Jurídica em Canais Web:

3.1.10.1.3.1 Cinco (05) milhões de usuários em potencial;

3.1.10.1.3.2 Dois (02) milhões de usuários únicos diários;

3.1.10.1.3.3 Três (03) milhões de usuários únicos mensais.

3.1.10.1.4 Usuários internos:

3.1.10.1.4.1 Duzentos (200) mil usuários totais, aptos a acessarem diariamente.

3.1.11 A PROPONENTE deve ser capaz de suportar crescimento do número de usuários, sem incorrer em aumento do custo para a CONTRATANTE, durante o prazo do contrato de suporte;

3.1.12 A SOLUÇÃO deve ser capaz de efetuar a distribuição de instalação para todos os usuários do componente de proteção de dispositivo, de acordo com os públicos alvo e cronogramas definidos pela CONTRATANTE;

3.1.13 A SOLUÇÃO deve ser capaz de efetuar a distribuição de atualizações de configuração em até 300 minutos para todos os dispositivos que tenham o componente de proteção de dispositivo instalado e estejam aptos ao recebimento da atualização;

3.1.14 A SOLUÇÃO deve ser capaz de efetuar a distribuição de atualizações de proteção em até 12 horas para todos os dispositivos que tenham o componente de proteção de dispositivo instalado e estejam aptos ao recebimento da atualização;

3.1.15 As funcionalidades de proteção do componente de proteção de dispositivo não podem acrescentar latência perceptível para os usuários em suas interações com os aplicativos da CONTRATANTE, devendo estar limitado a um acréscimo máximo de 100 milissegundos, incluindo a requisição e a resposta da interação;

3.1.16 As funcionalidades de detecção do componente de detecção de anomalias web não podem acrescentar latência perceptível para os usuários em suas interações com os aplicativos da CONTRATANTE, devendo estar limitado a um acréscimo máximo de 200 milissegundos, incluindo a requisição e a resposta da interação;

3.1.17 O componente gerenciador de eventos deve ser capaz de responder às consultas *online* para obtenção do índice de risco em um tempo máximo de 200 milissegundos, incluindo a requisição e a resposta da API de integração;

3.1.18 O componente gerenciador de eventos deve ser capaz, de enviar os eventos de alerta coletados em tempo real (*online*) para a CONTRATANTE.

4 Prestação de serviços de suporte técnico operacional

4.1.1 Prestação dos Serviços

4.1.1.1 A prestação de serviços para a solução compreende, no mínimo:

4.1.1.1.1 Assistência técnica operacional no local com, no mínimo 2 (dois) técnicos residentes para apoiar continuamente a equipe técnica do CONTRATANTE em período de 8 x 5 (oito horas por dia, cinco dias por semana), compreendendo as seguintes atividades:

4.1.1.1.1.1 Oferecer suporte presencial aos técnicos do CONTRATANTE;

4.1.1.1.1.2 Apoiar o monitoramento dos eventos gerados pela solução;

4.1.1.1.1.3 Diagnosticar ataques;

4.1.1.1.1.4 Auxiliar na operacionalização da solução.

4.1.1.1.2 Prestar todo tipo de suporte necessário aos usuários finais quanto ao adequado uso, manutenção, atualização, configuração, instalação e/ou remoção da SOLUÇÃO em suas estações, dentro dos prazos estabelecidos no Acordo de Nível de Serviços.

4.1.1.1.3 Compartilhar informações para apoiar o CONTRATANTE na gestão de risco e gestão operacional de todo processo de combate às fraudes eletrônicas;

4.1.1.1.4 Compartilhar conhecimento sobre ataques e ameaças digitais;

4.1.1.1.5 Apoiar no estabelecimento de regras táticas de forma a identificar transações potencialmente suspeitas de serem fraudulentas.

4.1.1.1.6 Possuir suporte técnico de segundo nível "*on-site*" e/ou suporte técnico remoto para utilização pelos técnicos do CONTRATANTE, de acordo com os parâmetros estabelecidos no Acordo de Nível de Serviços.

4.1.1.1.7 A PROPONENTE deverá prestar o serviço de suporte especializado com profissionais que apresentem a seguinte qualificação:

4.1.1.1.7.1 Experiência na análise e elaboração de regras para prevenção de fraude;

4.1.1.1.7.2 Experiência na implantação e/ou operacionalização de solução antifraude para instituições financeiras;

4.1.1.1.7.3 Domínio em ferramentas de mineração de dados.

4.1.1.1.8 Fornecer manutenção das tecnologias que compõem a SOLUÇÃO, geralmente denominado como "*upgrades*", com a sua garantia limitada ao escopo das funcionalidades da solução, com vistas a:

4.1.1.1.8.1 Mantê-la disponível;

4.1.1.1.8.2 Corrigir suas falhas;

4.1.1.1.8.3 Melhorar seu desempenho;

4.1.1.1.8.4 Adequá-la aos novos requisitos e melhorias de seus processos funcionais decorrentes das evoluções tecnológicas e computacionais impulsionadas pelo mercado;

4.1.1.1.8.5 Manter as proteções da SOLUÇÃO atualizadas, sempre que novas técnicas de ataque forem identificadas pela PROPONENTE e/ou pelo CONTRATANTE;

4.1.1.1.8.6 Atualizar as versões dos componentes utilizados pela solução.

4.1.1.1.9 Realizar otimizações e adequações contínuas na SOLUÇÃO de forma que a mesma se mantenha robusta e compatível com as necessidades do CONTRATANTE face ao movimento do cenário dos ataques digitais e necessidades operacionais ou de infraestrutura;

4.1.1.1.10 Manter continuamente atualizada a base de conhecimento para a defesa e respostas a incidentes de segurança decorrentes das novas ameaças que atacam o setor financeiro como um todo, ou as ameaças dirigidas diretamente contra as aplicações Web e/ou Java do CONTRATANTE;

4.1.1.1.11 Por sugestão do CONTRATANTE, estudar e implementar quando julgado pertinente, novas funcionalidades para a SOLUÇÃO e adaptá-las em função de sua estratégia de segurança e combate à fraude ou necessidade de conformação com as alterações na infraestrutura tecnológica, sem que isso implique em reajuste dos valores contratados;

4.1.1.1.12 Implementar todas as atualizações necessárias, inclusive de caráter preventivo quanto às possíveis novas modalidades de ataques ou artefatos maliciosos, fruto das pesquisas e técnicas de combate produzidas pela PROPONENTE, que visem a melhor proteção contra as ameaças dirigidas ao CONTRATANTE;

4.1.1.1.13 Fornecer documentação inicial e, sempre que for efetuada manutenção, atualização, configuração e versionamento dos componentes da SOLUÇÃO, com as especificações técnicas da SOLUÇÃO, bem como uma matriz correspondente à todas as proteções e suas funcionalidades, por sistemas operacionais, inclusive com informação de ativação ou não dos recursos em produção.

