ANEXO

ESPECIFICAÇÃO DE REQUISITOS DAS SOLUÇÃO

1. INTRODUÇÃO

1.1. O presente Anexo tem por objetivo estabelecer as especificações técnicas mínimas e os requisitos que deverão ser atendidos pela solução de Observabilidade *Full Stack* a ser contratada.

Considerando a diversidade tecnológica existente no ambiente do BANCO, composto por soluções de diferentes fabricantes, arquiteturas, plataformas e versões, a solução deverá ser capaz de consolidar informações provenientes desses ambientes em uma visão única de observabilidade, permitindo a correlação entre métricas, logs, eventos, traces distribuídos e demais dados operacionais necessários à identificação, análise e tratamento de incidentes, problemas de desempenho e degradações de serviço.

As especificações constantes neste Anexo representam os requisitos mínimos obrigatórios para aceitação da solução ofertada.

2. TECNOLOGIAS MÍNIMAS SUPORTADAS

2.1. A solução deverá possuir capacidade de monitoramento, coleta, observabilidade e correlação de dados dos produtos e tecnologias existentes no ambiente do BANCO, considerando, no mínimo, as versões indicadas na tabela a seguir.

TECNOLOGIA	VERSÃO
.Net Core	2.0.3
Active Directory	Windows2012R2
ASP NET	3
CICS	5
COM+	3 +
F5 Big IP	17.5.1
Framework .NET	4.5
IBM ACE	V 10.1.1
IBM Broker	V9
IBM DB2 (plataforma alta e baixa)	V12R1M505
IBM IIB	10
IBM MQ (plataforma alta e baixa)	V9.3.0
Java	8
JBoss	7.6.11.GA
Kafka	3.8.0
Liberty/Open Liberty	1.5.0
Linux (RedHat Enterprise Linux)	7
Mobile e Frameworks (iOS e Android)	>10
MS SQL Server	2012
Openshift	3.11
Postgres	10
Power Builder	10

RABBITMQ	4.1.1
React	18
Redis	6.2.7
RH BK	26.2.14
TomCat	7
Visual Basic (VB)	6
VMware (vSphere)	7.0.3
Web Sphere Application Server	7.0.0.43
Windows Server	2008R2

2.2. A compatibilidade com versões às indicadas e superiores deverá ser mantida durante toda a vigência contratual.

2.3. A compatibilidade poderá ser implementada por meio de funcionalidades nativas da solução, agentes, coletores, APIs, conectores, exporters, SDKs, protocolos padronizados de mercado ou outros mecanismos oficialmente suportados pelo fabricante, desde que seja assegurada a coleta, processamento, correlação e visualização integrada dos dados na plataforma de observabilidade.

3. REQUISITOS DA SOLUÇÃO

3.1. Os requisitos técnicos da solução encontram-se relacionados na tabela abaixo.

1. Requisitos Gerais da Solução	
1.1 Plataforma SaaS de observabilidade unificada	a) A solução deverá ser disponibilizada na modalidade Software as a Service (SaaS), cabendo ao fornecedor prover e manter todas as licenças, atualizações, correções, suporte técnico e demais serviços necessários ao seu pleno funcionamento durante toda a vigência contratual.
	b) A solução deverá prover visibilidade completa, contínua e correlacionada do ambiente tecnológico do Contratante.
	c) A solução deverá ser capaz de consolidar, em uma única plataforma integrada, a coleta, o processamento e a análise de diferentes tipos de telemetria, incluindo, mas não se limitando a métricas, logs, eventos, traces distribuídos, fluxos de rede e informações de experiência do usuário, garantindo capacidade de correlação entre esses dados em tempo real.
	d) Deverá permitir o acompanhamento das transações críticas de negócio de ponta a ponta, mesmo quando estas atravessarem múltiplas camadas tecnológicas, incluindo sistemas legados de alta plataforma, aplicações modernas distribuídas, middleware, bancos de dados e infraestrutura de rede, assegurando rastreabilidade completa e contextualizada.
	e) A plataforma deverá operar de forma unificada, eliminando a necessidade de utilização de múltiplas ferramentas isoladas para

	coleta, análise ou visualização, devendo oferecer interface única para navegação, investigação e análise de causa raiz, suportando o trabalho integrado das equipes de Operações, SRE, DevOps, Segurança e Negócio.
1.2 Integração com Plataforma de ITSM	a) A solução deverá prover integração nativa e bidirecional com a plataforma corporativa de IT Service Management (ITSM) adotada pelo Contratante, permitindo a automação do ciclo de vida de incidentes a partir de eventos detectados na observabilidade.
	b) Deverá possibilitar a criação automática de incidentes a partir de alertas gerados na plataforma, com enriquecimento contextual contendo informações técnicas relevantes, tais como logs correlacionados, métricas, serviços impactados, topologia de dependências e evidências associadas.
	c) A integração deverá permitir sincronização completa entre as plataformas, incluindo estados de incidentes, atualizações, comentários, atribuições e encerramentos, de forma que qualquer alteração em um sistema seja refletida automaticamente no outro.
	d) A solução não deverá depender de desenvolvimento customizado para viabilizar a integração, devendo utilizar conectores nativos, APIs oficiais ou mecanismos declarativos suportados pelo fabricante.
1.3 Visibilidade Fim a Fim das Jornadas de Negócio	a) A solução deverá permitir o monitoramento integrado das jornadas de negócios, possibilitando rastreamento completo desde a interação do usuário até os sistemas de backend, permitindo identificação rápida de gargalos, falhas e degradações.
2. Arquitetura da Solução	
2.1 Arquitetura SaaS com Coleta Local de Dados	a) A solução de observabilidade deverá ser fornecida e operada no modelo Software as a Service (SaaS), não sendo permitida a dependência de infraestrutura de backend analítico instalada ou mantida no ambiente do Contratante.
	b) A arquitetura deverá contemplar a coleta de dados de telemetria diretamente no ambiente on-premises do Contratante, por meio de componentes oficiais, como agentes, coletores, exporters, bridges ou SDKs, sendo estes responsáveis pela captura contínua de métricas, logs, traces, eventos e fluxos de rede.
	c) A solução deverá garantir a transmissão segura dos dados para a plataforma SaaS, por meio de protocolos criptografados, podendo ainda executar localmente funções de pré-processamento, incluindo filtragem, agregação, anonimização, mascaramento e roteamento, de acordo com as políticas de segurança e privacidade definidas pelo Contratante.

	d) A comunicação entre a infraestrutura do Contratante e a solução deverá ocorrer por meio de um ponto único de comunicação, tais como gateway, proxy ou componente equivalente. Não será permitida a comunicação direta entre os servidores que suportam os sistemas do Banco do Nordeste e a solução contratada.
	e) A solução deverá assegurar que a coleta local não comprometa a performance dos ativos monitorados, devendo operar com baixo consumo de recursos e capacidade de resiliência a falhas de conectividade, incluindo mecanismos de buffer e retransmissão.
2.2 Monitoramento de Infraestrutura, Aplicações e Rede	a) A solução deverá contemplar o monitoramento completo e integrado dos componentes de infraestrutura, incluindo servidores físicos, máquinas virtuais, contêineres e serviços essenciais, abrangendo indicadores de desempenho e disponibilidade, sendo compatível com as versões dos softwares especificadas na Tabela X – Versões Mínimas de Software e com suas versões superiores.
	b) Deverá ser capaz de coletar e apresentar métricas detalhadas, tais como utilização de CPU, memória, I/O de disco, throughput de rede, latência, disponibilidade de serviços e outros indicadores relevantes para a operação.
	c) A solução deverá suportar monitoramento de equipamentos de rede por meio de protocolos padrão (SNMP, ICMP ou equivalentes), permitindo visualização da topologia lógica e física, análise de capacidade, utilização de interfaces e identificação de dependências entre componentes.
	d) A solução deverá permitir o monitoramento de fluxos de rede, possibilitando rastreamento de tráfego entre aplicações e infraestrutura, identificação de gargalos, análise de comunicação entre serviços e correlação com eventos de aplicação.
2.3 Monitoramento de Aplicações (APM) e Tracing de Alta Plataforma	a) A solução deverá prover funcionalidade nativa de Application Performance Monitoring (APM), com suporte a tracing distribuído de ponta a ponta, permitindo o rastreamento de transações que atravessem múltiplos serviços, componentes e tecnologias. As funcionalidades de monitoramento e instrumentação deverão ser compatíveis com as versões dos softwares especificadas na Tabela X – Versões Mínimas de Software, bem como com suas versões superiores.

	b) A solução deverá suportar ambientes heterogêneos, incluindo aplicações modernas baseadas em microsserviços e sistemas legados, com capacidade de rastrear interações que envolvam middleware, filas, APIs e bancos de dados.
	c) A solução deverá suportar a instrumentação de aplicações que interagem com sistemas legados, incluindo tecnologias como IBM MQ, DB2 e WebSphere, ou equivalentes, assegurando a visibilidade de transações híbridas por meio de instrumentação baseada em padrões abertos (OpenTelemetry), bridges, adaptadores ou conectores oficialmente suportados.
	d) A solução deverá preservar o contexto transacional, permitindo identificar o caminho completo de uma requisição, incluindo tempos de execução, dependências, falhas e gargalos de desempenho.
2.4 Abrangência e Enriquecimento da Telemetria	a) A solução deverá ser capaz de coletar, processar e correlacionar diferentes tipos de dados de telemetria, incluindo métricas, logs, eventos e traces, provenientes de todos os componentes monitorados.
	b) Os dados coletados deverão ser automaticamente enriquecidos com contexto operacional relevante, incluindo identificação de host, aplicação, serviço, ambiente, localização, usuário, entre outros atributos que facilitem a análise e investigação.
	c) A plataforma deverá permitir navegação integrada entre os dados, proporcionando capacidade de análise multidimensional, onde um evento identificado em uma métrica possa ser correlacionado com logs, traces e demais sinais relevantes.
2.5 Plataforma Unificada e Correlação Inteligente	a) A solução deverá operar em uma plataforma unificada, com interface única de acesso a todas as funcionalidades de observabilidade, segurança e análise operacional.
	b) Deverá ser capaz de correlacionar automaticamente métricas, logs, traces, eventos e fluxos de rede, sem necessidade de configuração manual extensiva, reduzindo a complexidade operacional e o tempo de diagnóstico de incidentes.
	c) A solução deverá contemplar mecanismos de detecção de anomalias baseados em algoritmos de natureza probabilística e estatística e em modelos de aprendizado de máquina, podendo ser apoiados por modelos de linguagem de

