Especificação Técnica

1. Objeto
   1.1. Contratação de subscrições, serviços, treinamento e consultoria, para solução de monitoração de infraestrutura, aplicações e logs no ambiente de Tecnologia da Informação.

2. Disposições gerais
   2.1. Todos os itens constantes nesta especificação técnica são de atendimento obrigatório.
   2.2. A SABESP fornecerá informações adequadas, seguindo o princípio do privilégio mínimo e necessidade de conhecimento, para todas as atividades deste objeto.
   2.3. As referências relacionadas a termos usados nesta especificação estão descritas no "Anexo III – Glossário".
   2.4. Até o máximo de 5 (cinco) dias úteis após a assinatura do contrato, a CONTRATADA e a SABESP farão uma reunião para iniciar as atividades. Após a reunião, a CONTRATADA terá o máximo de 5 (cinco) dias úteis para iniciar os trabalhos, em conjunto com a equipe técnica da SABESP.
   2.5. Para a contabilização de todos os prazos, será utilizado o calendário de feriados nacionais, em conjunto com o calendário de feriados do município de Curitiba, Paraná.

3. Dimensionamento do ambiente a ser atendido

<preencher com dimensionamento>

4. Subscrições
   4.1. A contratação será na modalidade de subscrições. A SABESP terá o direito de uso, suporte técnico e atualizações de versão durante toda a vigência do contrato.
   4.2. Esta modalidade não inclui a compra de licenças do software.
   4.3. As subscrições deverão incluir todos os softwares necessários para a execução da solução.
   4.4. Serão contratadas tantas subscrições quanto necessárias para o atendimento ao dimensionamento previsto nesta especificação.
   4.5. A contratação será para um período de 36 (trinta e seis) meses, prorrogáveis dentro dos limites das leis.

5. Serviços
   5.1. A implantação consiste em atividades de:
      5.1.1. Configuração da solução em ambiente de nuvem.
      5.1.2. Configuração do ambiente SABESP para ser monitorado pela solução, incluindo, mas não restrito a:
         5.1.2.1. Instalação e configuração de todos os componentes necessários para o correto funcionamento da solução.
      5.1.3. Documentação, em conjunto com equipes técnicas da SABESP, de todas as etapas do processo.
      5.1.4. Disponibilização da solução para os usuários;
      5.1.5. Operação assistida, por um período de 30 dias após a disponibilização para os usuários.

6. Treinamento
   6.1. Os treinamentos serão ministrados independentemente da disponibilidade de calendário da CONTRATADA e do FABRICANTE em seus centros de treinamento oficiais. Deverão ser realizados na condição de turma fech ada, ou seja, somente profissionais da SABESP poderão participar dos treinamentos.
   6.2. Se o FABRICANTE possuir programas de certificação, o instrutor deverá ser certificado, e a certificação deverá ser válida até o final do treinamento. Caso o FABRICANTE não possua programas de certificação:
      6.2.1. o FABRICANTE ele deverá fornecer uma declaração, indicando que tal programa não existe;
      6.2.2. a CONTRATADA deverá fornecer uma declaração de que o instrutor é apto a ministrar o treinamento, com conhecimentos avançados da solução.
   6.3. Todos os custos relativos a instrutores (viagem, hospedagem, alimentação, seguro, e tudo o mais necessário),
   ficarão a cargo da CONTRATADA.
   6.4. Ao final dos treinamentos, a CONTRATADA deverá distribuir fichas de avaliação da SABESP para serem preenchidas pelos participantes. Se o resultado dos treinamentos for considerado insatisfatório (avaliação média abaixo de 75% de satisfeitos), de acordo com avaliação feita pelos técnicos da

SABESP, a CONTRATADA fornecerá, sem ônus, treinamento de igual duração e conteúdo, a ser realizada por outro(s) instrutor(es). Os novos treinamentos deverão ter início em até no máximo 10 (dez) dias úteis ao(s) treinamento(s) considerado(s) insatisfatório(s).

6.5. Ao final dos treinamentos a CONTRATADA deverá emitir um certificado de participação para cada treinando, constando nome do curso, carga horária e data de realização.

6.6. Deverão ser realizados em semanas subsequentes e contíguas.

6.7. Os treinamentos devem ser ministrados de maneira remota.

6.7.1. Não serão aceitos treinamentos na modalidade EAD (Ensino à Distância), no qual as aulas ministradas são vídeos pré-gravados.

6.7.2. O instrutor deverá estar presente em todos os encontros.

6.8. A CONTRATADA poderá ministrar o curso de forma presencial.

6.9. Toda a infraestrutura para os treinamentos será fornecida pela CONTRATADA incluindo, mas não restrito a: local, equipamentos, rede, software e quaisquer outros recursos necessários para que o treinamento seja completo.

