

ANEXO IV

REQUISITOS DE ASSISTÊNCIA E SUPORTE TÉCNICO

O presente anexo descreve os requisitos relacionados à prestação de assistência e suporte técnico para os serviços especificados no Edital e demais Anexos, de modo a garantir a continuidade da prestação dos referidos serviços.

Todos os requisitos apresentados têm caráter obrigatório, devendo ser integralmente atendidos pelo CONTRATADO. O não atendimento a qualquer dos requisitos apresentados, no todo ou em parte, sujeitará os CONTRATADOS às sanções previstas em contrato, e às medidas legais cabíveis.

1 CARACTERÍSTICAS GERAIS DOS SERVIÇOS

1.1. Responsabilidades do CONTRATADO

O CONTRATADOS deverão oferecer como parte integrante dos serviços prestados, assistência e suporte técnico, na forma abaixo especificada, envolvendo todos os componentes fornecidos no escopo dos serviços ou necessários a sua execução, além de zelar pelo perfeito funcionamento dos demais recursos relacionados à prestação dos referidos serviços.

Os CONTRATADO deverão contribuir para a manutenção do pleno e correto funcionamento da solução fornecida, através das seguintes modalidades de atuação:

- **Pró-ativa:** Identificação de problemas potenciais, sugestão de melhorias e novas formas de implementação, análises quantitativas e qualitativas de utilização dos recursos, relatórios gerenciais e acompanhamento da prestação de assistência e suporte técnico;
- **Reativa:** Atendimento para implementação de funcionalidades suportadas e tomada de providências para contorno ou resolução de incidentes, notificando falhas nos serviços prestados quando ocorrer indisponibilidade, incompatibilidade entre comportamento observado e especificações técnicas, configurações inadequadas, ou outras circunstâncias na utilização da solução que ponham em risco, com qualquer grau de severidade, os negócios do BANCO, observando os níveis de serviços estabelecidos.

Todos os requisitos objetos desse Anexo deverão ser plenamente atendidos durante toda a vigência contratual e ocorrerão às expensas e inteira responsabilidade do CONTRATADO, sem nenhum ônus adicional para o BANCO, contada a partir da emissão do primeiro de aceite por parte do BANCO, seja ele o Termo de Aceite Provisório – TAP ou do Termo de Aceite Definitivo (TAD) para qualquer outro item da Implantação, inclusive no tocante aos seguintes aspectos:

- Deslocamento, hospedagem e alimentação de técnicos, inclusive residentes;
- Impostos, taxas, tarifas, seguros obrigatórios e demais despesas legais relacionadas à prestação dos serviços.

A CONTRATADA deve realizar todas as operações de administração, gerenciamento e monitoramento da ferramenta ofertada, incluindo, mas não se limitando a:

- Configuração dos módulos adquiridos, realizando a inserção/busca de ativos, customização de *scans* de vulnerabilidades, configuração de *scanners*, conectores e agentes etc;
- Interação com a equipe técnica do Banco do Nordeste responsável pela configuração de ferramentas que eventualmente se integrarão com a solução

ofertada, como, por exemplo, *firewalls*, *proxies*, *Microsoft Active Directory*, dentre outros;

- *Backup e restore*;
- Resolução de problemas;
- Suporte;
- Atualização, de acordo com as recomendações do fabricante;

A CONTRATADA deverá apresentar um conjunto de configurações pré-estabelecidas para ativação. Estas configurações somente serão implementadas após a aprovação do Banco do Nordeste;

A CONTRATADA é responsável pela execução de todas as atividades de gestão, manutenção, configuração, suporte e administração da ferramenta ofertada;

A CONTRATADA deve manter atualizados os módulos das soluções ofertadas, instalar patches, correções e versões ou releases mais recentes dos softwares, provisionamento dos serviços de configuração e implementação de facilidades de configuração para atualização ou modificação dos recursos lógicos dos módulos da solução, dentro do prazo de validade do contrato;

Durante todo o período do contrato, o Contratado obriga-se a substituir, recuperar e/ou modificar os softwares instalados, sem ônus de qualquer natureza ao Banco do Nordeste, nos casos comprovados de mau funcionamento, falhas de segurança e de outras falhas, de modo a ajustá-los aos resultados que atendam às especificações técnicas. O Contratado deverá comunicar ao Banco a descoberta de quaisquer problemas, bugs ou limitações presentes na solução imediatamente após a descoberta do problema;

A CONTRATADA deve executar procedimentos para fazer o ajuste fino (tunning) de toda a solução ofertada, adequando-a ao ambiente do Banco do Nordeste e realizando as customizações de configuração necessárias;