	grande porte (LLMs) de mercado, como os fornecidos por OpenAI e Anthropic, entre outros, contribuindo para a identificação proativa de comportamentos anômalos.
	d) Deverá ainda permitir criação de dashboards personalizados para diferentes perfis (técnico, gerencial e executivo), integrando dados técnicos e indicadores de negócio.
2.6 Independência Tecnológica e Interoperabilidade	a) A solução deverá suportar padrões abertos de observabilidade, como o OpenTelemetry/OTLP, garantindo interoperabilidade entre diferentes tecnologias e permitindo instrumentação independente de fornecedor.
2.7 Previsibilidade de Custos e Eficiência Operacional	a) A solução deverá disponibilizar mecanismos para acompanhamento do nível de utilização e da projeção de consumo de seus módulos e recursos licenciados, permitindo o gerenciamento eficiente da capacidade contratada e a adoção de ações preventivas para evitar a utilização além dos limites estabelecidos em contrato.
2.8 Conformidade Regulatória e Auditoria	a) A solução deverá garantir a integridade, a rastreabilidade e a auditabilidade dos dados coletados, incluindo logs operacionais e trilhas de auditoria, assegurando que todas as ações realizadas na plataforma sejam devidamente registradas.
	b) A solução deverá contemplar mecanismos de mascaramento de dados sensíveis, controle de acesso baseado em perfis (Role-Based Access Control – RBAC) e políticas de retenção de dados aderentes aos requisitos legais, regulatórios e normativos aplicáveis, bem como às diretrizes institucionais do Banco.
3. Requisitos Funcionais	
3.1 Coleta Unificada e Correlação Automática de Métricas, Logs, Traces e Eventos	a) A solução de observabilidade deverá prover a coleta unificada, contínua e em tempo real de dados provenientes das diversas camadas do ambiente tecnológico do Contratante, incluindo infraestrutura, aplicações, serviços, rede, bancos de dados e experiência do usuário.
	b) A coleta deverá abranger, de forma integrada, métricas, logs, traces distribuídos e eventos operacionais, permitindo a construção de uma visão ponta a ponta das transações de negócio, inclusive em ambientes distribuídos e híbridos.
	c) A solução deverá operar sobre um modelo unificado de ingestão e análise, no qual os dados coletados sejam automaticamente correlacionados entre si, sem necessidade de consolidação manual ou uso de ferramentas

	distintas. Essa correlação deverá considerar contexto como serviço, host, aplicação, usuário e demais metadados relevantes, possibilitando identificar rapidamente relações entre eventos e anomalias.
	d) Deverá ser suportada a navegação bidirecional entre os diferentes tipos de telemetria, permitindo que o usuário percorra de forma fluida entre métricas, logs e traces, preservando o contexto da investigação.
	e) A solução deverá ainda ser compatível com padrões abertos de observabilidade, incluindo OpenTelemetry, bem como suportar o uso de agentes, coletores e conectores oficiais, garantindo flexibilidade e cobertura do ambiente, incluindo sistemas legados e integrações com alta plataforma.
	f) A solução deverá oferecer gestão centralizada da coleta, permitindo controle da frota de agentes e coletores, incluindo inventário, monitoramento de saúde, versionamento e aplicação de configurações em escala.
	g) Toda a operação deverá atender aos requisitos de segurança e governança, contemplando controle de acesso por papéis (RBAC), trilhas de auditoria e compatibilidade com políticas de segurança do Contratante.
3.2 Suporte Nativo e Abrangente a OpenTelemetry/OTLP	a) A solução de observabilidade deverá ser plenamente compatível com padrões abertos de telemetria, com destaque para o OpenTelemetry (OTel) e protocolo OTLP, permitindo instrumentação, coleta, ingestão, exportação e correlação de dados de observabilidade de forma agnóstica a fornecedor (vendor-neutral).
	b) Deverá ser possível ingerir e processar métricas, logs, traces e eventos provenientes de aplicações e serviços instrumentados com OpenTelemetry, bem como de componentes que utilizem padrões equivalentes de mercado, assegurando integração entre sistemas distribuídos, legados e ambientes heterogêneos.
	c) A solução deverá suportar o uso de coletores, exporters, bridges, SDKs e agentes compatíveis com OTel, sejam eles nativos da plataforma ou homologados, garantindo flexibilidade na coleta e interoperabilidade com diferentes tecnologias utilizadas pelo Contratante.
	d) Deverá ainda suportar a correlação de transações híbridas, incluindo cenários que envolvam integração entre sistemas distribuídos e componentes de alta plataforma, preservando o contexto ponta a ponta da transação, mesmo

	quando a propagação de contexto ocorrer por mecanismos intermediários (ex.: bridges ou adaptadores).
	e) A Contratada deverá ser responsável por garantir a correta implementação da instrumentação baseada em padrões abertos, assegurando a consistência, integridade e correlação dos dados no ambiente do Contratante, incluindo transações críticas de negócio.
3.3 Pipeline de Dados de Observabilidade	a) A solução poderá disponibilizar, como diferencial funcional, um pipeline nativo de processamento e roteamento de dados de observabilidade, capaz de atuar sobre métricas, logs, traces e eventos antes de seu armazenamento ou envio à plataforma SaaS.
	b) O pipeline de dados deverá permitir a aplicação de regras de tratamento em tempo real, incluindo filtragem, transformação, enriquecimento, mascaramento e roteamento de dados, com o objetivo de otimizar o volume de ingestão, garantir conformidade com políticas de segurança e ampliar a flexibilidade de uso da telemetria.
	c) A solução deverá permitir a definição de políticas de tratamento e roteamento de dados, incluindo, mas não se limitando, à eliminação de dados redundantes ou de baixa relevância, à anonimização ou ao mascaramento de informações sensíveis, à padronização e transformação de campos, ao enriquecimento de registros com metadados adicionais e ao encaminhamento simultâneo dos dados para múltiplos destinos, tais como soluções de SIEM, data lakes corporativos e outras ferramentas de processamento ou análise.
	d) O pipeline deverá operar em tempo real e com baixa latência, sendo gerenciado por meio de interface gráfica ou configuração declarativa, preferencialmente sem necessidade de programação (no-code).
	e) O pipeline de dados deverá estar integrado ao restante da plataforma, garantindo que o uso do pipeline não comprometa a correlação dos dados de observabilidade, segurança e operação, especialmente no suporte a investigações de incidentes e análises forenses.
3.4 Dashboards e Visualização Operacional	a) A solução deverá disponibilizar recursos nativos para criação, personalização e compartilhamento de dashboards e painéis de observabilidade, permitindo a visualização integrada de dados técnicos e operacionais em tempo real.

	b) Os dashboards deverão suportar a consolidação de informações provenientes de múltiplas fontes, como infraestrutura, aplicações, bancos de dados, rede e demais componentes monitorados, possibilitando uma visão unificada do ambiente.
	c) A solução deverá oferecer componentes visuais variados, como gráficos de série temporal, barras, tabelas, indicadores numéricos e mapas de topologia, permitindo a construção de painéis adequados a diferentes perfis de uso (operacional, técnico e gerencial).
	d) A criação e edição dos dashboards deverá ocorrer de forma intuitiva e assistida, preferencialmente por meio de interface gráfica (drag-and-drop), sem necessidade de desenvolvimento ou uso de linguagem de programação, permitindo autonomia das equipes do Contratante.
	e) Deverá ser possível aplicar filtros dinâmicos e segmentações por atributos e tags, possibilitando análises contextualizadas por ambiente, aplicação, serviço ou qualquer dimensão relevante.
	f) A solução deverá permitir o compartilhamento controlado dos dashboards, com aplicação de controle de acesso baseado em papéis (RBAC), garantindo que diferentes usuários tenham acesso apenas às informações pertinentes ao seu perfil.
3.5 Exploração de Dados e Análise de Logs, Métricas e Traces	a) A solução deverá permitir a exploração e análise de logs, métricas e traces por meio de interface unificada.
	b) A solução deverá permitir a consulta e análise dos dados sem exigir conhecimento de linguagens de consulta, programação ou desenvolvimento de código.
	c) A solução deverá disponibilizar construtores visuais de consultas (no-code).
	d) Os construtores visuais deverão suportar, no mínimo: I – seleção de campos e atributos; II – aplicação de filtros dinâmicos; III – utilização de facetas; IV – agregações automáticas; V – seleção de períodos de tempo; VI – autocompletar de campos e atributos disponíveis.
	e) A solução deverá permitir navegação contextual entre os diferentes domínios da

	observabilidade, incluindo logs, métricas e traces correlacionados.
	f) A solução deverá suportar operações analíticas sobre os dados coletados.
	g) As operações analíticas deverão contemplar, no mínimo: I – médias; II – máximos; III – mínimos; IV – somatórios; V – contagens; VI – percentis; VII – taxas (rates); VIII – rollups; IX – comparações relativas.
	h) A solução deverá permitir a correlação entre múltiplas fontes de dados monitoradas pela plataforma.
	i) As funcionalidades de correlação deverão permitir, no mínimo: I – restringir logs de uma aplicação aos períodos em que uma métrica ultrapassar determinado limiar; II – correlacionar métricas de infraestrutura com eventos de aplicação ou de rede; III – identificar traces de transações associadas a anomalias ou violações de indicadores de desempenho.
	j) A solução deverá disponibilizar modo avançado de consulta baseado em expressões, fórmulas ou linguagem de consulta, sem que sua utilização seja necessária para as atividades operacionais cotidianas.
	k) A solução deverá permitir o salvamento de consultas, visualizações e painéis para reutilização posterior.
	l) A solução deverá permitir o compartilhamento de consultas, visualizações e painéis entre usuários e grupos autorizados.
	m) O compartilhamento das informações deverá respeitar os controles de acesso baseados em papéis (Role-Based Access Control – RBAC).
	n) A solução deverá permitir a exportação dos resultados de consultas e análises por meio de APIs oficiais ou mecanismos equivalentes suportados pelo fabricante.
	o) A exportação dos resultados deverá preservar a rastreabilidade das informações analisadas.

	p) A exploração dos dados deverá ocorrer de forma integrada entre logs, métricas e traces, sem necessidade de alternância entre ferramentas distintas para realização de análises correlacionadas.
3.6 Alertas Personalizáveis e Orientados ao Negócio	a) A solução deverá disponibilizar mecanismo de gerenciamento de alertas para criação, personalização e manutenção de regras de monitoramento.
	b) A configuração e manutenção dos alertas deverá ser realizada por meio de interface gráfica, sem necessidade de programação, scripts ou edição manual de arquivos.
	c) A solução deverá permitir a criação de regras de alerta baseadas em métricas, logs, traces ou combinações lógicas entre essas fontes de dados.
	d) A solução deverá suportar operadores booleanos, expressões condicionais e janelas de tempo configuráveis na definição das regras de alerta.
	e) A solução deverá permitir a criação de alertas compostos e correlacionados considerando múltiplas fontes de dados ou condições simultâneas.
	f) A solução deverá suportar limiares dinâmicos (dynamic thresholds) para geração de alertas.
	g) Os limiares dinâmicos deverão poder ser definidos com base em comportamento histórico ou algoritmos de detecção de anomalias.
	h) A solução deverá permitir a criação de alertas baseados em indicadores operacionais e indicadores de negócio, podendo serem baseados, no mínimo, em: I – objetivos de nível de serviço (SLOs); II – indicadores-chave de desempenho (KPIs); III – transações de negócio; IV – quantidade de usuários ativos; V – volume de requisições.
	i) A interface de configuração de alertas deverá disponibilizar, no mínimo: I – preenchimento assistido (autocomplete); II – validação automática dos critérios configurados; III – visualização prévia das condições de disparo dos alertas.
	j) A solução deverá suportar múltiplos canais de notificação, sendo, no mínimo: I – correio eletrônico; II – SMS;