6.10. Os treinamentos a serem ministradosserão preferencialmente os cursos oficiais da FABRICANTE. É facultado o fornecimento de treinamentos customizados pela CONTRATADA, desde que contemple o conteúdo mínimo descrito nesta especificação.

6.11. Os treinamentos deverão ser ministrados e realizados em língua portuguesa, sendo que o material didático poderá estar escrito nos idiomas português ou inglês.

6.12. Deverão conter os aspectos funcionais da solução de forma a permitir que a SABESP possa conduzir o suporte e a sustentação das mesmas após o período de Operação Assistida.

6.13. Deve compreender os recursos básicos e avançados da solução, customizações, configurações e parametrizações de recursos.

6.14. Os treinamentos devem obedecer aos requisitos dispostos na tabela abaixo:

Treinamento	Carga horária mínima	Qtd. vagas	Conteúdo mínimo
1. Gestão e administração da plataforma	16	6	• Instalação de Agentes • Configuração de Agentes • Instalação e configuração de Integrações • Configuração de recursos a serem monitorados (logs, experiência de usuário, aplicações e infraestrutura) • Gestão de usuários • Gestão de licenciamento • Melhores práticas de tageamento
2. Operação e uso da plataforma	24	16	• Criação de Dashboards • Criação de Monitores • Criação de SLAs, SLOs e SLIs • Visualização de Incidentes • Visualização de Mapa de Serviços • Visualização de Traces • Visualização de Logs • Tratamento de problemas encontrados

7. Consultoria

7.1. Serão contratadas 200 (duzentas) horas de serviços de consultoria, na forma de banco de horas.

7.2. A consultoria deverá ser prestada por teleconferência, usando o software Microsoft Teams.

7.2.1. Opcionalmente a consultoria poderá ser prestada presencialmente, porém apenas com a anuência da SABESP, e em endereço previamente designado por ela.

7.3. O pedido de consultoria deverá ser feito pela SABESP com pelo menos 10 (dez) dias corridos de antecedência. Pedidos feitos com antecedência menor serão avaliados pela CONTRATADA.

7.4. As horas contratadas poderão ser usadas durante toda a vigência do contrato, sem que seja exigido

um número mínimo de horas para faturamento. Serão faturadas apenas as horas efetivamente trabalhadas.

7.5. Serão realizadas sempre em blocos de 4 (quatro) horas.

7.6. Deverá ser realizada em língua portuguesa.

7.7. A CONTRATADA deverá enviar à SABESP, com antecedência mínima de 5 (cinco) dias úteis em relação ao início do módulo, cópia do certificado fornecido pela FABRICANTE ao consultor, atestando sua capacitação técnica. O envio poderá ser feito em meio digital (e-mail). Caso o FABRICANTE não possua programas de certificação, a CONTRATADA deverá fornecer documentação comprobatória de nível de conhecimento equivalente do consultor.

7.8. Todas as custas do(s) consultor(es) com viagem, hospedagem, alimentação, seguro, e outros, ficarão a cargo da CONTRATADA.

7.9. Não poderão ser faturadas, a título de consultoria, horas trabalhadas em ambiente externo à SABESP, como, por exemplo, hotéis ou as dependências da CONTRATADA ou FABRICANTE, para atividades como as abaixo, entre outras:

7.9.1. Planejamento das atividades a serem executadas durante a consultoria

7.9.2. Reuniões internas da CONTRATADA

7.9.3. Confecção de relatórios

8. NMS - Nível Mínimo de Serviço

8.1. A solução deverá ter uma garantia de disponibilidade mensal mínima de 99,741% (noventa e nove vírgula setecentos e quarenta e um por cento) para os data centers onde os serviços estarão hospedados, sendo aceita a comprovação por meio de certificação TIA 942 TIER II.

8.2. Chamados ao suporte técnico deverão ser atendidos conforme condições abaixo:

Canal de atendimento para abertura	• telefone, através de chamada gratuita (0800 ou equivalente); • e-mail; • website.
Período de controle	• Mensal
Criticidades	• Crítica: a solução está inoperante ou indisponível; métricas não são enviadas para a solução, ou recebidas por ela; alertas não são disparados; outras funcionalidades não estão disponíveis; monitoração de serviços críticos indisponível; não há previsão de retorno. • Alta: algumas funcionalidades da solução estão indisponíveis, ou existe um problema grave de performance; monitoração de serviços críticos indisponível; há previsão de retorno. • Média: algumas funcionalidades estão indisponíveis, mas sem impactos para a atividade de monitoração. • Baixa: consultas sobre questões técnicas ou de uso da solução.
Prazos de atendimento, conforme criticidade	• Crítica: 2 horas corridas para primeiro atendimento, 1 hora corrida entre iterações • Alta: 4 horas corridas para primeiro atendimento, 2 horas corridas entre iterações • Média: 8 horas úteis para primeiro atendimento, 2 horas úteis entre iterações • Baixa: 16 horas úteis para primeiro atendimento, 4 horas úteis entre iterações Onde: • Primeiro atendimento: após a abertura do chamado pela SABESP, tempo decorrido para a CONTRATADA. • Iteração: tempo decorrido entre as respostas entre as partes (CONTRATADA e SABESP).