A CONTRATADA deve realizar a gerência de segurança da solução fornecida, sendo responsável pela proteção das informações, restringindo o acesso à rede e impedindo o uso incorreto por parte de seus usuários, de forma intencional ou não;

A CONTRATADA deve realizar as operações de administração da solução fornecida para solicitação de criação de contas de acesso para os analistas do Banco do Nordeste, solicitação de registros de auditoria da ferramenta ou outras configurações solicitadas pelo Banco do Nordeste. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

A CONTRATADA deve configurar os perfis de acesso diferenciados, necessários para que os analistas do Banco do Nordeste utilizem todos os serviços contratados. A CONTRATADA deve fornecer possibilidade de perfis que permitam acesso a qualquer informação armazenada na solução fornecida;

A CONTRATADA deve fornecer, sob demanda do Banco do Nordeste, relatório contendo a lista de usuários cadastrados na ferramenta, o perfil de acesso, situação da conta e última data de acesso;

A CONTRATADA deve utilizar analistas capacitados e certificados na solução de gestão de vulnerabilidades fornecida para realizar as atividades descritas;

A CONTRATADA deve definir em comum acordo com o Banco do Nordeste o método mais eficiente para a implementação das configurações a serem realizadas no sistema de gestão de vulnerabilidades, de forma a não prejudicar o trabalho dos colaboradores do Banco. O procedimento proposto só será aceito após avaliado pelo Banco do Nordeste;

A CONTRATADA deve realizar as configurações na solução fornecida, de forma proativa ou sempre que solicitada pelo Banco do Nordeste;

A CONTRATADA deve fornecer base de conhecimento de métricas, indicadores de comprometimento, atualizadas periodicamente de acordo com a mudança do cenário de ameaças, permitindo monitorar e analisar mudanças no comportamento do usuário, rede ou aplicações, que podem significar uma atividade suspeita;

O Banco do Nordeste pode solicitar, a qualquer momento, a implementação de novas configurações na solução fornecida, baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar as configurações na solução. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

O Banco do Nordeste não deve realizar a edição de configurações sem o conhecimento da CONTRATADA;

O Banco do Nordeste deve fornecer dados de inteligência de negócio, como subsídios para que a CONTRATADA possa otimizar todas as configurações a serem implementadas, de forma a melhor identificar as vulnerabilidades nos ativos da organização, obtendo uma avaliação de risco efetiva de modo que seja possível corrigi-los ou mitigá-los, reduzindo assim a exposição cibernética da organização. Os dados fornecidos serão os mínimos necessários para a atividade, respeitando todas as restrições impostas pela legislação vigente e normativos internos do Banco do Nordeste;

A CONTRATADA deve realizar a configuração dos dashboards e relatórios de monitoramento na solução fornecida, de forma proativa ou sempre que solicitada pelo Banco do Nordeste;

A CONTRATADA deve configurar um conjunto básico de dashboards, contendo indicadores definidos de acordo com suas bases de conhecimento próprias, customizadas para o ambiente do Banco do Nordeste;

O Banco do Nordeste pode solicitar, a qualquer momento, a implementação de dashboards ou relatórios para apresentar indicadores próprios definidos baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar os dashboards na solução. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

O Banco do Nordeste pode solicitar acesso a quaisquer dos dashboards ou relatórios configurados na ferramenta, de acordo com o nível de acesso que o Banco do Nordeste definirá para cada um de seus analistas autorizados a acessar a ferramenta fornecida;

O Banco do Nordeste pode solicitar perfil de acesso aos seus analistas que possibilitem a construção de dashboards e relatórios customizados, visualização e a filtragem dos eventos e alertas na ferramenta ofertada.

2 ACORDO DE NÍVEIS DE SERVIÇO

2.1 Disponibilidade

Expressa o percentual do tempo em que um serviço estará operacional durante o período no qual ele é prestado e mensurado sob condições normais, ou seja, obedecendo aos requisitos técnicos estipulados no Edital e em todos seus Anexos.

A disponibilidade do serviço indicará o percentual de tempo, durante cada mês e ano de operação, em que o serviço permanecer em condições normais de funcionamento.

O serviço será considerado indisponível a partir do início de uma interrupção registrada até o restabelecimento à condição normal de funcionamento e a respectiva informação ao BANCO.