	III – plataformas corporativas de comunicação e colaboração.
	k) A solução deverá permitir integração com sistemas de gerenciamento de incidentes utilizados pelo Contratante.
	l) A solução deverá permitir controle de prioridade dos alertas.
	m) A solução deverá permitir supressão de alertas.
	n) A solução deverá permitir agrupamento de alertas correlacionados.
	o) A solução deverá disponibilizar mecanismos de redução de ruído (noise reduction).
	p) A solução deverá disponibilizar mecanismos de aprendizado contínuo e ajuste automático de limiares (thresholds) com base em comportamento sazonal, volume de transações e padrões históricos de operação.
	q) A solução deverá permitir a configuração e o acompanhamento dos alertas em tempo real.
	r) A solução deverá permitir a visualização dos estados dos alertas, contemplando, no mínimo: I – triggered; II – resolved; III – acknowledged.
	s) A solução deverá manter histórico completo dos alertas gerados, incluindo a sequência de eventos que originou cada alerta.
	t) A solução deverá implementar controle de acesso baseado em papéis (Role-Based Access Control – RBAC) para configuração e gerenciamento dos alertas.
	u) A solução deverá manter rastreabilidade das alterações realizadas na configuração dos alertas.
3.7 Integração com ServiceNow (ITSM e ITOM)	a) A solução deverá oferecer integração nativa, certificada e bidirecional com a plataforma ServiceNow, utilizada pelo Contratante para processos de IT Service Management (ITSM) e IT Operations Management (ITOM).
	b) A integração deverá abranger todo o ciclo de vida dos incidentes, desde a geração de alertas até sua resolução e encerramento, assegurando a sincronização das informações entre as plataformas integradas.

	c) A solução deverá permitir a criação automática de incidentes no ServiceNow a partir de alertas e eventos gerados pela plataforma de observabilidade, incluindo, mas não se limitando, a métricas, logs, traces, violações de SLOs, eventos de segurança e indicadores de negócio.
	d) A solução deverá permitir a definição de critérios configuráveis para abertura automática de incidentes, incluindo severidade, impacto, correlação de eventos, criticidade do serviço e outros parâmetros definidos pelo Contratante.
	e) A solução deverá permitir o mapeamento e preenchimento automático de campos dos registros do ServiceNow, incluindo, mas não se limitando, a categoria, prioridade, impacto, urgência, serviço afetado, responsável e descrição detalhada da ocorrência.
	f) O preenchimento e o mapeamento dos campos entre as plataformas deverão ser realizados por meio de mecanismos nativos de configuração, sem necessidade de desenvolvimento customizado para o fluxo principal de integração.
	g) A integração deverá suportar sincronização bidirecional dos atributos dos incidentes, incluindo, mas não se limitando, a status, severidade, impacto, urgência, atribuição, comentários, notas de trabalho e encerramento.
	h) Alterações realizadas no ServiceNow ou na plataforma de observabilidade deverão ser refletidas automaticamente na outra plataforma, incluindo atualizações de status, reconhecimento, resolução, reabertura, encerramento e priorização de incidentes.
	i) A solução deverá enriquecer automaticamente os incidentes criados no ServiceNow com informações provenientes da plataforma de observabilidade, incluindo, quando disponíveis, métricas correlacionadas, logs associados, traces distribuídos, topologia dos serviços afetados, dependências entre aplicações e demais informações relevantes para diagnóstico e análise de impacto.
	j) A integração deverá ser implementada por meio de conectores nativos, APIs oficiais, webhooks suportados pelo fabricante ou interface gráfica de configuração, sem exigir desenvolvimento customizado para sua operacionalização.
	k) A solução deverá suportar mecanismos de autenticação segura para a integração com o

	ServiceNow, incluindo OAuth 2.0, certificados digitais, tokens de acesso ou mecanismos equivalentes.
	l) A solução deverá permitir a automação de ações relacionadas ao ciclo de vida dos incidentes, incluindo, mas não se limitando, à atualização de status, alteração de prioridade, atribuição automática e encerramento automático mediante condições previamente definidas pelo Contratante.
	m) A solução deverá permitir o acompanhamento, em tempo real, do status dos incidentes integrados ao ServiceNow, preservando a rastreabilidade e o histórico das interações realizadas entre as plataformas.
3.8 Monitoramento Detalhado de Bancos de Dados	a) A solução deverá prover, de forma nativa e integrada à plataforma, funcionalidades de monitoramento de desempenho de sistemas gerenciadores de bancos de dados (Database Monitoring – DBM), sem dependência de ferramentas externas, produtos auxiliares ou módulos adicionais.
	b) A solução deverá coletar, armazenar, visualizar e correlacionar métricas operacionais e de desempenho dos bancos de dados monitorados.
	c) O monitoramento deverá permitir o acompanhamento, no mínimo, das seguintes métricas: I – utilização de CPU por instância, banco de dados ou nó monitorado; II – utilização de memória por instância, banco de dados ou nó monitorado; III – quantidade de sessões ou conexões ativas; IV – volume de operações de leitura e escrita (I/O throughput); V – latência de execução de consultas e comandos; VI – taxa de transações por segundo (Transactions Per Second – TPS); VII – tempo médio de processamento e confirmação de transações (commit time).
	d) A solução deverá disponibilizar funcionalidades de análise de desempenho de consultas SQL.
	e) As funcionalidades de análise de consultas SQL deverão permitir, no mínimo: I – identificação das consultas com maior tempo de execução; II – identificação das consultas com maior consumo de recursos computacionais; III – visualização e análise de planos de

	execução, exceto para o DB2; IV – detecção de bloqueios, contenções e deadlocks, incluindo os respectivos objetos afetados; V – acompanhamento da utilização e eficiência de índices.
	f) A solução deverá permitir correlacionar problemas identificados nos bancos de dados com impactos observados em aplicações, serviços, infraestrutura e demais componentes monitorados.
	g) A solução deverá permitir identificar relacionamentos de causa e efeito entre degradações de desempenho observadas em aplicações e eventos ocorridos nos bancos de dados monitorados.
	h) As informações de monitoramento dos bancos de dados deverão estar integradas à mesma interface e ao mesmo fluxo de investigação utilizado pelos demais domínios da observabilidade, permitindo navegação contextual entre aplicações, serviços, infraestrutura e bancos de dados.
	i) A solução deverá possuir coleta nativa e suporte ao monitoramento dos seguintes sistemas gerenciadores de bancos de dados: I – Microsoft SQL Server; II – PostgreSQL; III – IBM Db2.
	j) A solução deverá ser compatível com as versões dos SGBDs especificadas na Tabela X – Versões Mínimas de Software, bem como com versões superiores suportadas pelos respectivos fabricantes.
	k) As informações coletadas deverão estar disponíveis para consulta em tempo real ou próximo do tempo real.
	l) A solução deverá disponibilizar histórico de métricas, visualizações gráficas, consultas analíticas, alertas configuráveis e exportação de dados por meio de APIs oficiais.
	m) A solução deverá permitir a definição de alertas relacionados ao desempenho, disponibilidade e utilização dos bancos de dados monitorados, conforme critérios definidos pelo Banco.
	n) Para gerenciadores de banco de dados executados em ambiente de alta plataforma (mainframe), a coleta de métricas poderá ser realizada por meio de componentes ou

	conectores oficialmente suportados pelo fabricante, desde que integrados à plataforma de observabilidade e sem prejuízo das funcionalidades de monitoramento, correlação e análise previstas para os demais SGBDs.
3.9 Configuração Sem Necessidade de Programação (No-Code)	a) A solução deverá permitir que as atividades de administração e operação sejam executadas sem a necessidade de conhecimento em linguagens de programação.
	b) A criação, alteração e administração de alertas deverá ser realizada por meio de interface gráfica ou mecanismos declarativos suportados pelo fabricante, sem exigir a implementação de scripts ou código customizado.
	c) A criação, alteração e administração de dashboards, painéis e visualizações deverá ser realizada por meio de interface gráfica, sem exigir a implementação de scripts ou código customizado.
	d) A criação e manutenção de consultas operacionais sobre métricas, logs, traces e demais dados de observabilidade deverá ser realizada por meio de recursos nativos da plataforma, sem exigir conhecimentos de programação para sua utilização cotidiana.
	e) A configuração de integrações nativas suportadas pela solução deverá ser realizada por meio de interfaces gráficas, assistentes de configuração ou mecanismos declarativos fornecidos pelo fabricante, sem exigir desenvolvimento customizado para os cenários previstos neste Termo de Referência.
	f) A configuração de políticas de coleta, tratamento, roteamento e retenção de dados deverá ser realizada por meio de recursos nativos da plataforma, sem a necessidade de desenvolvimento de código.
	g) A administração de usuários, perfis, permissões e controles de acesso deverá ser realizada por meio de interface gráfica integrada à plataforma.
	h) A solução deverá disponibilizar mecanismos de validação das configurações realizadas pelos usuários, de forma a reduzir erros operacionais e inconsistências de parametrização.
	i) A solução deverá disponibilizar visualização prévia ou mecanismos equivalentes de validação das configurações antes de sua aplicação, quando tecnicamente aplicável.

	j) A solução deverá manter trilha de auditoria das alterações de configuração realizadas na plataforma, permitindo identificar a data, a hora e o responsável por cada alteração.
	k) A solução deverá permitir a manutenção de histórico de configurações e, quando aplicável à funcionalidade configurada, possibilitar a reversão (rollback) de alterações realizadas.
	l) A solução deverá aplicar controle de acesso baseado em papéis (Role-Based Access Control – RBAC) às atividades de configuração e administração da plataforma.
	m) A solução deverá permitir a exportação de configurações, políticas e parâmetros da plataforma para fins de auditoria, governança, documentação ou recuperação operacional.
	n) Funcionalidades que exijam desenvolvimento de código poderão ser disponibilizadas como recurso complementar, desde que sua utilização não seja necessária para a operação cotidiana das funcionalidades de alertas, dashboards, consultas, integrações nativas, administração de usuários e gestão de configurações previstas neste Termo de Referência.
3.10 Imutabilidade e Retenção dos Dados	a) A solução deverá garantir que os dados de observabilidade, especialmente logs, sejam armazenados de forma imutável, íntegra e protegida contra alterações ou exclusões não autorizadas, assegurando sua confiabilidade para fins operacionais, auditoria e conformidade regulatória.
	b) A solução deverá permitir a definição de políticas de retenção por tipo de dado (logs, métricas, traces e eventos), com suporte a diferentes períodos conforme necessidade do Banco, incluindo retenção em camadas distintas, como dados ativos e arquivados.
	c) Os dados deverão permanecer acessíveis para consulta durante todo o período definido, com possibilidade de recuperação (reidratação) de dados arquivados, sem perda de integridade ou rastreabilidade.
	d) A solução deverá suportar mecanismos que assegurem a integridade dos dados, como armazenamento em modo append-only, controle de acesso, trilhas de auditoria e proteção contra alterações indevidas.
	e) A solução deverá atender aos requisitos de segurança e privacidade, incluindo criptografia dos dados, controle de acesso baseado em papéis (RBAC) e conformidade com as políticas