4.1.1.2 Serviço de análise particularizada de artefatos maliciosos que ataquem o CONTRATANTE, consistindo em:

4.1.1.2.1 Efetuar a engenharia reversa de cada artefato;

4.1.1.2.2 Decifrar a técnica utilizada para tentar violar quaisquer componentes da solução, por cada artefato analisado;

4.1.1.2.3 Desenvolver metodologias de proteção aos componentes da solução e ao acesso a aplicação Web e ou Java para cada nova técnica identificada e utilizada pelos artefatos analisados.

5 Condições de Entrega e instalação:

5.1 A entrega da SOLUÇÃO e suas respectivas licenças deverão ser realizadas pela PROPONENTE na Unidade de Risco Operacional (URO), em Brasília-DF, localizada no endereço abaixo, no horário compreendido entre 8h e 18h, em dias úteis, de segunda a sexta-feira: SBS QUADRA, 1 BLOCO G LOTE 32, CEP 70073901, Brasília (DF).

5.2 Juntamente com a SOLUÇÃO, deverão ser entregues, impressos e em formato eletrônico (CD/DVD), quatro (04) conjuntos completos da documentação técnica e dos manuais técnicos, em língua portuguesa do Brasil, de todos os softwares e/ou componentes que integram a SOLUÇÃO, com a descrição de uso, instalação, administração, operação, integração e funcionalidades.

5.3 A PROPONENTE deve permitir ao Banco do Brasil a reprodução dos manuais para uso interno.

6 Condições de Implementação:

6.1 A PROPONENTE, no momento da RFP, deverá comprovar que possui *expertise* e *know how*, restando amplamente capacitada e habilitada, através de contratos de fornecimento de produtos/serviços de mesma natureza, finalidade e complexidade, anteriormente firmados junto ao mercado nacional e/ou internacional, preferencialmente em empresas do ramo financeiro/bancário e/ou de grande porte.

6.2 Satisfeita a condição do item anterior, deverá a PROPONENTE apresentar as características do(s) produto(s) e da prestação de serviços, detalhando todos os recursos, de qualquer natureza (física, lógica, etc.), necessários a implantação e implementação da sua solução completa, em produção, inclusive em relação à integração com os recursos tecnológicos do CONTRATANTE (sistemas legados) observando-se ainda todas as demais condições abaixo descritas, em caráter não exaustivo:

6.2.1. Comprovar que possui toda documentação original, referente o objeto desta RFP, especificação técnica, projeto de implantação, implementação, operacionalização, customização, atualização, manutenção e desinstalação ou descarte, em mídia impressa e digital, em português do Brasil;

6.2.2. Comprovar que possui todos os recursos necessários para suportar o CONTRATANTE na implantação, implementação, operacionalização, customização, atualização, manutenção e desinstalação ou descarte da solução, com disponibilidade integral - todos os dias, 7 dias por semana (24h x 7) - tanto para o desenvolvimento e homologação quanto para o ambiente de produção;

6.2.3. Constitui prerrogativa exclusiva do CONTRATANTE o estabelecimento de prazos, períodos e momentos mais oportunos e adequados para implantação e implementação da SOLUÇÃO, devendo a PROPONENTE permanecer sempre em condições de atender às necessidades do CONTRATANTE, observados todos os requisitos contidos neste documento;

6.2.4. A possível dilação de prazos pelo CONTRATANTE não configurará ou constituirá direito à PROPONENTE em apresentar e entregar os recursos necessários a implantação e implementação da sua solução completa, em homologação e/ou produção, fora do prazo máximo e improrrogável de 75 (setenta e cindo) dias corridos para homologar, e mais 45 (quarenta e cinco) dias corridos para entrada definitiva em produção, contados da data de assinatura do contrato e observadas as demais condições indispensáveis deste projeto.

6.2.5. A PROPONENTE deverá apresentar seu cronograma de implantação e implementação da SOLUÇÃO, observadas as seguintes condições:

6.2.5.1 A homologação da SOLUÇÃO e de todo seu processo técnico-operacional deverá ocorrer antes da assinatura do contrato de aquisição/contratação, devendo a PROPONENTE estar completamente capacitada e habilitada para executá-la no prazo máximo de 75 (setenta e cinco) dias corridos, contados do completo encerramento do processo licitatório e da assinatura do Termo de Responsabilidade e de Homologação de Produto/Solução a ser Adquirido/Contratada;

6.2.5.2 A homologação deverá ser efetuada em até duas aplicações do Autoatendimento pela Internet do CONTRATANTE, a critério deste, podendo ser inclusive mobile, devendo a PROPONENTE fornecer e disponibilizar todo e qualquer suporte necessário à implantação, implementação, operacionalização, customização, atualização, manutenção e desinstalação ou descarte, em tempo integral, destinada:

6.2.5.2.1 Desenvolvimento, adição e/ou complemento ou adequação de códigos das aplicações, no prazo máximo de 30 (trinta) dias corridos;

6.2.5.2.2 Configuração e/ou customização de infraestrutura, inclusive para banco de dados e rede física ou lógica, dentro dos mesmos 30 (trinta) dias corridos do item anterior;

6.2.5.2.3 Treinamento e capacitação de técnicos e gestores do CONTRATANTE sobre as principais funcionalidades da SOLUÇÃO e para acesso, operacionalização, customização, atualização, manutenção e desinstalação da sua Console de Gerenciamento, também dentro dos mesmos 30 (trinta) dias corridos dos itens anteriores;

6.2.5.2.4 Distribuição da SOLUÇÃO junto ao público alvo de clientes/usuários definido pelo CONTRATANTE, durante o prazo de 15 (quinze) dias, iniciando após a efetiva conclusão dos 3 itens anteriores, com utilização de infraestrutura tecnológica da PROPONENTE;

6.2.5.2.5 Acompanhamento de toda e qualquer possível ocorrência junto ao suporte técnico do CONTRATANTE, durante o prazo de 30 (trinta) dias corridos, no mínimo, prorrogável por igual período à critério do CONTRATANTE, iniciando no dia seguinte ao primeiro dia de distribuição da SOLUÇÃO;

6.2.5.2.6 Após a distribuição da SOLUÇÃO, mesmo que somente para uma parcela reduzida de usuários finais, ocorrendo fraudes eletrônicas via computadores, smartphones ou tablets de clientes/usuários do Autoatendimento na Internet do CONTRATANTE, que possuam ou possuíam a SOLUÇÃO em homologação instalada na data e no momento da fraude, deverá a PROPONENTE, sob demanda e supervisão do CONTRATANTE, efetuar a análise dos *modus operandi* e apresentar por escrito, em seu papel timbrado, a devida justificativa/resposta para a possível ou provável ineficiência da SOLUÇÃO, ainda que parcial, no prazo máximo de 3 (três) dias

corridos, contados da notificação com as informações das fraudes pelo CONTRATANTE, o que poderá ocorrer por e-mail e/ou via impressa, com o devido protocolo de recebimento;