Forma de cálculo para controle	NSA = 100 * [(Qc – Qcf) / Qc] Onde: • NSA: Nível mínimo de serviço atingido • Qc: Quantidade de chamados abertos no período • Qcf: Quantidade de chamados que não cumpriram prazos de atendimento. Os prazos se referem ao primeiro atendimento e ao tempo entre iterações.

9. Penalidades

9.1. Serão aplicadas as seguintes penalidades, no caso de descumprimento do NMS:

Descrição	Meta	Penalidades
Não cumprimento do nível mínimo de disponibilidade da solução.	Disponibilidade mensal mínima: 99,741%	a) 10% (dez por cento) do valor mensal faturado.
Nível mínimo de serviço atingido	Índice mensal de atendimento no prazo: 100% (cem por cento)	b) 2% (dois por cento) do valor mensal faturado, para cada chamado em atraso.

10. Responsabilidades da CONTRATADA

10.1. Prestar serviços conforme requisitos mínimos apresentados neste documento.

10.2. Respeitar as normas e políticas internas da SABESP.

10.3. Manter sigilo e confidencialidade dos documentos e informações que, por força dos serviços, a CONTRATADA tenha conhecimento, não podendo divulgá-los sob qualquer pretexto.

10.4. A CONTRATADA deverá ainda assinar Acordo de Confidencialidade contido no “Anexo IV – Acordo de confidencialidade", a fim de garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso, durante a prestação dos serviços de atendimento técnico, orientação técnica e capacitação técnica.

10.4.1. O Acordo de Confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente no âmbito desta contratação, sendo que a SABESP pode solicitar a qualquer momento a comprovação dessa obrigação.

10.4.2. O respectivo termo deve ser assinado e entregue à SABESP antes do início das atividades, pela empresa e pelos técnicos envolvidos nas atividades desta contratação.

10.4.3. No caso da incorporação de novos técnicos à execução desta contratação, ele deverá assinar e entregar o Acordo de Confidencialidade antes de iniciar suas atividades.

10.5. Responsabilizar-se por todas as obrigações concernentes à legislação trabalhista dos seus funcionários.

10.6. Manter a qualificação mínima da equipe técnica responsável pelos serviços nas tecnologias exigidas pela SABESP.

10.7. Responsabilizar-se pelos custos de deslocamentos, hospedagens em função de reuniões presenciais ou quaisquer despesas relacionadas ao serviço prestado.

10.8. Revogar todas as credenciais de usuário empregadas na prestação de serviços, bem como solicitar sua revogação

à SABESP:

- no mesmo dia do encerramento das atividades da CONTRATADA previstas nesta contratação;
- imediatamente após o desligamento ou afastamento de um técnico que execute atividades desta contratação.

10.9. A SABESP reserva-se o direito de solicitar, e a CONTRATADA se obriga a atender, a substituição de profissional a

qualquer tempo, se julgar de acordo com seus próprios critérios, que ele não esteja sendo efetivo nas atividades propostas. Os motivos incluem, mas não se limitam a:

10.9.1. O desempenho do profissional não atender ao esperado para ser efetivo na execução bem sucedida dos serviços contratados;

10.9.2. Por mau comportamento ou pela prática de atos que comprometam o bom andamento dos serviços, a segurança do trabalho e as relações humanas, seja na sua equipe ou com os empregados da SABESP;

10.9.3. A eventual substituição nos termos do presente item não implicará em qualquer ônus adicional para a SABESP, sendo de responsabilidade da CONTRATADA quaisquer encargos, responsabilidades trabalhistas ou previdenciárias relativamente aos empregados substituídos ou afastados.

11. Requisitos técnicos da solução

11.1. Disponibilização da solução

11.1.1. A solução deve ser disponibilizada obrigatoriamente na modalidade *SaaS*, em ambiente de nuvem.

11.1.2. É vedado(a):

11.1.2.1. A implantação da solução na modalidade on-premise.

11.1.2.2. A implantação de qualquer tipo de hardware na infraestrutura da SABESP.

11.1.2.3. A implantação de qualquer software na infraestrutura da SABESP, exceto quando ele for parte integrante da solução. Isso inclui, mas não se restringe a agregadores de métricas, proxies e agentes.

11.1.2.4. A implantação de qualquer software nas estações de trabalho dos usuários finais.

11.1.3. No caso de ser implantado algum software na infraestrutura da SABESP, ele deverá ser desenvolvido, mantido e suportado pelo mesmo fabricante da solução.