	do Contratante e regulamentações aplicáveis, como a LGPD.
3.11 Disponibilidade e Desempenho da Plataforma SaaS	a) A solução deverá operar em arquitetura altamente disponível, resiliente e distribuída, garantindo continuidade do serviço de observabilidade mesmo em cenários de falha parcial de infraestrutura ou degradação de componentes.
	b) A solução deverá ser projetada com mecanismos de redundância em múltiplas zonas de disponibilidade ou regiões, incluindo balanceamento de carga, failover automático e recuperação transparente para o usuário, sem necessidade de intervenção manual do contratante.
	c) A solução deverá ser executada em datacenters localizados no Brasil ou em países que possuem convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços serão ser prestados.
	d) A solução deverá assegurar disponibilidade mínima de 99,9% (noventa e nove vírgula nove por cento) ao longo do período de medição, considerando o acesso à plataforma, ingestão de dados e funcionalidades de análise.
	e) A solução deverá suportar escalabilidade automática, sendo capaz de crescer conforme o volume de dados, número de hosts monitorados ou quantidade de usuários, sem degradação perceptível da performance ou necessidade de intervenção por parte do contratante.
	f) Deverá contemplar mecanismos de resiliência na coleta de dados, garantindo que falhas temporárias de conectividade não resultem em perda definitiva de telemetria, por meio de estratégias como buffering local, reenvio automático e tolerância a falhas.
	g) Indisponibilidades ou degradações da solução de observabilidade não poderão, em hipótese alguma, ocasionar impacto na disponibilidade, no desempenho ou no funcionamento dos sistemas e serviços do Banco do Nordeste.
3.12 Monitoramento de Fluxos de Rede	a) A solução deverá prover, de forma nativa e integrada à plataforma, funcionalidades de monitoramento e análise de fluxos de rede (Network Flows), com suporte aos protocolos NetFlow v5, NetFlow v9, jFlow, sFlow v5 e IPFIX.
	b) A solução deverá permitir a ingestão contínua e escalável de dados de fluxo de rede

	provenientes de múltiplos dispositivos monitorados simultaneamente.
	c) A solução deverá suportar o processamento de, no mínimo, 1.000.000 (um milhão) de fluxos por minuto, considerados de forma agregada.
	d) A coleta e o processamento dos dados de fluxo não deverão ocasionar perda de informações, truncamento de registros ou comprometimento da integridade dos dados coletados.
	e) A solução deverá enriquecer automaticamente os fluxos de rede coletados com metadados associados aos dispositivos monitorados, incluindo, mas não se limitando a: I – nome da interface de rede de origem; II – VLAN associada; III – velocidade nominal da interface; IV – identificação do dispositivo de origem, incluindo nome (hostname), localização e tipo de dispositivo; V – protocolo utilizado; VI – endereços IP de origem e destino; VII – portas de origem e destino; VIII – volume de bytes e pacotes transferidos.
	f) A solução deverá armazenar e disponibilizar para consulta os dados de fluxo de rede coletados, permitindo a configuração do período de retenção de acordo com as necessidades do Banco.
	g) A solução deverá permitir a exportação ou o arquivamento dos dados de fluxo de rede para retenção por períodos superiores aos mantidos na plataforma. A exportação ou o arquivamento dos dados não deverá comprometer as capacidades de consulta, análise, correlação ou auditoria das informações armazenadas.
	h) A solução deverá disponibilizar funcionalidades de análise gráfica e tabular dos fluxos de rede.
	i) A solução deverá permitir a realização de consultas e filtros dinâmicos sobre os dados de fluxo, incluindo, mas não se limitando, a endereço IP, interface de rede, aplicação, dispositivo, serviço, VLAN, protocolo, portas, volume de tráfego e padrões comportamental.
	j) A solução deverá permitir a navegação contextual entre os fluxos de rede e os respectivos dispositivos, interfaces, serviços e aplicações relacionados, viabilizando: I – a identificação de padrões anômalos de tráfego e variações significativas de utilização da rede;

	II – a análise histórica da utilização de banda na comunicação entre componentes monitorados; III – o rastreamento das comunicações entre sistemas e das tentativas de acesso indevido; IV – a correlação dos dados de fluxo com métricas, logs, traces, alertas, eventos e demais informações coletadas pela plataforma.
	k) A solução deverá permitir a exportação programável dos dados de fluxo de rede para sistemas externos, incluindo, mas não se limitando, a soluções de SIEM, data lakes, plataformas de auditoria e repositórios corporativos de dados, preservando a integridade, a consistência e os respectivos registros temporais (timestamps) das informações exportadas.
	l) A solução deverá integrar e correlacionar os dados de fluxo de rede com os demais domínios da observabilidade, incluindo métricas, logs, traces, eventos e experiência digital, permitindo análises de causa raiz e investigações de incidentes em um contexto unificado.
	m) A solução deverá integrar e correlacionar os dados de fluxo de rede com os demais domínios da observabilidade, incluindo, mas não se limitando a, métricas, logs, traces, eventos e dados de experiência digital, permitindo a realização de análises de causa raiz e a investigação de incidentes em um contexto unificado.
3.13 Gestão e Visibilidade de Custos da Solução	a) A solução deverá disponibilizar, de forma nativa e integrada à plataforma, funcionalidades para acompanhamento, controle e governança do consumo dos recursos contratados.
	b) A solução deverá permitir a visualização do consumo dos recursos contratados em tempo real ou próximo do tempo real.
	c) A solução deverá permitir a segregação e análise do consumo dos recursos contratados por diferentes critérios de agrupamento, incluindo, mas não se limitando, a tipo de telemetria, produto, aplicação, serviço, ambiente, unidade organizacional, centro de custo e etiquetas (tags) definidas pelo Banco.
	d) A solução deverá disponibilizar relatórios de utilização dos recursos contratados. Os relatórios deverão permitir a visualização, no mínimo, das seguintes informações: I – histórico de consumo; II – tendências de utilização por tipo de recurso; III – projeções de consumo com base no comportamento observado;

	IV – comparativos entre aplicações, ambientes, sistemas, serviços ou unidades organizacionais.
	e) A solução deverá permitir a configuração de alertas relacionados ao consumo dos recursos contratados.
	f) A solução deverá permitir a definição de limites e gatilhos de consumo, possibilitando o envio de notificações quando percentuais ou valores previamente definidos forem atingidos.
	g) A solução deverá permitir a segregação, atribuição e rateio do consumo dos recursos contratados por unidade organizacional, centro de custo, ambiente, aplicação, serviço ou etiquetas (tags) definidas pelo Banco.
	h) A solução deverá disponibilizar funcionalidades de showback e/ou chargeback para análise e distribuição dos custos associados à utilização da plataforma.
	i) Todos os dados de utilização e consumo deverão poder ser exportados por meio de APIs ou mecanismos nativos suportados pelo fabricante.
	j) A solução deverá permitir a integração dos dados de consumo com ferramentas corporativas de gestão, planejamento, governança, análise ou inteligência de negócios.
	k) A solução deverá permitir a visualização e análise individualizada do consumo associado aos módulos, produtos e funcionalidades licenciadas da plataforma.
	l) A solução deverá disponibilizar mecanismos de projeção de consumo e previsão de utilização dos recursos contratados.
	m) A solução deverá disponibilizar alertas relacionados a tendências de consumo, anomalias de utilização e riscos de extrapolação dos limites contratados.
	n) A solução deverá disponibilizar recomendações ou informações que auxiliem a identificação de oportunidades de otimização do consumo dos recursos contratados.
	o) As funcionalidades de governança, acompanhamento e controle do consumo deverão estar disponíveis na própria interface da plataforma.
	p) Caso sejam necessários componentes adicionais para disponibilizar as funcionalidades previstas nesta seção, estes deverão fazer parte

	da solução ofertada e estar contemplados na proposta comercial.
3.14 Correlação Full-Stack e DevSecOps	a) A solução deverá disponibilizar funcionalidades de correlação entre os diferentes domínios de observabilidade monitorados pela plataforma.
	b) A solução deverá permitir a navegação contextual e a correlação entre, no mínimo: I – métricas de infraestrutura física, virtualizada, em nuvem e contêineres; II – métricas e traces distribuídos de aplicações (APM) III – dados de experiência real do usuário (RUM); IV – métricas e fluxos de rede; V – métricas, consultas, planos de execução e eventos de bancos de dados; VI – logs e eventos operacionais de sistemas; VII – eventos de pipeline de entrega contínua (CI/CD); VIII – achados de segurança de código, dependências, infraestrutura como código (Infrastructure as Code – IaC), segredos e vulnerabilidades identificadas em runtime; IX – entidades do catálogo de serviços; X – dispositivos de usuário final e dispositivos operacionais monitorados.
	c) A solução deverá permitir a propagação e correlação de identificadores distribuídos (trace IDs) entre os componentes monitorados.
	d) A solução deverá permitir correlacionar interações de usuários, traces distribuídos, aplicações, bancos de dados e componentes de infraestrutura envolvidos em uma mesma transação.
	e) A solução deverá disponibilizar interface gráfica unificada para consulta, visualização, filtragem e correlação dos dados monitorados.
	f) A solução deverá permitir navegação (drill-down) entre os diferentes domínios monitorados.
	g) A solução deverá permitir a visualização integrada dos eventos relacionados aos processos de CI/CD.
	h) A solução deverá permitir correlacionar eventos de CI/CD, incluindo builds, testes, commits, pull requests, implantações (deployments) e rollbacks, com alterações observadas no comportamento das aplicações monitoradas.
	i) A correlação entre os domínios monitorados deverá ocorrer de forma automática e contínua.

	j) A correlação deverá suportar dados provenientes de componentes nativos da solução, padrões abertos suportados pelo fabricante e instrumentações oficialmente homologadas.
	k) É desejável que a solução utilize recursos de inteligência artificial para identificação automática de anomalias, agrupamento de eventos relacionados e sugestão de possíveis causas associadas aos eventos monitorados.
	l) A solução deverá permitir investigação bidirecional entre os domínios de observabilidade, segurança de aplicações e engenharia de software.
	m) A partir de incidentes operacionais, a solução deverá permitir identificar, quando disponíveis: I – implantações recentes; II – commits; III – pull requests; IV – alterações em pipelines; V – testes com falha; VI – vulnerabilidades associadas; VII – logs, traces e métricas correlacionados; VIII – responsáveis técnicos (owners); IX – serviços impactados.
	n) A partir de vulnerabilidades ou eventos de segurança identificados pela plataforma, a solução deverá permitir identificar, quando disponíveis: I – serviços em produção afetados; II – aplicações associadas; III – ambiente; IV – responsável técnico (owner); V – criticidade; VI – evidências técnicas relacionadas; VII – logs, traces e métricas correlacionados; VIII – implantações associadas; IX – incidentes correlatos.
	o) A correlação contextual deverá utilizar identificadores, entidades, metadados e marcações (tags) comuns entre os diferentes domínios monitorados pela plataforma.
	p) A solução deverá permitir preservar investigações e análises realizadas em dashboards, casos, incidentes, relatórios, notebooks, runbooks ou mecanismos equivalentes suportados pela solução.
	q) Os registros de investigação deverão preservar, no mínimo, evidências técnicas, histórico de ações, responsáveis e trilha de auditoria.

	r) A solução deverá permitir correlacionar dados de dispositivos de usuário final e dispositivos operacionais com aplicações, serviços, rede, infraestrutura, bancos de dados, logs, traces e incidentes monitorados.
	s) Quando não for possível realizar coleta direta por meio de agentes, a solução deverá suportar mecanismos alternativos oficialmente suportados pelo fabricante, incluindo integração por APIs, logs, telemetria de rede, monitoramento sintético privado ou mecanismos equivalentes.
3.15 Monitoramento Sintético de Aplicações e APIs	a) A solução deverá prover, de forma nativa e integrada, recursos de monitoramento sintético de aplicações web, serviços e APIs, permitindo a execução automatizada de testes que simulem transações e jornadas de negócio críticas, independentemente da existência de usuários reais utilizando os sistemas.
	b) A plataforma deverá possibilitar a criação e execução programada de testes sintéticos para validação de disponibilidade, desempenho, funcionalidade e experiência digital, permitindo monitorar continuamente aplicações web, APIs, portais, serviços internos e demais componentes críticos do ambiente do contratante.
	c) Deverá ser possível executar os testes a partir de diferentes localidades e pontos de monitoramento, incluindo ambientes externos e internos, possibilitando identificar problemas relacionados à conectividade, indisponibilidade, degradação de desempenho ou falhas funcionais percebidas pelos usuários.
	d) Os resultados obtidos deverão ser armazenados e disponibilizados para consulta histórica, permitindo análises de tendência, comparação de desempenho e identificação de regressões ao longo do tempo.
	e) A solução deverá permitir a correlação automática dos resultados dos testes sintéticos com os demais dados coletados pela plataforma, incluindo, mas não se limitando, a métricas, logs, traces, aplicações, componentes de infraestrutura e serviços monitorados.
3.16 Perfilação Contínua (Continuous Profiling)	a) A solução deverá disponibilizar funcionalidade de perfilação contínua de aplicações em produção, integrada de forma nativa à coleta e análise de métricas, logs e traces.
	b) A funcionalidade de perfilação contínua deverá operar de forma ininterrupta durante a execução das aplicações monitoradas.