6.2.5.2.6.1 A notificação supra citada poderá ser emitida pelo CONTRATANTE em qualquer momento do processo de homologação, assim como, durante toda a vigência do contrato, se efetiva e formalmente celebrado;

6.2.5.2.6.2 A ausência de justificativa/resposta à notificação no prazo acima estipulado carretará a imediata desclassificação da PROPONENTE, considerando que não atende aos requisitos técnicos funcionais mínimos descritos neste projeto;

6.2.5.2.7 A justificativa/resposta descrita no item anterior não necessariamente eliminará/descartará a PROPONENTE, mas será determinante para aplicação de multa/sansão prevista em Acordo de Nível de Serviço (ANS) a ser constituído entre CONTRATANTE e PROPONENTE, nos termos descritos neste projeto.

6.2.5.3 Homologada a SOLUÇÃO, ou seja, verificada que atende ao objeto deste projeto, tanto nos requisitos funcionais como não funcionais, deverá esta ser disponibilizada, à critério do CONTRATANTE, para as demais aplicações de Autoatendimento via Internet, inclusive mobile, seja para pessoa física ou jurídica, correntista ou não correntista.

6.2.5.4 A assinatura do contrato de aquisição/contratação só ocorrerá se o todo o processo de homologação for concluído com sucesso e, caso essa condição não se verifique, deverá ser acionada a SEGUNDA PROPONENTE melhor classificada no processo licitatório, reiniciando os procedimentos de homologação.

6.2.5.5 Superada com sucesso a homologação da SOLUÇÃO, efetivada a aquisição/contratação, durante a vigência do contrato a PROPONENTE permanecerá prestando todo o suporte, de qualquer natureza, para a implantação, implementação operacionalização, customização, atualização, manutenção e desinstalação ou descarte da SOLUÇÃO em toda e qualquer aplicação do CONTRATANTE do Autoatendimento pela Internet, em efetiva produção, ainda que novas aplicações sejam desenvolvidas e disponibilizadas.

7 Condições de Garantia, Assistência Técnica, Manutenção e Suporte Técnico

7.1 O PROPONENTE concederá garantia integral on-site, assistência técnica, manutenção e suporte técnico da SOLUÇÃO, incluindo as mídias das licenças e dos manuais, pelo prazo total contratado de 60 (sessenta) meses contados da data de aceite da implementação.

7.2 A garantia da SOLUÇÃO será prestada pelo PROPONENTE de forma integral.

7.3 O PROPONENTE prestará manutenção e suporte técnico à SOLUÇÃO e seus componentes, bem como às licenças de software, que incluem os ajustes e correções necessárias a seu pleno funcionamento, correções de bugs e dúvidas relacionadas à instalação, bem como sua atualização tecnológica.

7.4 O PROPONENTE deverá implementar correções tempestivas a problemas relacionados a disponibilidade ou técnicas de proteção (contra novas técnicas de ataques, novas ameaças, *malwares*, vulnerabilidades, etc) verificados em quaisquer dos componentes da SOLUÇÃO, sem qualquer custo adicional para o Banco do Brasil.

7.5 Durante os períodos de garantia técnica e de manutenção e suporte técnico, o PROPONENTE deverá garantir a evolução tecnológica da SOLUÇÃO, entendida como a disponibilização de novas versões/releases, as correções de erros, novas técnicas de proteção e as adequações necessárias para atender determinações legais e de órgãos reguladores, com a respectiva documentação técnica, quando aplicável.

7.6 O PROPONENTE deverá garantir a compatibilidade das novas versões com as anteriores, mantendo as customizações existentes, bem como o reaproveitamento das parametrizações que porventura sejam efetuadas durante o uso da SOLUÇÃO.

7.7 Em caso de alteração de versão de software fornecido na SOLUÇÃO integrada que implique em deformação ou inabilitação de funcionalidades, o PROPONENTE executará as alterações necessárias ao atendimento de todos os requisitos descritos neste documento, sem qualquer custo adicional para o Banco do Brasil.

7.8 A PROPONENTE deve comunicar formalmente a CONTRATANTE a mudança de qualquer funcionalidade que implique em versionamento no protocolo de INTEGRAÇÃO entre os componentes da SOLUÇÃO e os sistemas da CONTRATANTE com no mínimo 90 (noventa) dias de antecedência.

7.9 A PROPONENTE deve comunicar formalmente a CONTRATANTE qualquer versionamento que implique em mudança na experiência do usuário com no mínimo 60 (sessenta) dias de antecedência.

7.10 Os serviços de garantia técnica e de manutenção e suporte técnico devem cobrir todas as adequações que forem feitas na SOLUÇÃO durante a vigência do contrato, sejam elas decorrentes de determinações legais e de órgãos reguladores ou de evolução tecnológica.

7.11 O PROPONENTE assegura que a SOLUÇÃO, quando utilizada nos dispositivos e ambientes especificados, funcionará em conformidade com as especificações.

7.12 Durante os períodos de garantia técnica e de manutenção e suporte técnico, o PROPONENTE compromete-se a eliminar erros detectados no software que impeçam seu pleno funcionamento, de acordo com as especificações exigidas neste Projeto Básico, sem qualquer ônus adicional para o Banco do Brasil.

7.13 O CONTRATANTE reserva-se o direito de efetuar integração da SOLUÇÃO a outras soluções, de software ou de hardware, desenvolvidas internamente ou adquiridas de outros fornecedores. Desde que tal iniciativa não implique em incompatibilidade com a solução, a PRONENTE não poderá, sob qualquer hipótese ou pretexto, eximir-se ou desobrigar-se da prestação da garantia técnica, dos serviços de manutenção e suporte técnico e demais compromissos previstos.

7.14 O suporte técnico do PROPONENTE deverá disponibilizar os seguintes serviços para a abertura de chamado, esclarecimento de dúvidas e SOLUÇÃO de problemas, no horário compreendido entre 08:00 e 20:00 horas, em dias úteis, inclusive feriados locais, de segunda a sexta-feira, durante o período de vigência contratual:

7.14.1. Atendimento via telefone (serviço 0800 ou local), em português;

7.14.2. Atendimento pela Internet via e-mail ou através de formulário WEB, em português (Brasil) ou inglês (EUA); em qualquer caso, as informações prestadas para a abertura do chamado, contidas nos e-mails ou nos formulários WEB, serão em Português (Brasil);

7.14.3. Caso sejam utilizados formulários WEB para a abertura de chamados, o PROPONENTE deverá informar a URL completa e, se for o caso, senha para autenticação, no ato de assinatura do contrato;

7.14.4. Atendimento *on-site*, que deverá disponibilizar profissional com perfil técnico para suporte da SOLUÇÃO objeto deste Projeto Básico, nas dependências do Banco do Brasil, em Brasília (DF);

7.14.5. A critério do Banco do Brasil poderá ser solicitada ao PROPONENTE a substituição do profissional do atendimento on-site.