Os serviços deverão estar disponíveis 24 horas por dia, 7 dias por semana, 365 (trezentos e sessenta e cinco) dias por ano. O prazo máximo para reparo/restabelecimento integral de qualquer funcionalidade do sistema de gerenciamento dos serviços de comunicação de dados será de **04 (quatro) horas corridas**.

2.2 Tempo de resposta a incidentes de segurança

Em caso de incidentes de segurança, o BANCO pode solicitar informações detalhadas sobre a vulnerabilidade encontrada. Isso inclui a natureza do incidente, a extensão do impacto, e as possíveis soluções e ações corretivas que serão implementadas para mitigar os riscos. A resposta aos incidentes de segurança deve ser rápida e eficiente, proporcionando ao BANCO as garantias necessárias de que a situação está sob controle e que medidas preventivas serão adotadas para evitar futuras ocorrências semelhantes.

Tempo de resposta a incidentes de segurança:

- 15 (quinze minutos) após a abertura do chamado para incidentes de alto risco.

Entende-se por alto risco uma falha crítica que pode ser explorada para comprometer significativamente a confidencialidade, integridade ou disponibilidade dos sistemas do BANCO, causando potencialmente grandes danos financeiros ou à reputação.

- 30 (trinta minutos) após a abertura do chamado para as demais ocorrências
- 24 (vinte e quatro) horas após abertura do chamado para esclarecimentos de dúvidas

A classificação dos chamados será de inteira discricionariedade do BANCO, que determinará a criticidade e prioridade de cada incidente ou solicitação conforme seus critérios internos.

2.3 Alteração de configuração

Alteração de configuração refere-se a quaisquer modificações realizadas nas configurações do sistema ou nas permissões de acesso, ajuste de perfis administrativos, personalização, ou atualização de parâmetros operacionais.

Estas solicitações deverão ser atendidas em **8 horas úteis**.

2.4 Configuração de dashboards

Solicitações de criação de gráficos e disponibilização de dashboards com novas métricas monitoradas devem ser atendidas em até **48 horas corridas**. Esta obrigação contratual visa garantir que as informações e indicadores necessários para o acompanhamento e análise dos serviços estejam sempre atualizados e acessíveis de forma clara e precisa, permitindo uma

tomada de decisão mais eficiente e informada por parte do CONTRATANTE. Além disso, a agilidade na atualização das métricas monitoradas é essencial para identificar rapidamente qualquer desvio ou necessidade de intervenção, assegurando a manutenção dos níveis de serviço acordados.

2.5 Configuração de relatórios

Os novos modelos de relatórios devem ser configurados de acordo com as necessidades específicas do CONTRATANTE, contemplando todas as variáveis e métricas acordadas previamente. O prazo para atendimento é de **5 dias corridos** após abertura de chamado

2.6 Atualizações de segurança

- **5 (cinco) dias:** Atualização da solução por meio da implementação de patches e fixes, incluído neste limite o tempo necessário à homologação do pacote pela contratada. Contados a partir da liberação da atualização pelo fabricantes
- **12 (doze) horas:** Atualização de bases externas de assinatura de ataques e vulnerabilidades divulgadas pelo fabricante ou por serviços especializados da CONTRATADA.

2.7 Níveis de Impacto

Impacto		Nível do Impacto			Aplicabilidade
		Impacto Alto	Impacto Médio	Impacto Baixo	
Disponibilidade		Recurso totalmente inoperante	Recurso operante com performance degradada	Não se aplica	A cada hora ou fração de hora excedente, sobre o valor da fatura
Tempo de resposta a incidentes de segurança	Alto risco	Excedeu o prazo informado	Não se aplica	Não se aplica	A cada quarto de hora, ou fração, sobre o valor da fatura
	Demais categorias	Não se aplica	Excedeu o prazo informado	Não se aplica	A cada meia hora ou fração, sobre o valor da fatura
	Esclarecimento de dúvidas	Não se aplica	Não se aplica	Excedeu o prazo informado	A cada 24h de atraso, sobre o valor da fatura
Alteração de configuração		Não se aplica	Excedeu o prazo informado	Não se aplica	A cada 24h, ou fração, sobre o valor da fatura
Configuração de Dashboard		Não se aplica	Excedeu o prazo informado	Não se aplica	A cada 24h, ou fração, sobre o valor da fatura
Atualizações de Segurança	implementação de patches e fixes	Excedeu o prazo informado	Não se aplica	Não se aplica	A cada 24h, ou fração, sobre o valor da fatura
	Atualização de bases externas de assinatura de ataques	Excedeu o prazo informado	Não se aplica	Não se aplica	A cada hora ou fração, sobre o valor da fatura