	c) A funcionalidade de perfilação contínua deverá operar com baixo impacto no desempenho das aplicações monitoradas.
	d) A funcionalidade de perfilação contínua deverá permitir a coleta de informações sobre o comportamento interno das aplicações monitoradas em ambientes distribuídos.
	e) As informações coletadas pela funcionalidade de perfilação contínua deverão incluir, no mínimo: I – utilização de CPU por método, classe ou função; II – alocação e liberação de memória; III – tempo de espera decorrente de mecanismos de bloqueio ou sincronização; IV – contenção de threads ou filas; V – chamadas frequentes ou de elevado custo computacional durante a execução da aplicação.
	f) A solução deverá permitir a correlação dos perfis de execução com traces de APM.
	g) A correlação entre perfis de execução e traces de APM deverá permitir, no mínimo: I – navegação do trace para o respectivo perfil de CPU da execução analisada; II – identificação dos pontos de maior consumo de recursos durante a execução; III – identificação de gargalos associados ao código relacionado ao problema investigado.
	h) A solução deverá disponibilizar visualização histórica dos perfis de desempenho coletados.
	i) A visualização histórica deverá permitir, no mínimo: I – visualização dos perfis de desempenho por serviço; II – visualização dos perfis de desempenho por método; III – visualização dos perfis de desempenho por classe; IV – comparação de perfis ao longo do tempo para identificação de regressões; V – análise de perfis correlacionados a aumentos inesperados no consumo de recursos computacionais.
3.17 Inteligência Artificial e Assistente Virtual para Operações de TI - AIOPs	a) A solução deverá disponibilizar funcionalidades de inteligência artificial aplicadas à monitoração, análise e operação dos ambientes monitorados, com o objetivo de apoiar a detecção, análise, investigação e resolução de incidentes por meio de modelos de aprendizado de máquina, algoritmos analíticos, assistentes conversacionais e agentes especializados.

	b) A solução deverá permitir a detecção automática de anomalias por meio de modelos probabilísticos de aprendizado de máquina. A detecção automática de anomalias deverá permitir, no mínimo: I – identificar desvios relevantes de comportamento sem necessidade de limiares (thresholds) previamente configurados; II – reconhecer padrões sazonais ou comportamentos usuais dos ambientes monitorados; III – gerar alertas relacionados a comportamentos anômalos que possam indicar falhas potenciais.
	c) A solução deverá disponibilizar funcionalidade de análise assistida de causa raiz por inteligência artificial.
	d) A funcionalidade de análise assistida de causa raiz deverá permitir, no mínimo: I – correlacionar eventos provenientes de diferentes domínios monitorados pela plataforma, incluindo infraestrutura, aplicações, bancos de dados, rede, CI/CD e demais dados de observabilidade disponíveis; II – identificar possíveis causas associadas aos incidentes analisados; III – apresentar sínteses e informações consolidadas sobre os incidentes investigados, destacando a provável origem da ocorrência ou a possível causa raiz identificada.
	e) A solução poderá fornecer recomendações automatizadas de ações corretivas relacionadas a eventos, alertas ou incidentes monitorados.
	f) As recomendações automatizadas poderão incluir, quando aplicável: I – ajuste de recursos para serviços com utilização crítica; II – sugestão de reversão (rollback) após alterações correlacionadas a falhas; III – revisão de regras de alerta com base no comportamento recente do ambiente monitorado.
	g) A solução deverá permitir integração com fluxos de automação e ferramentas de ITSM para execução controlada de ações corretivas, quando suportado pela plataforma e autorizado pelo Contratante.
	h) Os recursos de inteligência artificial descritos nesta seção deverão estar integrados à solução principal, sem exigir contratação separada de módulos externos para atendimento das funcionalidades ofertadas.

	i) Os recursos de inteligência artificial deverão observar as políticas de segurança, privacidade e proteção de dados definidas pelo Contratante, especialmente quanto à manipulação de dados sensíveis.
	j) As ações executadas de forma autônoma pelos agentes deverão ser registradas em trilha de auditoria, permitindo a rastreabilidade do agente responsável, da data e hora da ação, do contexto utilizado, da ação executada e do resultado obtido.
3.18 Análise Avançada da Experiência do Usuário – Session Replay	a) A solução deverá disponibilizar funcionalidades de Session Replay, permitindo a gravação e reprodução controlada das interações realizadas pelos usuários nas aplicações monitoradas. Esse recurso deverá complementar as capacidades de monitoramento da experiência digital, fornecendo contexto visual para análises de incidentes, falhas de navegação, erros de aplicação e dificuldades enfrentadas pelos usuários.
	b) A funcionalidade deverá permitir a reprodução das ações executadas durante uma sessão, incluindo navegação entre páginas, cliques, movimentação, preenchimento de formulários e demais interações relevantes, possibilitando que equipes de suporte, operação e desenvolvimento compreendam com maior precisão o comportamento observado pelo usuário no momento da ocorrência.
	c) As sessões registradas deverão estar automaticamente correlacionadas com outras informações da plataforma, como dados de RUM, logs, métricas, traces distribuídos e erros de aplicação, permitindo análises investigativas mais rápidas e completas.
	d) A solução deverá disponibilizar mecanismos para proteção de informações sensíveis, incluindo mascaramento, anonimização ou exclusão de dados confidenciais durante a captura e reprodução das sessões, assegurando aderência às políticas de segurança e privacidade do Contratante e à legislação aplicável.
	e) A solução deverá permitir a parametrização do percentual de sessões de usuários a serem gravadas, possibilitando sua configuração de acordo com critérios e necessidades definidos pelo Banco.
3.19 Observabilidade de Dados, Jobs e Linhagem	a) A solução deverá disponibilizar funcionalidades de observabilidade de dados

	(Data Observability), integradas à mesma plataforma de observabilidade.
	b) A solução deverá permitir o monitoramento da saúde, qualidade, atualidade, integridade e rastreabilidade dos ativos de dados monitorados.
	c) A solução deverá permitir o monitoramento da execução de jobs, pipelines, fluxos de dados e processos de transformação de dados.
	d) A solução deverá permitir a identificação de falhas, atrasos, degradações de desempenho e quebras de dependência em jobs, pipelines e fluxos de dados monitorados.
	e) A solução deverá permitir a identificação de problemas relacionados à qualidade dos dados, incluindo, mas não se limitando, a: I – atrasos na disponibilização dos dados; II – volumes anômalos de registros; III – incompletude de dados; IV – inconsistências de dados; V – violações de regras de qualidade definidas pelo Banco.
	f) A solução deverá disponibilizar funcionalidades de linhagem de dados (Data Lineage), permitindo a visualização e o rastreamento dos fluxos de dados entre suas origens, transformações e destinos.
	g) A solução deverá permitir a correlação dos eventos relacionados a dados com os demais domínios da observabilidade, incluindo, mas não se limitando, a aplicações, infraestrutura, integrações, redes, logs, métricas, traces e incidentes operacionais.
	h) As informações de observabilidade de dados deverão estar disponíveis na mesma interface utilizada pelos demais domínios da plataforma, permitindo navegação integrada e contextualizada.
	i) A solução deverá disponibilizar alertas configuráveis para eventos relacionados à qualidade, disponibilidade, integridade e processamento dos dados monitorados.
	j) A solução deverá disponibilizar dashboards e visualizações para acompanhamento dos ativos de dados monitorados e dos processos de tratamento de dados.
	k) A solução deverá permitir a exportação dos dados, métricas, eventos e alertas associados à observabilidade de dados por meio de APIs ou mecanismos nativos suportados pelo fabricante.

	l) A solução deverá permitir a correlação entre problemas identificados em ativos ou fluxos de dados e os impactos observados em aplicações, serviços, processos de negócio ou demais componentes monitorados pela plataforma.
3.20 Segurança de Aplicações, Código, Dependências, Infraestrutura como Código e Runtime	a) A solução deverá prover, de forma nativa e integrada à plataforma principal, recursos de segurança de aplicações e de código ao longo de todo o ciclo de desenvolvimento e execução, contemplando a identificação, priorização, prevenção, investigação e remediação de vulnerabilidades em código próprio, bibliotecas open source, dependências transitivas, infraestrutura como código (Infrastructure as Code – IaC), segredos, APIs, aplicações em runtime e serviços produtivos.
	b) As capacidades desta seção deverão estar integradas aos dados de observabilidade, pipelines de CI/CD, catálogo de serviços, responsáveis técnicos (owners), incidentes e informações de runtime, permitindo a priorização de riscos com base no contexto real de execução e no impacto para os serviços monitorados.
	c) A solução deverá prover funcionalidades de Static Application Security Testing (SAST), ou capacidade equivalente de análise estática de código-fonte, aplicável a repositórios, branches e pull requests.
	d) A análise estática deverá identificar vulnerabilidades, más práticas de segurança e violações de qualidade, apresentando, no mínimo, evidência técnica, severidade, arquivo, linha de código, regra aplicada e recomendação de correção.
	e) A solução deverá prover funcionalidades de Software Composition Analysis (SCA) ou capacidade equivalente para identificação de bibliotecas diretas e transitivas utilizadas pelas aplicações.
	f) A análise de composição de software deverá identificar, no mínimo, versões vulneráveis, CVEs associadas, severidade, recomendação de atualização e relacionamento com os serviços e aplicações que utilizam as dependências identificadas.
	g) A solução deverá prover análise de vulnerabilidades em runtime, Interactive Application Security Testing (IAST) ou capacidade equivalente, permitindo identificar vulnerabilidades efetivamente presentes ou alcançáveis em serviços em execução.