7.15 Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem de tempo de atendimento a partir do momento de acionamento.

7.16 Os problemas serão classificados de acordo com as criticidades abaixo definidas:

7.16.1. Prioridade 1: chamados referentes a situações de emergência ou problema crítico, caracterizados pela paralisação total ou parcial, problemas de performance ou de segurança;

7.16.2. Prioridade 2: chamados associados a situações de erros, falhas ou defeitos onde o usuário não pode contornar a falha;

7.16.3. Prioridade 3: chamados associados a situações de erros, falhas ou defeitos onde o usuário pode contornar a falha, ou associados a situações onde o problema se apresente de forma intermitente;

7.16.4. Prioridade 4: chamados associados a situações de erros, falhas ou defeitos que não impedem o uso das funcionalidades do sistema, ou chamados com objetivo de formular perguntas para sanar dúvidas quanto ao uso ou à implementação do produto.

7.17 O PROPONENTE deve solucionar os problemas causados por inoperância e/ou mau funcionamento da SOLUÇÃO, seja por apontamento da CONTRATANTE, um de seus clientes ou, identificados pela PROPONENTE, de acordo com o nível de Prioridade e as condições abaixo:

7.17.1. Prioridade 1:

7.17.1.1 Os chamados de Prioridade 1 serão atendidos em no máximo 1 (uma) hora após a sua abertura e contarão com esforço concentrado do PROPONENTE com vistas a solução em até 2 (duas) horas após a abertura do chamado;

7.17.1.2 O atendimento de Prioridade 1 não poderá ser interrompido até o completo restabelecimento do serviço envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

7.17.2. Prioridade 2:

7.17.2.1 Os chamados de Prioridade 2 serão atendidos em no máximo 2 (duas) hora após a sua abertura e contarão com esforço concentrado do PROPONENTE com vistas a resolução em até 4 (quatro) horas após a abertura do chamado;

7.17.2.2 O atendimento de Prioridade 2 não poderá ser interrompido até o completo restabelecimento do serviço envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

7.17.3. Prioridade 3:

7.17.3.1 Os chamados de Prioridade 3 serão atendidos em no máximo 12 (doze) horas após a sua abertura e contarão com esforço concentrado do PROPONENTE com vistas a resolução em até 24 (vinte e quatro) horas após a abertura do chamado;

7.17.3.2 O atendimento de Prioridade 3 não poderá ser interrompido até o completo restabelecimento do serviço envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

7.17.4. Prioridade 4:

7.17.4.1 Os chamados de Prioridade 4 serão atendidos em no máximo 24 (vinte e quatro) horas após a sua abertura e contarão com esforço concentrado do PROPONENTE com vistas a resolução em até 48 (quarenta e oito) horas após a abertura do chamado.

7.18 Por necessidade de serviço, o Banco do Brasil também poderá solicitar a reclassificação de chamado para níveis superiores de prioridades. Os prazos dos chamados escalados passam a contar do início novamente.

7.19 Em todos os níveis de prioridade, se o problema for solucionado por meio de correção provisória, para qualquer nível de criticidade, o PROPONENTE deverá apresentar ao Banco do Brasil, num prazo de até 10 (dez) dias úteis, um plano de ação para a solução definitiva.

7.20 O monitoramento do atendimento dos chamados será efetuado pelo Banco do Brasil, observando:

7.20.1. Todos os chamados serão controlados por sistema de informação do PROPONENTE, no qual o Banco do Brasil terá acesso de consulta para acompanhamento e verificação;

7.20.2. Para efeito de acompanhamento das providências e do tempo decorrido desde a sua abertura, o Banco do Brasil será informado sobre cada abertura e fechamento de chamado;

7.20.3. O fechamento do chamado poderá se dar pela aplicação de correção ao produto ou pela aplicação de medida alternativa de contorno que possibilite a operação do sistema;

7.20.4. A entrega de medida corretiva definitiva poderá, a critério do PROPONENTE, vir a ser incorporada em futuras versões do software;

7.20.5. Um chamado fechado sem anuência do Banco do Brasil ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado;

7.20.6. Em caso do não restabelecimento do serviço envolvido durante o horário comercial, o atendimento poderá se estender pelo período noturno e/ou dias não úteis, sem ônus para o Banco do Brasil, sempre que ocorrer uma das seguintes situações:

7.20.6.1 Receber uma mensagem de erro e não conseguir solucionar a ocorrência com base nas instruções contidas em documentação fornecida;

7.20.6.2 Surgirem dúvidas que não possam ser esclarecidas através das informações contidas na documentação fornecida;

7.20.6.3 O produto não estiver funcionando conforme definido na documentação.

7.21 O PROPONENTE deverá emitir relatórios ou disponibilizar os dados referentes à prestação dos serviços incluindo informações sobre a disponibilização de novas versões sempre que solicitados.

7.22 O PROPONENTE deverá enviar ao Banco do Brasil, quando requerido, relatórios de todas as intervenções realizadas, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências.

7.22.1. Serviço complementar à ação das tecnologias de software que compõem a solução, transferindo para o CONTRATANTE conhecimento especializado sobre as tecnologias e metodologia de análise dos dados que possam apoiar a detecção, a identificação e apontar indícios de ataques de forma a viabilizar tratamento de detecção e prevenção para as ocorrências em andamento e ações preventivas visando evitar novas ocorrências, compreendendo, pelo menos, as seguintes atividades:

7.22.1.1 Compartilhar informações para apoiar o CONTRATANTE na gestão de risco e gestão operacional da SOLUÇÃO;

7.22.1.2 Transferir conhecimento sobre ataques digitais;

7.22.1.3 Apoiar no estabelecimento de regras táticas de forma a identificar risco em transações anômalas.

7.22.2. A PROPONENTE deverá prestar o serviço de suporte especializado com profissionais que apresentem a seguinte qualificação:

7.22.2.1 Experiência na análise de ataques e risco em transações anômalas;

7.22.2.2 Experiência na implantação e/ou operacionalização de solução antifraude para instituições financeiras;

7.22.3. Serviço de manutenção das tecnologias que compõem a SOLUÇÃO geralmente denominadas como atualização ou "*upgrade*", com a sua garantia limitada ao escopo das funcionalidades da solução, com vistas a:

7.22.3.1 Mantê-la disponível;

7.22.3.2 Corrigir suas falhas;

7.22.3.3 Melhorar seu desempenho e usabilidade;

7.22.3.4 Adequá-la aos novos requisitos e melhorias de seus processos funcionais decorrentes das evoluções tecnológicas e computacionais impulsionadas pelo mercado;

7.22.3.5 Atualização da proteção sempre que novas técnicas de ataque forem descobertas;

7.22.3.6 Atualização de versão dos softwares utilizados pela solução.

7.22.3.7 Realizar otimizações e adequações contínuas na ferramenta de forma que a SOLUÇÃO se mantenha robusta e compatível com as necessidades do CONTRATANTE face ao crescimento e evolução dos ataques digitais e necessidades operacionais ou de integração;

7.22.3.8 Manter continuamente atualizada a base de conhecimento para a defesa e respostas a incidentes de segurança decorrentes das novas ameaças que atacam o setor financeiro como um todo, ou as ameaças dirigidas diretamente contra as interfaces de canal *web* ou *mobile* do CONTRATANTE;

7.22.3.9 Por sugestão do CONTRATANTE, estudar e implementar quando julgado pertinente, novas funcionalidades para a solução e adaptá-las em função de sua estratégia de segurança e combate à ataques digitais ou necessidade de integração com novas tecnologias adotadas pela CONTRATANTE, sem que isso implique em reajuste dos valores contratados;

7.22.3.10 Implementar todas as atualizações necessárias, inclusive de caráter preventivo quanto às possíveis novas modalidades de ataques ou artefatos maliciosos, fruto das pesquisas e técnicas de combate produzidas pela PROPONENTE, que visem a melhor proteção contra as ameaças dirigidas ao CONTATANTE.

7.22.4. Serviço de análise particularizada de artefatos maliciosos que ataquem o contratante, consistindo em:

7.22.4.1 Efetuar a engenharia reversa de cada artefato;

7.22.4.2 Decifrar a técnica utilizada para tentar violar quaisquer componentes da solução, por cada artefato analisado;

7.22.4.3 Desenvolver metodologias de proteção aos componentes da solução e ao acesso a interfaces de canal web e mobile, para cada nova técnica identificada e utilizada pelos artefatos analisados.

7.23 A PROPONENTE deverá efetuar o ressarcimento ao CONTRATANTE das perdas ou prejuízos causados por má execução ou falha no serviço contratado.

8 Transferência de Tecnologia:

8.1 A PROPONENTE procederá, sob demanda do CONTRATANTE, sem ônus adicionais, à transferência de tecnologia abrangendo os requisitos especificados neste projeto básico, incluindo tipologias e modus operandi de ataques digitais, família de malwares, administração, operação e suporte técnico em cada um dos componentes das soluções licitadas, cujo agendamento se fará de comum acordo entre as partes.

8.2 Os eventos de transferência de tecnologia deverão iniciar-se após a entrega das soluções, conforme o cronograma a ser estabelecido de entre PROPONENTE e CONTRATANTE.

8.3 O CONTRATANTE poderá alterar o cronograma e o conteúdo da transferência de tecnologia caso julgue necessário para o melhor aproveitamento de seus funcionários, desde que dentro do escopo de requisitos especificados neste projeto básico.

8.4 O resultado da transferência de tecnologia será avaliado pelo CONTRATANTE. Caso não tenha alcançado o objetivo esperado, o evento deverá ser melhorado e realizado novamente, sem ônus adicionais para o CONTRATANTE.

8.5 A PROPONENTE será responsável pelo fornecimento de todo o material técnico e de suporte necessários à execução da transferência de tecnologia, sem qualquer ônus para o CONTRATANTE.

8.6 Todo conteúdo a ser transferido deverá ser realizado em português e o material didático deverá estar redigido em língua portuguesa e/ou inglesa.

8.7 O CONTRATANTE poderá, a seu critério, solicitar novos eventos extemporâneos de transferência de tecnologia em caso de alterações significativas nas funcionalidades da SOLUÇÃO ou em qualquer de seus componentes, decorrentes de mudança de versão ou atualização tecnológica.

8.8 A transferência de tecnologia será realizada em local adequado e indicado pelo CONTRATANTE.

9 Documentação Técnica:

9.1 A PROPONENTE deve apresentar a documentação:

9.1.1. Comprovação de que a PROPONENTE está autorizado a comercializar, licenciar/sublicenciar, instalar, no Brasil, os softwares objeto desta RFP, bem como a prestar serviços de garantia técnica e suporte para os referidos softwares.

9.1.2. Relação de todos os softwares e/ou componentes que da solução, contendo:

9.1.2.1 Fabricante: nome do Fabricante do(s) software(s);

9.1.2.2 Nome do produto: nome do(s) software(s)

9.1.2.3 Versão: versão do(s) software(s);

9.1.2.4 Procedência: procedência do(s) software(s) - país de origem;

9.1.2.5 Suporte: endereço da Internet (site) do Fabricante onde seja possível a obtenção de literatura técnica (especificações detalhadas, consumíveis, FAQ, etc.), últimas versões, patches, fixes, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo Banco do Brasil para o acesso, em língua portuguesa.

9.2 Juntamente com a entrega da solução, a PROPONENTE deve apresentar a documentação a seguir para a realização da avaliação técnica:

9.2.1. Documentação que contenha a descrição detalhada de todos os softwares e componentes da solução, através de folders, catálogos e manuais técnicos, que possam comprovar a adequação do produto com a especificação técnica.

9.2.1.1 Esta documentação deverá estar grifada com caneta tipo marca-texto, no local exato onde a característica técnica é mencionada.

9.2.2. PLANILHA DE VERIFICAÇÃO DE CONFORMIDADE TÉCNICA, que deverá:

9.2.2.1 Listar cada item desta especificação técnica e seu correspondente atendimento na documentação oficial da PROPONENTE, com o respectivo nome da publicação a página e o(s) parágrafo(s) onde estão atendidos os itens;

9.2.2.2 Ser emitida em papel que identifique a PROPONENTE (timbrado), conforme o exemplo abaixo:

Item	**Descrição**	**Documento**	**Página/Paragrafo**
X.X.X	Permitir a instalação do Sistema operacional XXXX	Manual XXX	XX/XX

10 Avaliação Técnica:

10.1 A avaliação técnica será realizada no horário compreendido entre 8h e 18h, em dias úteis, de segunda a sexta-feira, em local a ser definido pelo Banco do Brasil.

10.2 A critério do Banco do Brasil, a avaliação técnica poderá ser executada em dias não úteis e/ou fora do horário aqui definido, mediante acordo prévio entre as partes.

10.3 A PROPONENTE deverá preparar laboratório de demonstração ou ambiente de testes, no local indicado pelo Banco do Brasil, que contemple todos os componentes da SOLUÇÃO integrados, com o objetivo de demonstrar na prática cada um dos requisitos indicados na especificação técnica.