	h) A análise de vulnerabilidades em runtime deverá permitir a priorização dos achados com base em ambiente, criticidade, exposição, utilização real, tráfego observado, serviço afetado, responsável técnico (owner) e contexto operacional.
	i) A solução deverá prover análise de infraestrutura como código (Infrastructure as Code – IaC), contemplando, no mínimo, arquivos Terraform, manifestos Kubernetes e tecnologias equivalentes utilizadas pelo Contratante.
	j) A análise de IaC deverá identificar configurações inseguras, permissões excessivas, exposições indevidas, ausência de controles e violações de políticas antes da implantação dos ambientes.
	k) A solução deverá prover mecanismos de detecção de segredos, credenciais, chaves, tokens ou informações sensíveis expostas em repositórios, branches, commits ou pull requests.
	l) A detecção de segredos deverá apresentar, no mínimo, classificação do achado, evidência, severidade, recomendação de correção e possibilidade de aplicação de políticas de bloqueio ou exceção controlada.
	m) A solução deverá permitir comentários automáticos em pull requests ou mecanismo equivalente de feedback ao desenvolvedor, apresentando achados relevantes diretamente no fluxo de desenvolvimento.
	n) Os comentários ou mecanismos equivalentes deverão apresentar, no mínimo, arquivo afetado, linha de código, severidade, regra aplicada, explicação do achado e orientação de correção.
	o) A solução deverá permitir a implementação de gates de pull request baseados em políticas de segurança e qualidade definidas pelo Contratante.
	p) Os gates deverão considerar, no mínimo, achados de SAST, SCA, análise de IaC, detecção de segredos, cobertura de código e testes instáveis.
	q) A solução deverá permitir o bloqueio de merge quando as condições mínimas de segurança ou qualidade definidas pelo Contratante não forem atendidas.
	r) A solução deverá priorizar vulnerabilidades considerando, no mínimo, severidade, existência de exploit público, exposição externa ou interna, ambiente, serviço em produção, versão em

	execução, dependência efetivamente utilizada, tráfego observado, responsável técnico (owner) e criticidade operacional.
	s) A solução deverá relacionar cada achado de segurança ao serviço correspondente no catálogo da plataforma.
	t) A associação dos achados ao catálogo deverá incluir, quando disponíveis, responsável técnico (owner), equipe responsável, repositório, pipeline, ambiente, criticidade, SLO, runbook, histórico de deployments e incidentes relacionados.
	u) A solução deverá disponibilizar dashboards e relatórios de gestão de risco.
	v) Os dashboards e relatórios deverão permitir a visualização dos riscos, no mínimo, por aplicação, serviço, equipe, repositório, ambiente, severidade, criticidade, status de remediação, idade do achado, reincidência, exceções aprovadas e tendências de redução de risco.
	w) A solução deverá permitir o acompanhamento do ciclo de vida dos achados de segurança, incluindo identificação, priorização, atribuição, tratamento, exceção, remediação e encerramento.
	x) A solução deverá permitir a exportação dos achados, evidências e indicadores de risco por meio de API oficial ou mecanismo equivalente suportado pelo fabricante.
	y) A solução deverá integrar, de forma nativa, as capacidades de segurança de código, segurança de aplicações, observabilidade e gerenciamento de serviços de TI (ITSM).
	z) A exportação dos achados e evidências deverá permitir integração com soluções de auditoria, GRC, ITSM, BI, data lakes ou plataformas de conformidade utilizadas pelo Contratante.
	aa) A solução deverá aplicar controle de acesso baseado em papéis (Role-Based Access Control – RBAC) às funcionalidades de segurança de aplicações, código, dependências, IaC, segredos e runtime.
	ab) A solução deverá manter trilha de auditoria das ações realizadas sobre achados, políticas, exceções, integrações, aprovações e alterações de configuração relacionadas às funcionalidades desta seção.

	ac) Integrações com ferramentas externas de SAST, SCA, repositórios, CI/CD, scanners, GRC ou ITSM serão aceitas como complementares, mas não substituirão a obrigatoriedade de recursos nativos de análise, priorização e correlação de segurança de código e runtime exigidos nesta seção.
3.21 Observabilidade de CI/CD, DORA, Testes, Cobertura e PR Gates	a) A solução deverá prover, de forma nativa e integrada, visibilidade completa sobre o ciclo de desenvolvimento e entrega de software, permitindo monitorar pipelines de CI/CD, testes, cobertura de código, qualidade de entregas, deployments e indicadores de desempenho das equipes.
	b) A plataforma deverá coletar e correlacionar informações provenientes das ferramentas de integração contínua, entrega contínua e repositórios de código utilizados pelo Banco, permitindo acompanhar a execução de pipelines, seus estágios, falhas, tempos de execução, artefatos gerados e implantações realizadas nos ambientes monitorados.
	c) A solução deverá disponibilizar métricas relacionadas à eficiência e confiabilidade do processo de entrega de software, incluindo indicadores DORA, possibilitando análises por aplicação, serviço, equipe, repositório, ambiente e período.
	d) Deverá ainda fornecer visibilidade sobre a execução de testes automatizados, cobertura de código e qualidade das entregas, permitindo identificar falhas recorrentes, testes instáveis (flaky tests), degradações de qualidade e riscos associados às mudanças implantadas.
	e) A solução deverá correlacionar alterações realizadas no ciclo de desenvolvimento com impactos observados em produção, possibilitando identificar rapidamente se um deployment, commit ou alteração recente possui relação com incidentes, degradações de desempenho, aumento de erros ou problemas de segurança.
	f) A solução deverá permitir a implementação de controles de qualidade no processo de desenvolvimento, incluindo regras e políticas para validação de pull requests, assegurando aderência aos padrões definidos pelo Contratante.
3.22 Catálogo de Serviços, Scorecards e Mapeamento Operacional de Serviços	a) A solução deverá prover, de forma nativa e integrada, funcionalidades de catálogo e governança de serviços, permitindo identificar, organizar, documentar e monitorar os serviços de tecnologia utilizados pelo Contratante, bem

	como suas dependências técnicas e relacionamentos operacionais.
	b) A plataforma deverá possibilitar a descoberta e manutenção de um inventário consolidado de serviços, aplicações, APIs, componentes de infraestrutura, bancos de dados, pipelines e demais ativos relacionados, associando essas entidades aos respectivos responsáveis (owners), equipes, ambientes, criticidade, documentação operacional, runbooks e acordos de nível de serviço (SLOs).
	c) A solução deverá disponibilizar mecanismos de visualização das dependências entre serviços e componentes tecnológicos, permitindo análise de impacto, investigação de incidentes e entendimento da arquitetura operacional do ambiente. Essas informações deverão estar integradas aos dados de observabilidade, segurança, CI/CD, vulnerabilidades e gestão de incidentes.
	d) A plataforma deverá suportar a utilização de scorecards de maturidade e governança, permitindo avaliar a aderência dos serviços a padrões definidos pelo contratante, tais como monitoramento implementado, documentação disponível, definição de responsáveis, cobertura de observabilidade, requisitos de segurança e práticas de engenharia.
	e) As informações do catálogo deverão servir como elemento central de contextualização da plataforma, apoiando processos de operação, desenvolvimento, segurança, auditoria e governança tecnológica.
3.23 EUDM – Monitoramento de Dispositivos de Usuário Final, Agências e Caixas Eletrônicos	a) A solução deverá prover, de forma nativa ou por integração oficialmente suportada, funcionalidades de monitoramento de dispositivos de usuário final, abrangendo estações de trabalho, notebooks, terminais operacionais, equipamentos utilizados nas agências e caixas eletrônicos (ATMs), quando tecnicamente suportados.
	b) A solução deverá permitir o monitoramento da saúde, disponibilidade, desempenho e conectividade dos dispositivos monitorados, disponibilizando, no mínimo, informações sobre utilização de CPU, memória, disco e rede, tempo de atividade (uptime), processos monitorados, reinicializações, erros de sistema e eventos críticos.
	c) Os dados coletados deverão ser integrados aos demais domínios da plataforma, permitindo correlacionar problemas observados nos dispositivos com aplicações, serviços,

	infraestrutura, rede, incidentes, eventos de segurança e demais componentes monitorados. Dessa forma, será possível identificar rapidamente se uma degradação percebida por usuários ou agências possui origem local, de rede, aplicação ou serviços corporativos.
	d) A solução deverá permitir segmentar e analisar os dispositivos por critérios como agência, região, ambiente, sistema operacional, tipo de equipamento, criticidade ou qualquer outro atributo definido pelo Banco.
	e) Quando a instalação de agentes não for possível por limitações técnicas ou operacionais, a plataforma deverá disponibilizar mecanismos alternativos de monitoramento oficialmente suportados, preservando a capacidade de observação e correlação dos ativos.
3.24 Assistentes de IA, Agentes Autônomos e Automação de Fluxos Operacionais na Plataforma	a) A solução deverá disponibilizar, de forma nativa e integrada à plataforma, assistentes de inteligência artificial, agentes autônomos e funcionalidades de automação operacional voltadas ao apoio às atividades de monitoração, investigação e resolução de incidentes.
	b) Assistente conversacional integrado à plataforma b.1) A solução deverá disponibilizar assistente de inteligência artificial integrado à plataforma. b.2) O assistente deverá permitir consultas em linguagem natural sobre o ambiente monitorado. b.3) O assistente deverá ter acesso aos dados de observabilidade disponíveis na plataforma, incluindo métricas, logs, traces, eventos, incidentes, vulnerabilidades e alertas. b.4) O assistente deverá ser capaz de: I – sugerir hipóteses de investigação e possíveis causas associadas a eventos, alertas e incidentes; II – criar ou configurar monitores, dashboards e alertas por meio de instruções em linguagem natural; III – apresentar resumos de incidentes ativos, incluindo serviços afetados e informações disponíveis na plataforma; IV – recomendar ações de mitigação com base nos dados disponíveis; V – correlacionar informações provenientes de diferentes fontes monitoradas pela plataforma e apresentar análises consolidadas; VI – consultar o estado dos ambientes monitorados; VII – identificar aplicações, serviços ou

	componentes com degradação ou indisponibilidade; VIII – consultar alterações ocorridas em períodos específicos.
	c) Agente autônomo de investigação e remediação (SRE Agent) c.1) A solução deverá disponibilizar agente autônomo especializado em operações de confiabilidade (Site Reliability Engineering – SRE), sendo capaz de, no mínimo: I – executar atividades de análise e triagem de incidentes; II – correlacionar sinais e informações provenientes dos ambientes monitorados; III – identificar possíveis causas associadas aos incidentes analisados; IV – gerar recomendações de remediação com base nos dados disponíveis; V – integrar-se a ferramentas de ITSM para criação e atualização de registros relacionados a incidentes; VI – gerar relatórios pós-incidente contendo histórico da investigação e evidências técnicas coletadas. c.2) O agente deverá suportar protocolos abertos de integração de ferramentas, incluindo o Model Context Protocol (MCP) ou tecnologia equivalente.
	d) Agente autônomo de desenvolvimento e qualidade de código d.1) A solução deverá disponibilizar agente de inteligência artificial voltado ao ciclo de desenvolvimento de software. O agente deverá ser capaz de, no mínimo: I – correlacionar dados de observabilidade de produção com o código-fonte; II – identificar commits associados a degradações, erros ou vulnerabilidades detectadas; III – identificar funções associadas a degradações, erros ou vulnerabilidades detectadas; IV – identificar dependências associadas a degradações, erros ou vulnerabilidades detectadas.
	e) Automação de fluxos operacionais e.1) A solução deverá disponibilizar mecanismo nativo de automação de fluxos operacionais, contemplando, no mínimo: I – construção visual de fluxos de trabalho por meio de interface gráfica, sem necessidade de

	programação para os cenários suportados pela solução; II – gatilhos baseados em alertas, eventos, horários programados, webhooks, resultados de monitoramento ou sinais de segurança; III – ações nativas para envio de notificações, atualização de registros em ferramentas de ITSM, execução de scripts remotos, consultas a APIs externas, enriquecimento de contexto e controle de acesso condicional; IV – histórico auditável das execuções realizadas, contendo registros das etapas executadas, decisões tomadas, resultados obtidos e usuário responsável pela configuração; V – suporte a lógica condicional, ramificações, loops, tratamento de erros e execução paralela ou sequencial de etapas.
	f) A solução deverá suportar a integração com protocolos abertos de agentes de inteligência artificial, incluindo o Model Context Protocol (MCP).
	g) A integração com modelos de linguagem e protocolos de agentes deverá permitir acesso seguro e padronizado aos dados de observabilidade da plataforma por ferramentas externas de inteligência artificial.
	h) Os agentes e assistentes de inteligência artificial deverão operar sobre o contexto operacional da plataforma, observando os mesmos controles de acesso, permissões e políticas aplicáveis ao usuário executor, de forma a garantir a segurança, a rastreabilidade e a conformidade das ações realizadas.
	i) A solução deverá observar as políticas de segurança, privacidade e proteção de dados definidas pelo Contratante.
	j) As ações executadas de forma autônoma pelos agentes deverão ser registradas em trilha de auditoria. A trilha de auditoria deverá registrar, no mínimo: I – identificação do agente responsável; II – data e hora da ação; III – contexto da ação realizada; IV – resultado obtido.
3.25 Gerenciamento de Logs com Residência Local de Dados (Bring Your Own Cloud – BYOC)	a) A solução deverá possibilitar o armazenamento e o gerenciamento dos dados de logs em infraestrutura de armazenamento sob controle do próprio contratante, adotando modelo Bring Your Own Cloud (BYOC) ou abordagem equivalente de residência dos dados.