10.4 O Banco do Brasil avaliará as demonstrações executadas pela PROPONENTE, confrontando os resultados dos testes e demonstrações com os itens do edital e respectivas informações dos documentos técnicos indicadas na PLANILHA DE VERIFICAÇÃO DE CONFORMIDADE TÉCNICA, para verificar o atendimento de cada item da especificação técnica.

10.5 Caso algum item seja considerado não atendido pelo Banco, a PROPONENTE terá 5 (cinco) dias úteis para uma nova demonstração que comprove o atendimento dos itens.

10.6 Após esse prazo, e não demonstrando o atendimento, o Banco considerará que a SOLUÇÃO não atendeu aos itens do edital e que a PROPONENTE será desclassificado da concorrência.

10.7 É obrigatório o atendimento a todos os requisitos técnicos funcionais e não funcionais especificados neste projeto básico.

10.8 O não atendimento que qualquer requisito constituirá motivo suficiente para desconsideração da proposta encaminhada pela PROPONENTE e sua imediata desclassificação.

11 Precificação:

11.1 A PROPONENTE deverá apresentar proposta com preço fixo global;

11.2 A PROPONENTE deverá desmembrar os componentes do preço global, para fins referenciais, informando:

12 Condições de Pagamento:

12.1 O pagamento será feito por meio de crédito em conta corrente mantida pelo PROPONENTE no Banco do Brasil S.A., conforme abaixo:

12.2 O pagamento referente à cessão de direito de uso permanente do *software* e aos serviços de serviços de instalação, customização, implementação, treinamento, garantia, compreendendo atualização, manutenção e suporte técnico da Solução, será efetuado em até 10 dias corridos, contados da data de aceite de implementação.

12.3 O pagamento relativo à prestação dos serviços de suporte técnico operacional serão pagos em 60 (sessenta) parcelas mensais e consecutivas, contadas do mês subsequente ao aceite da implementação

13 Acordos de Nível de Serviço (ANS):

13.1 CONCEITOS PRELIMINARES

13.1.1. Atendimento do Chamado.

13.1.1.1. O atendimento do chamado corresponde à ação da **PROPONENTE** de receber a notificação da ocorrência reportada pela CONTRATANTE, fazer a análise preliminar e passar instruções também preliminares de como se deve proceder, até que o problema seja considerado resolvido.

13.1.1.2. O atendimento do chamado pode gerar uma Solução de Contorno ou a implementação de uma Solução Definitiva.

13.1.2. Escalada.

13.1.2.1. Escalada é o ato de invocar níveis hierárquicos crescentes com o objetivo de obter os tempos de resolução de incidentes desejados para correção de falhas que afetam ou podem afetar os processos e negócios da CONTRATANTE.

13.1.2.2. Os objetivos do processo de escalada são:

13.1.2.3 Efetuar um melhor gerenciamento dos problemas, dando maior visibilidade aos mesmos.

13.1.2.4. Assegurar que os recursos apropriados estão focados na obtenção dos compromissos de serviços.

13.1.2.5. Invocar os procedimentos de recuperação quando apropriado.

13.1.2.6. Alertar os grupos corretos dentro de cada organização para os problemas atuais dos serviços.

13.1.3. Severidade Alta.

13.1.3.1. Situação considerada de emergência ou problemas críticos, caracterizados pela existência de sistema parado (inoperante), funcionamento deficiente, problemas que estejam vulnerabilizando o sistema de segurança do Banco do Brasil, em qualquer um dos componentes da solução.

13.1.4. Severidade Média.

13.1.4.1. Situação de baixo impacto associado ao uso de qualquer um dos componentes da solução ou para aqueles problemas que se apresentam de maneira intermitente.

13.1.5. Severidade Baixa.

13.1.5.1. Acionamento tiver por objetivo formular perguntas com o objetivo de sanar dúvidas quanto ao uso ou à implementação de qualquer um dos componentes da solução.

13.1.6. Solução de Contorno.

13.1.6.1. A Solução de Contorno compreende quaisquer serviços que se fizerem necessários para obter o retorno das funcionalidades previstas para qualquer dos componentes da solução, devendo a **PROPONENTE** atender, nas condições ora estabelecidas, a todo e qualquer acionamento que venha a receber da CONTRATANTE, conforme os prazos estabelecidos neste documento.

13.1.6.2. A Solução de Contorno será aceita pela CONTRATANTE, desde que não impeça a solução, ou qualquer um de seus componentes, de funcionar normalmente, devendo ser substituída pela Solução Definitiva conforme os prazos acordados entre as partes para cada caso.

13.1.6.3. Entende-se como solução do problema pela implementação de uma Solução de Contorno, a restauração da solução ou um de seus componentes ao estado de funcionamento, mesmo que parcial, desde que não impeça a Aplicação Web, ou qualquer outro site protegido pela solução, de funcionar normalmente.

13.1.6.4. O tempo para a disponibilização pela PROPONENTE da Solução Definitiva do problema reportado será acordado entre as partes após a mensuração, pela PROPONENTE, de esforço para seu desenvolvimento e/ou implementação.

13.1.6.5. O prazo para a solução do problema será definido de acordo com a criticidade do problema estabelecida pela CONTRATANTE de comum acordo com a **PROPONENTE**.

13.1.7. Solução Definitiva.

13.1.7.1. A Solução Definitiva é a restauração da solução, ou de um de seus componentes, ao pleno estado de funcionamento.

13.1.7.2. Será aceito pela CONTRATANTE como Solução Definitiva, a disponibilização pela **PROPONENTE** de uma nova versão de qualquer um dos componentes da solução que venham a sanar o defeito ou mau funcionamento reportado.

13.1.7.3. Considera-se totalmente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma Solução de Contorno.

13.2. Objetivo

13.2.1. O objetivo deste Acordo de Nível de Serviço (ANS) é definir as responsabilidades e dependências entre a **PROPONENTE** e a CONTRATANTE para Serviços e Produtos de Tecnologia da Informação.

13.2.2. Os acordos operacionais previstos neste ANS não devem ter precedência nem limitar as respectivas obrigações e responsabilidades já descritas no contrato feito entre a CONTRATANTE e a **PROPONENTE**.

13.3. Aspectos do ANS

13.3.1. O ANS descreve como a CONTRATANTE e a PROPONENTE irão tratar seu relacionamento, para assegurar que os serviços serão corretamente entregues a CONTRATANTE.

13.3.2. Define os compromissos requeridos entre a PROPONENTE - como provedora de serviços e tecnologias - e a CONTRATANTE, para a entrega dos serviços contratados.

13.3.3. Servirá como ponto de referência e detalhamento sobre como cada parte irá operar e o que é esperado de cada uma das partes.

13.4. Obrigações da **PROPONENTE**

13.4.1. Manter a CONTRATANTE sempre informado de todas as versões e atualizações disponibilizadas pelo fabricante, entregando a documentação relativa à nova versão entregue.

13.4.2. Entregar ao CONTRATANTE em um prazo máximo de 5 (cinco) dias úteis, contados a partir do aceite da solicitação, nova versão e/ou atualização do

componente de segurança, bem como respectiva documentação descrevendo analiticamente as funcionalidades, alterações, correções e implementações da nova versão ou atualização entregue, inclusive com descrição de possíveis casos práticos.

13.4.3. Suprir a CONTRATANTE com bases de assinatura atualizadas diariamente.

13.4.4. Fornecer, sempre que solicitado, boletins técnicos e manuais de uso atualizados;

13.4.5. Tomar as providências cabíveis e imediatas para alterar o produto, caso sejam detectados erros no mesmo, que motivem a interrupção do processamento.

13.4.6. Não divulgar dados ou informações relacionadas aos serviços e produtos objeto do presente, mantendo sigilo absoluto em relação a todos os dados acessados ou que venham a ser gerados, no processo de prestação dos serviços.

13.4.7. Fornecer e manter a relação atualizada com nome e qualificação dos técnicos responsáveis pela execução do serviço nos ambientes da CONTRATANTE.

13.4.8. Emitir, para cada chamado, relatório técnico conclusivo da causa do problema e da solução que foi adotada para o seu restabelecimento.

13.5. Prazos de Atendimento

13.5.1. O atendimento, contado a partir do acionamento, será prestado de acordo com o nível de severidade definido para cada caso, conforme o quadro abaixo:

SEVERIDADE				
	Cliente	**Servidor**	**Cliente**	**Servidor**
ALTA	5 horas corridas	5 horas corridas	Próxima versão	Próxima versão
MÉDIA	72 horas corridas	72 horas corridas	Próxima versão	Próxima versão
BAIXA	120 horas corridas	120 horas corridas	Próxima versão	Próxima versão

Nota: Próxima versão, desde que não cause impacto operacional significativo.

13.5.2. A **PROPONENTE** poderá pedir a ampliação dos prazos acima em situações especiais e/ou imprevistas, desde que a justificativa apresentada seja aceita pelo CONTRATANTE.

13.5.3. O fechamento de um chamado técnico se dará com a concordância da CONTRATANTE com a solução apresentada, a qual terá o prazo de até 2 (dois) dias úteis para fazê-lo.

13.6. Obrigações da CONTRATANTE

13.6.1. Ao solicitar o Suporte Técnico, a CONTRATANTE deverá fazer previamente uma análise do problema, inclusive, apresentar um caso.

13.6.2. A CONTRATANTE fará os acionamentos (chamados) diretamente aos representantes da **PROPONENTE** informando o nível de severidade e repassando as explicações que vinculem o problema ao nível de severidade.

13.6.3. A CONTRATANTE deverá prover e manter um laboratório de testes em suas instalações com todos os recursos necessários à avaliação das novas versões e releases de qualquer um dos componentes da solução.

13.6.3.1. Este laboratório deverá ser configurado para abranger no mínimo a emulação dos cenários/ambientes descritos no item 2 deste projeto básico.

13.6.4. O tratamento das informações armazenadas na console de monitoração deverão ser realizadas diariamente pela CONTRATANTE, na mesma periodicidade que for definida a carga de dados.

13.6.5. A CONTRATANTE deverá homologar todos os componentes da SOLUÇÃO em um prazo máximo de 10 (dez) dias úteis, a contar da apresentação dos componentes.

13.6.6. É prerrogativa da CONTRATANTE não disponibilizar a versão para seus clientes, entretanto, todas as ocorrências dessa natureza deverão ser comunicadas à **PROPONENTE**, isentando-a de qualquer responsabilidade pela não publicação da versão.

13.6.7. Caso alguns clientes da CONTRATANTE tenham sidos lesados e os mesmos possuam o componente de segurança instalado, a CONTRATANTE deverá promover, por amostragem, visitas ao cliente, para diagnosticar a forma de operar dos fraudadores.

13.6.7.1. Constatando que sofreu um ataque por meio eletrônico, a CONTRATANTE deverá instruir imediatamente a **PROPONENTE** para que ela promova a defesa necessária, de caráter corretivo e preventivo.

13.6.8. Qualquer mudança na estrutura da Aplicação Web da CONTRATANTE, tais como: alteração e/ou inserção de novos IP's, Url's e layout´s, a **PROPONENTE** deverá ser notificada o mais rapidamente possível.

13.6.9. O prazo para a comunicação descrita no item anterior é de 5 (cinco) dias úteis a contar da constatação da necessidade de alterações na solução em decorrência destas mudanças.

13.6.10. A CONTRATANTE deverá registrar na console de monitoração todas as contas-correntes que foram lesadas.

13.6.11. A constatação da necessidade de alterações na solução poderá ser formalizada por qualquer uma das partes, conforme diagnóstico realizado pela CONTRATANTE ou pela **PROPONENTE**.

13.6.12. A CONTRATANTE compromete-se a apresentar mensalmente, ou quando solicitada, um quadro com a tendência dos resultados contabilizados em fraudes, baseado na quantidade de ataques no canal Internet que efetivamente geraram prejuízo para a CONTRATANTE. Esta medida tem como finalidade prover a **PROPONENTE** de meios para avaliar a efetividade de sua solução no ambiente da CONTRATANTE.

13.7. Penalidades e Multas

13.7.1. Poderão ser consideradas para efeito de multa as conseqüências sobre a tecnologia provocada pela ação de hackers no sentido de reduzir, comprometer parcialmente ou eliminar eficácia e eficiência da tecnologia, conforme apresentado no item 1 deste Acordo de Nível de Serviço - ANS.

13.7.2. A não apresentação de proposta de solução da ocorrência dentro do prazo estabelecido para acionamentos da severidade "ALTA" e desde que não seja acordado novo prazo de solução do problema ensejará a aplicação da multa. A cada 50% do tempo excedente será aplicado adicional de 0,1% contados a partir do final do prazo especificado na tabela de severidade e continua assim até que a ocorrência seja atendida ou que se atinja a limite estabelecido.

13.7.3. A não apresentação de proposta de solução da ocorrência dentro do prazo estabelecido para acionamentos das categorias de severidade "MÉDIA" e "BAIXA" e desde que não seja acordado novo prazo, ensejará a aplicação de multa de 5% (cinco por cento). Caso o atraso chegue a 50% do tempo excedente será aplicado adicional de 5% (cinco por cento) contados a partir do final do prazo especificado na tabela de severidade e continua assim até que a ocorrência seja atendida ou que se atinja a limite estabelecido.