	b) As capacidades analíticas da plataforma deverão permanecer disponíveis mesmo quando os dados de logs estiverem armazenados em repositórios gerenciados pelo Banco.
	c) A solução deverá permitir que os dados armazenados externamente continuem disponíveis para pesquisa, correlação, investigação, geração de alertas, dashboards e demais funcionalidades da plataforma, preservando a experiência operacional unificada e a correlação com métricas, traces, eventos, dados de segurança e demais componentes monitorados.
	d) A arquitetura deverá suportar grandes volumes de dados e crescimento contínuo do ambiente monitorado, assegurando desempenho adequado para consultas e análises, bem como mecanismos de segurança compatíveis com os requisitos do Contratante.
	e) A solução deverá permitir que a gestão do ciclo de vida dos dados, incluindo retenção, arquivamento, criptografia e exclusão, permaneça sob governança do Contratante, observadas as políticas de segurança, privacidade e conformidade regulatória aplicáveis.
3.26 Aplicativo Operacional Móvel Integrado à Plataforma	a) A solução deverá disponibilizar aplicativo móvel oficial para dispositivos Android e iOS, permitindo que equipes de operação, sustentação, SRE, gestão de incidentes e plantão tenham acesso às principais funcionalidades da plataforma de observabilidade por meio de dispositivos móveis.
	b) O aplicativo deverá permitir o acompanhamento em tempo real da saúde dos serviços monitorados, incluindo visualização de dashboards, alertas, incidentes, escalonamentos, indicadores operacionais e demais informações críticas para a tomada de decisão durante a operação.
	c) A solução deverá disponibilizar mecanismos de atuação remota sobre eventos operacionais, permitindo reconhecer alertas, acompanhar incidentes, consultar evidências relacionadas, executar ações autorizadas e interagir com fluxos de gerenciamento de incidentes diretamente pelo dispositivo móvel.
	d) Deverá ainda oferecer integração com os mecanismos de notificação da plataforma, possibilitando o recebimento de alertas críticos por meio de notificações push e apoiando processos de plantão, sobreaviso e resposta rápida a incidentes.

	e) O aplicativo deverá operar com os mesmos controles de segurança adotados pela plataforma principal, incluindo autenticação segura, integração com mecanismos corporativos de identidade, controle de acesso baseado em papéis (RBAC) e rastreabilidade das ações realizadas.
3.27 Páginas de Status de Serviço para Comunicação Operacional	a) A solução deverá disponibilizar funcionalidades nativas para criação e gerenciamento de Páginas de Status de Serviço, destinadas à comunicação transparente e centralizada da disponibilidade e do estado operacional dos serviços monitorados.
	b) A plataforma deverá permitir a publicação de informações sobre incidentes, degradações, indisponibilidades, manutenções programadas e recuperação de serviços, possibilitando que diferentes públicos acompanhem, em tempo real, a situação dos ambientes e sistemas.
	c) As páginas de status deverão estar integradas aos mecanismos de monitoramento e gestão de incidentes da plataforma, permitindo atualização manual ou automática com base em alertas, eventos e incidentes registrados, reduzindo esforços operacionais e garantindo consistência das informações divulgadas.
	d) A solução deverá possibilitar a criação de diferentes páginas ou visões de status, direcionadas a públicos específicos, como equipes internas, áreas de negócio, parceiros ou usuários de determinados serviços, observando as políticas de acesso e confidencialidade definidas pelo Contratante.
	e) A solução deverá permitir a manutenção de histórico de incidentes e eventos operacionais, contribuindo para a transparência, comunicação institucional e acompanhamento dos níveis de serviço prestados.
3.28 Integração com Ambientes de Desenvolvimento Integrado	a) A solução deverá disponibilizar plugins ou extensões oficiais para ambientes de desenvolvimento integrado (IDEs), permitindo que desenvolvedores acessem informações de observabilidade, qualidade, segurança e operação diretamente em seu ambiente de trabalho, sem necessidade de alternar continuamente entre múltiplas ferramentas.
	b) Os plugins deverão possibilitar a visualização contextual de erros, exceções, vulnerabilidades, resultados de análises de código, testes, pipelines de CI/CD e demais informações relevantes associadas ao sistema em desenvolvimento. Dessa forma, os

	desenvolvedores poderão correlacionar rapidamente problemas observados em produção com o código-fonte correspondente.
	c) A integração deverá permitir acesso a informações provenientes da plataforma de observabilidade, incluindo logs, traces, métricas, eventos de erro, resultados de testes, cobertura de código e achados de segurança, facilitando atividades de diagnóstico, correção e melhoria contínua das aplicações.
	d) A solução deverá disponibilizar integração com assistentes inteligentes ou recursos de IA da plataforma, permitindo consultas contextualizadas sobre falhas, vulnerabilidades, comportamento das aplicações e impactos observados em produção.
	e) Todas as funcionalidades disponibilizadas nos plugins deverão respeitar os controles de segurança, autenticação, autorização e auditoria definidos pelo Banco, garantindo que cada usuário tenha acesso apenas às informações compatíveis com seu perfil.
3.29 Rastreabilidade de Código-Fonte e Monitoramento Nativo de Erros	a) A solução deverá oferecer integração nativa com repositórios de código-fonte e funcionalidades de rastreamento e análise de erros e exceções.
	b) A solução deverá permitir a correlação entre erros e exceções identificados em produção e o respectivo código-fonte associado.
	c) A solução deverá ser capaz de rastrear erros, exceções e falhas capturadas em aplicações monitoradas.
	d) A solução deverá permitir o agrupamento automático de erros e exceções por tipo, stack trace, versão e serviço.
	e) A solução deverá permitir a identificação automática de regressões, possibilitando detectar o reaparecimento de erros previamente corrigidos após novas implantações (deployments).
	f) A solução deverá permitir a atribuição automática de erros a commits e pull requests associados às alterações que originaram a falha.
	g) A solução deverá permitir a identificação do responsável técnico associado ao arquivo ou módulo afetado, com base no histórico de alterações disponível nos repositórios integrados.

	h) A solução deverá permitir a correlação dos erros e exceções com dados de APM, RUM e logs.
	i) A integração com os repositórios de código-fonte deverá permitir, no mínimo: I – navegação direta da linha de erro presente no stack trace para o respectivo código-fonte no repositório; II – visualização das alterações (diffs) associadas aos commits relacionados às implantações correlacionadas aos erros identificados; III – correlação entre eventos de CI/CD, implantações e o surgimento de novos padrões de erro.
	j) A solução deverá suportar o monitoramento de erros em aplicações frontend e backend.
	k) A solução deverá permitir o agrupamento automático de ocorrências semelhantes e a supressão de registros duplicados.
	l) A solução deverá permitir a configuração de monitores e alertas baseados em erros e exceções. Os monitores e alertas deverão permitir, no mínimo: I – a detecção de novos tipos de erros; II – a geração de alertas quando a taxa de erros ultrapassar limites configuráveis; III – a detecção de regressões associadas a novas implantações (deployments).
3.30 Análise de Comportamento, Jornada e Experiência Digital do Usuário (Product Analytics)	a) A solução deverá disponibilizar funcionalidades de análise de comportamento e jornada digital dos usuários, permitindo compreender como clientes e colaboradores interagem com aplicações, portais e canais digitais monitorados.
	b) A plataforma deverá possibilitar a captura e análise de eventos de navegação, interações e fluxos de utilização, permitindo identificar padrões de uso, pontos de abandono, gargalos operacionais e oportunidades de melhoria na experiência digital. Essas informações deverão ser apresentadas de forma integrada aos dados de observabilidade, possibilitando correlacionar comportamentos dos usuários com métricas de desempenho, erros de aplicação, indisponibilidades e degradações de serviço.
	c) A solução deverá permitir a construção e análise de jornadas digitais, acompanhando o percurso dos usuários em processos relevantes de negócio e identificando etapas que

	apresentem maior taxa de abandono, falhas ou redução de conversão.
	d) Deverá também possibilitar segmentações por perfis de usuário, canal, dispositivo, versão da aplicação, localização ou outros atributos relevantes, permitindo análises mais aprofundadas do comportamento observado.
	e) Todas as informações coletadas deverão respeitar os requisitos de segurança, privacidade e proteção de dados aplicáveis, incluindo mecanismos de anonimização, mascaramento e controle de acesso quando necessário.
3.31 Gerenciamento de Feature Flags e Experimentação Controlada	a) A solução deverá prover plataforma nativa de gerenciamento de ativação e desativação de recursos em tempo de execução (Feature Flags), que seja intrinsecamente integrada ao ecossistema de observabilidade, métricas e telemetria da aplicação (englobando Logs, APM - Monitoramento de Performance de Aplicações, UX - Monitoramento de Usuários Reais e SLOs).
	b) A solução deverá ser capaz de correlacionar cada mudança de estado de uma feature flag diretamente aos dados de telemetria do sistema, permitindo visualizar o impacto imediato da alteração na performance e na confiabilidade da aplicação em um painel unificado.
	c) A solução deverá suportar a orquestração de implantações graduais (Canary Releases) de novas funcionalidades, utilizando dados de monitoramento e telemetria coletados pela própria plataforma para orientar, controlar e validar a progressão das implantações.
	d) A solução deverá ser capaz de identificar degradações de desempenho, aumento na taxa de erros ou outros comportamentos anômalos decorrentes da implantação de novas funcionalidades e executar, de forma automática e em tempo real, a reversão (rollback) da implantação. Essa capacidade deverá estar disponível tanto para aplicações monolíticas quanto para arquiteturas baseadas em microsserviços, sem a necessidade de intervenção manual ou da execução de scripts customizados.
	e) A solução deve registrar as alterações de flags na linha do tempo da aplicação para facilitar a identificação da causa raiz (Root Cause Analysis) de forma ágil durante a mitigação de incidentes.
	f) A solução deve possuir mecanismos (heurísticos ou baseados em inteligência artificial/automação) para identificar, alertar e

	auxiliar na eliminação de feature flags obsoletas (stale flags), visando a simplificação da base de código e a redução do débito técnico.
	g) A solução deve ser capaz de ajustar parâmetros do sistema em tempo real e em ambiente produtivo, validando o impacto no usuário final exclusivamente com base nos dados nativos de confiabilidade.
3.32 Identificação e Proteção de Dados Sensíveis na Telemetria	a) A solução deverá disponibilizar, de forma nativa e integrada à plataforma, funcionalidades de identificação, tratamento e proteção de dados sensíveis presentes nos dados de telemetria coletados.
	b) A solução deverá permitir a identificação automática de dados sensíveis em logs, traces, eventos e demais dados de telemetria processados pela plataforma.
	c) A identificação de dados sensíveis deverá contemplar, no mínimo: I – dados de identificação pessoal, incluindo CPF, RG, CNPJ, nome, data de nascimento, endereço, e-mail e telefone; II – dados financeiros, incluindo números de cartão de pagamento, informações bancárias, números de conta e dados de transações; III – credenciais e segredos, incluindo senhas, chaves de acesso, certificados, tokens e strings de conexão; IV – dados de saúde e demais informações classificadas como dados sensíveis pela legislação aplicável ou pelas políticas definidas pelo Banco.
	d) A solução deverá permitir a aplicação de ações automáticas sobre os dados sensíveis identificados. As ações de tratamento deverão contemplar, no mínimo: I – mascaramento parcial dos dados; II – ocultação ou redação completa dos dados; III – aplicação de funções de hash irreversível; IV – manutenção dos dados originais quando expressamente autorizada por política definida pelo Contratante.
	e) A solução deverá disponibilizar catálogo pré-configurado de padrões para identificação de dados sensíveis.
	f) A solução deverá permitir a criação e manutenção de regras customizadas para identificação de dados sensíveis.