13.7.4. O somatório das penalidades acima estão limitadas a 50% (cinco por cento) do valor da fatura mensal do mês em que se verificar a ocorrência.

13.7.5. Fica assegurado à PROPONENTE o direito ao contraditório e a ampla defesa.

13.7.6. As penalidades acima citadas serão aplicadas na fatura do mês em que se verificar a ocorrência ou em faturas a vencer caso o direito de defesa ainda não tenha sido julgado.

13.7.7. Caso a CONTRATANTE não disponibilize os recursos de infra-estrutura previamente acordados e necessários para execução do suporte, não haverá incidência de multas e penalidades para a PROPONENTE. O tempo de resolução somente será contabilizado a partir da disponibilização do ambiente e requisitos necessários para a prestação do serviço de suporte.

13.7.8. O atraso será contado a partir da comunicação da parte que detectar o inadimplemento.

13.8. Ressalvas

13.8.1. A qualquer momento, por iniciativa de qualquer uma das partes, poderá ser iniciado o processo de renegociação deste Acordo de Nível de Serviço - ANS.

13.8.2. A renegociação não significa a aceitação implícita de quaisquer condições, e deverá iniciar-se em um prazo máximo de 30 (trinta) dias corridos contados a partir da data de sua formalização.

13.8.3. Caso o prazo constante no item anterior não seja cumprido, significará, automaticamente, a continuidade das condições previamente acordadas pelas partes.

13.8.4. A solicitante do processo de renegociação poderá cancelar a solicitação a qualquer momento, e não será gerada qualquer penalidade por este cancelamento.

13.8.5. No cancelamento da solicitação de renegociação, automaticamente ocorrerá a continuidade das condições previamente acordadas pelas partes.

13.8.6. A renegociação das penalidades e das multas originará um novo documento assinado por representantes constituídos a ser anexado ao presente Acordo de Nível de Serviço - ANS.

14. Aspectos de Segurança:

14.1. Aspectos gerais de segurança

14.1.1. Os empregados, sócios, diretores e mandatários da empresa PROPONENTE, deverão manter total sigilo e confidencialidade dos serviços prestados ao Banco do Brasil no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados.

14.1.2. O PROPONENTE deverá respeitar as imposições relativas ao sigilo bancário.

14.1.3. O PROPONENTE deverá respeitar integralmente as normas de segurança estabelecidas pelo Banco do Brasil e atender os padrões de segurança e controle para acesso e uso das instalações e equipamentos do Banco do Brasil, zelando por sua integridade, mantendo sigilo e considerando confidenciais todos os dados e informações pertinentes aos serviços prestados.

14.1.4. A disponibilização de profissional para atendimento on-site estará sujeita às políticas de Gestão de Segurança do Banco do Brasil.

14.1.5. Os acessos às dependências e aos equipamentos do Banco do Brasil necessários ao suporte ou implantação da SOLUÇÃO deverão obedecer às normas de segurança utilizadas pelo Banco do Brasil.

14.1.6. O PROPONENTE gerenciará a segurança das informações e dados para restringir acessos não autorizados e deverá garantir que seus empregados e representantes estejam inteiramente cientes dos riscos associados com problemas inerentes à segurança da informação.

14.2. Sigilo

14.2.1. O PROPONENTE obriga-se por si, seus empregados, sócios, diretores e mandatários, a manter total sigilo e confidencialidade dos serviços prestados ao Banco do Brasil no que se refere a não divulgação, por qualquer meio, das informações ou documentos aos quais venha a ter acesso, em decorrência da prestação dos serviços executados por força do contrato. Também se compromete a respeitar as imposições relativas ao sigilo bancário as quais o Banco do Brasil está sujeita.

14.2.2. O PROPONENTE obriga-se a revelar as informações decorrentes deste documento, exclusivamente, a seus prepostos e funcionários diretamente envolvidos nas atividades objeto do contrato.

14.2.3. O PROPONENTE obriga-se, ainda, a respeitar integralmente as normas de segurança estabelecidas pelo Banco do Brasil e atender os padrões de segurança e controle para acesso e uso das instalações e equipamentos do Banco do Brasil, zelando por sua integridade.

14.2.4. Não serão considerados confidenciais quaisquer documentos, dados ou informações do presente documento, e informações de domínio público, que o PROPONENTE venha ter conhecimento lícito através de terceiros e aqueles que o Banco do Brasil vier a tornar públicos.

14.2.5. A obrigação das partes de não divulgação das informações tidas como sigilosas e confidenciais sobreviverá à rescisão do contrato, até que ocorra a liberação pela parte proprietária das informações, por determinação judicial ou pela ocorrência dos eventos indicados no contrato como liberadores dessa obrigação.

14.3. Acessos especiais

14.3.1. Nos casos em que forem imprescindíveis à prestação dos serviços objetos deste documento e por solicitação expressa do PROPONENTE, contendo as devidas justificativas, poderão ser concedidos, pelo Banco do Brasil e a seu exclusivo critério, os acessos lógicos a recursos tecnológicos do seu ambiente, para usuários externos, assim considerados os empregados do PROPONENTE.

14.3.2. Os acessos lógicos serão restritos aos dias da semana e horários de trabalho, constantes da solicitação do PROPONENTE, que deverão conter o nome do empregado, os dias da semana e os horários de entrada, saída e intervalo do empregado, além de serem concedidos pelo prazo máximo de 180 dias, devendo ser temporariamente suspensos nos casos de afastamentos superiores a 7 (sete) dias.

14.3.3. Nos casos de substituições ou afastamentos de empregados do PROPONENTE, definitivos ou temporários, este deverá comunicar ao Banco do Brasil com antecedência mínima de 2 dias úteis, bem como recolher e entregar os respectivos cartões de acesso e/ou crachás de identificação.

14.4. Crachás de Identificação e Atualização das Listas de Entrada

14.4.1. No término da vigência do contrato e em caso de sua rescisão, deverão ser devolvidos ao Banco do Brasil todos os elementos de identificação utilizados por empregados do PROPONENTE na prestação dos serviços.

14.4.2. O PROPONENTE obriga-se a fornecer ao Banco do Brasil o Termo de Responsabilidade do Usuário firmado junto ao Banco do Brasil, conforme modelo a ser fornecido, para cada um dos seus empregados que venham a participar da prestação dos serviços objetos do contrato.

14.4.3. O PROPONENTE obriga-se a solicitar autorização ao Banco do Brasil, por meio da Solicitação de Acessos Especiais para Terceiros, conforme modelo a ser fornecido, para os equipamentos e softwares de terceiros que, exclusivamente no interesse do serviço e previstos contratualmente, necessitem ser utilizados ou conectados logicamente aos recursos tecnológicos do Banco do Brasil.

15. VIGÊNCIA:

15.1 A vigência inicia-se na data de sua assinatura e se estenderá até o final do prazo de garantia.