	g) As regras customizadas deverão suportar, no mínimo, expressões regulares, palavras-chave e mecanismos equivalentes de identificação.
	h) A solução deverá realizar a identificação e o tratamento dos dados sensíveis durante o processo de ingestão da telemetria.
	i) Os dados sensíveis identificados deverão poder ser tratados antes de sua indexação, armazenamento ou disponibilização para consulta pelos usuários da plataforma.
	j) A solução deverá disponibilizar relatórios e painéis de acompanhamento das ocorrências de dados sensíveis identificadas. Os relatórios e painéis deverão permitir visualizar, no mínimo: I – quantidade de ocorrências identificadas; II – tipo de dado identificado; III – regra responsável pela identificação; IV – origem dos dados; V – ação aplicada ao dado identificado.
	k) A solução deverá permitir o controle de acesso às funcionalidades de identificação e tratamento de dados sensíveis por meio de controle de acesso baseado em papéis (Role-Based Access Control – RBAC).
	l) A solução deverá manter trilha de auditoria das alterações realizadas nas regras e políticas associadas à identificação e tratamento de dados sensíveis.
	m) A trilha de auditoria deverá registrar, no mínimo, a data, o horário e o usuário responsável pela criação, alteração ou desativação de regras.
	n) A funcionalidade deverá contemplar, no mínimo, a identificação e tratamento de dados sensíveis presentes em logs e traces.
	o) A funcionalidade deverá suportar a identificação e tratamento de dados sensíveis presentes em métricas customizadas e eventos processados pela plataforma.
3.33 Segurança e Observabilidade de Modelos de Inteligência Artificial Generativa	a) A solução deverá disponibilizar funcionalidades de segurança, observabilidade e governança para aplicações baseadas em inteligência artificial generativa, integradas à plataforma de observabilidade.
	b) A solução deverá permitir o monitoramento de requisições e respostas processadas por modelos de linguagem (Large Language Models – LLMs).

	c) A solução deverá permitir a identificação de tentativas de prompt injection, jailbreak, extração de dados sensíveis e geração de conteúdo inadequado.
	d) A solução deverá permitir a identificação e o mascaramento automático de dados pessoais e informações sensíveis presentes nas entradas e saídas processadas pelos modelos de IA.
	e) A solução deverá permitir o monitoramento do consumo dos serviços de IA generativa utilizados pelas aplicações monitoradas. O monitoramento deverá permitir, no mínimo, a visualização das seguintes informações: I – consumo dos modelos utilizados; II – latência das requisições; III – custo por requisição; IV – taxa de erros das interações realizadas.
	f) A solução deverá permitir a identificação de comportamentos anômalos relacionados à utilização dos modelos de IA, incluindo, mas não se limitando a: I – alucinações recorrentes; II – desvios de tópico; III – degradação da qualidade das respostas produzidas pelos modelos monitorados.
	g) A solução deverá disponibilizar mecanismos configuráveis de guardrails para aplicações de IA generativa.
	h) Os mecanismos de guardrails deverão permitir a definição de políticas relacionadas, no mínimo, a: I – conteúdos proibidos; II – tópicos restritos; III – requisitos de formatação das respostas.
	i) A aplicação das políticas definidas deverá ser automática e auditável.
	j) Os dados monitorados pelas funcionalidades de IA generativa deverão estar integrados aos demais domínios da observabilidade da plataforma.
	k) A solução deverá permitir a correlação dos eventos relacionados às aplicações de IA generativa com serviços, usuários, aplicações e componentes de infraestrutura monitorados.
4. Requisitos não funcionais	
4.1 Segurança da Informação	a) A solução deverá atender aos mais elevados padrões de segurança da informação, garantindo a proteção dos dados processados,

	armazenados e transmitidos pela plataforma, bem como a proteção dos mecanismos de autenticação (Office 365 com autenticação em duplo fator usando usuário e senha de rede), autorização, auditoria e integração utilizados pelo Contratante.
	b) A solução deverá assegurar a confidencialidade, integridade, disponibilidade e rastreabilidade das informações, adotando mecanismos de proteção compatíveis com ambientes corporativos de missão crítica e com os requisitos regulatórios aplicáveis ao setor financeiro.
	c) Todos os dados de telemetria, incluindo métricas, logs, traces, eventos, fluxos de rede e metadados, deverão ser protegidos durante a transmissão e durante o armazenamento, mediante utilização de mecanismos robustos de criptografia e controles de segurança reconhecidos pelo mercado.
	d) A solução deverá suportar autenticação via Office 365 com autenticação em duplo fator usando usuário e senha de rede centralizada, integração com provedores de identidade e mecanismos de autenticação forte, possibilitando a aplicação das políticas de segurança definidas pelo Contratante.
	e) O controle de acesso deverá ser baseado em papéis e privilégios mínimos necessários para execução das atividades dos usuários, permitindo segregação adequada de funções administrativas, operacionais, auditoria, desenvolvimento e segurança.
	f) A solução deverá manter trilhas de auditoria completas e invioláveis sobre as ações realizadas por usuários, integrações e processos automatizados, possibilitando investigação, conformidade e rastreabilidade das operações executadas.
	g) A solução ofertada deverá possuir certificação ISO/IEC 27001 vigente e relatório SOC 2 Tipo II válido, emitidos por organismos ou entidades independentes, como evidência da adoção de controles de segurança da informação e governança compatíveis com as melhores práticas de mercado.
4.2 Conformidade e Auditoria	a) A solução deverá oferecer mecanismos abrangentes de conformidade, governança e auditoria, assegurando a rastreabilidade completa das atividades realizadas na plataforma e o atendimento aos requisitos regulatórios, normativos e institucionais aplicáveis ao Contratante.

	b) A plataforma deverá registrar de forma íntegra e auditável todas as ações relevantes executadas por usuários, integrações, processos automatizados e componentes da solução, permitindo a reconstrução completa de eventos, investigações e atividades administrativas sempre que necessário.
	c) Os registros de auditoria deverão preservar informações de autoria, data, hora, origem, tipo de ação executada, objeto afetado e resultado da operação, garantindo rastreabilidade adequada para fins de auditoria, conformidade, investigação forense e governança corporativa.
	d) A solução deverá disponibilizar mecanismos para visualização, consulta, pesquisa, retenção e exportação dos registros de auditoria, permitindo integração com ferramentas corporativas de GRC (Governança, Risco e Compliance), SIEM, auditoria e gestão de riscos.
	e) A plataforma deverá suportar classificação, identificação e proteção de dados sensíveis, incluindo mecanismos de mascaramento, segregação, controle de acesso e rastreamento de utilização dessas informações, observando os requisitos da LGPD, as normas do Banco Central do Brasil e as políticas corporativas do Contratante.
	f) Deverá ser possível implementar políticas distintas para retenção, descarte, arquivamento e recuperação de informações, considerando requisitos regulatórios, necessidades operacionais e critérios de governança definidos pelo Contratante.
	g) A solução deverá disponibilizar evidências e relatórios que apoiem processos de auditoria interna, auditoria externa, fiscalização regulatória, investigações de segurança e atividades de controle corporativo.
4.3 Escalabilidade e Desempenho	a) A solução deverá apresentar arquitetura escalável e de alto desempenho, capaz de suportar o crescimento contínuo do ambiente monitorado, assegurando estabilidade operacional, capacidade de processamento e experiência adequada aos usuários da plataforma.
	b) A plataforma deverá suportar expansão horizontal e/ou vertical dos recursos computacionais necessários para coleta, ingestão, processamento, armazenamento, análise e visualização dos dados de observabilidade, sem necessidade de

	substituição da solução ou reestruturações complexas da arquitetura.
	c) A solução deverá manter desempenho consistente mesmo diante do crescimento do volume de métricas, logs, traces, eventos, fluxos de rede, sinais de segurança e demais dados processados pela plataforma, preservando a capacidade de análise, investigação e correlação em tempo hábil.
	d) A arquitetura deverá permitir a ampliação gradual da cobertura de monitoramento, suportando a inclusão de novos servidores, aplicações, bancos de dados, dispositivos de rede, serviços, usuários, ambientes e componentes tecnológicos sem degradação significativa da operação.
	e) A solução deverá ser capaz de absorver aumentos sazonais ou permanentes de carga, bem como eventos de pico de utilização, mantendo níveis adequados de disponibilidade, desempenho e confiabilidade.
	f) A plataforma deverá disponibilizar mecanismos de monitoramento de sua própria saúde operacional, permitindo identificar gargalos, saturação de recursos, degradação de desempenho e necessidades de expansão de capacidade.
4.4 Suporte e Atualizações	a) A Contratada deverá assegurar suporte técnico especializado durante toda a vigência contratual, garantindo atendimento adequado para resolução de incidentes, esclarecimento de dúvidas, orientação técnica, suporte operacional e tratamento de problemas relacionados à plataforma e seus componentes.
	b) O suporte deverá ser prestado por profissionais qualificados e com conhecimento comprovado da solução ofertada, utilizando processos estruturados de atendimento, acompanhamento e escalonamento técnico, de forma compatível com a criticidade dos ambientes monitorados pelo Contratante.
	c) A solução deverá receber atualizações evolutivas, corretivas e de segurança de forma contínua, preservando a estabilidade operacional, a integridade das configurações implementadas e a compatibilidade com os recursos contratados.
	d) As atualizações deverão ocorrer de forma transparente e planejada, minimizando impactos à operação do Contratante e assegurando a continuidade dos serviços monitorados.

	e) Alterações relevantes de arquitetura, funcionalidades, interfaces, integrações, requisitos técnicos ou componentes da solução deverão ser comunicadas previamente ao Contratante, possibilitando análise de impacto e planejamento das ações necessárias.
	f) A Contratada deverá assegurar a manutenção da compatibilidade das integrações implantadas, garantindo retrocompatibilidade sempre que tecnicamente possível e disponibilizando orientações formais quando alterações forem necessárias.

Pelo Banco do Nordeste do Brasil S.A