11.2. Interface e usabilidade

11.2.1. A interface deve ser executada integralmente pelo menos nos navegadores de internet abaixo:

- Google Chrome versão 84 e superiores
- Mozilla Firefox versão 78 e superiores
- Microsoft Edge versão 79 e superiores
- Safari versão 14 e superiores

11.2.2. É vedado o uso de plugins e extensões nos navegadores web para viabilizar o uso da solução.

11.2.3. A interface deve ser adaptativa, ou seja, deve se ajustar automaticamente ao tamanho e resolução de tela, de acordo com o dispositivo usado pelo usuário final, como desktops, noteboos, tables e smartphones.

11.2.4. Permitir ao usuário definir o intervalo de tempo (data e hora inicial e final) no qual os dados serão mostrados (timeline).

11.2.5. Possibilitar triagem rápida de transações de negócio com desempenho insatisfatório, através do recurso de drill-down.

11.2.6. Permitir ao usuário definir o intervalo de tempo (data e hora inicial e final) no qual os dados serão mostrados (timeline).

11.3. Segurança

11.3.1. Prover acesso web à solução em conexão segura criptografada (HTTPS).

11.3.2. Controlar o acesso à solução a partir de perfis de usuário.

11.3.3. Permitir integração com o Microsoft Active Directory, no nível de usuários e grupos, para a autenticação e autorização de usuários, bem como para a associação de grupos aos perfis criados na ferramenta.

11.3.4. Permitir a criação de usuários e perfis locais na solução, independentemente da integração com o Microsof Active Directory.

11.3.5. No caso de a solução precisar se comunicar com a rede interna da SABESP a partir de sua plataforma SaaS, deverá ser utilizada obrigatoriamente a tecnologia de VPN site-to-site, cuja infraestrutura será fornecida pela SABESP.

11.3.6. Permitir que as permissões de acesso sejam concedidas ao nível de interface e funcionalidade, de modo que seja possível que, numa mesma tela da solução, sejam dadas permissões diferentes

para determinados usuários.

11.3.7. Permitir a consulta de ações realizadas por usuário, apresentando quais informações foram alteradas por ele, e em qual data e hora, através de relatórios de trilha de auditoria.

11.3.8. Ser aderente à LGPD (Lei Geral de Proteção de Dados) ou GDPR (General Data Protection Regulation).

11.4. Alertas

11.4.1. Permitir a criação de alertas para qualquer métrica individual ou grupos de métricas configuradas na solução.

11.4.2. Permitir que a visualização de alertas se adeque ao perfil do usuário logado.

11.4.3. Permitir a configuração de thresholds para qualquer métrica monitorada.

11.4.4. Deflagar alertas quando uma regra for violada, permitindo notificações no mínimo por:

- Email, contendo obrigatoriamente o link direto para acessar a violação.
- Chamadas a webhooks de outras ferramentas.
- Chamadas a APIs de outras ferramentas.

11.4.5. Permitir a inserção de comentários em alertas e notificações. Comentários devem poder ser customizados, com informações constantes no alerta.

11.4.6. Permitir múltiplas condições, usando lógica E/OU, para disparo de alertas e execução de ações.

11.4.7. Permitir desativação de regras temporariamente, para períodos de manutenção.

11.4.8. Combinar diferentes métricas, com uma lógica complexa, em uma única regra de ação/alerta.

11.4.9. Classificar alertas em categorias, de acordo com sua criticidade.

11.4.10. Permitir o agrupamento de métricas em categorias.

11.4.11. Permitir a detecção de alertas usando pelo menos os seguintes métodos:

- Threshold: quando thresholds configurados no alerta forem ultrapassados.
- Mudança: quando o valor de uma métrica for alterado por um determinado período de tempo, sendo que o período é configurável.
- Baseline: quando uma métrica se comporta de maneira diferente de seu comportamento passado.
- Valor atípico: quando uma métrica agrupada tem um comportamento atípico das demais métricas de um grupo.
- Predição: avalia o comportamento e fatores relacionados a uma métrica, detectando quando houver
  a possibilidade futura dela ultrapassar um threshold. Por exemplo, se uma aplicação grava muitos arquivos em disco (como logs e imagens, entre outros), é possível deflagrar um alerta quando houver a possibilidade de exaurir o espaço em disco.

11.4.12. Gerar alertas baseado nas alterações de *baselines*.

11.4.13. Disponibilizar alertas para as seguintes métricas:

- infraestrutura: memória, CPU, disco e rede;
- aplicação: tempos de resposta, taxa de falhas, taxa de erros;
- experiência do usuário: quantidade de ações de usuário, duração das ações de usuário;
- bancos de dados: tempos de resposta, taxa de falhas e taxa de erros.

11.4.14. Gerar apenas um alerta para um problema. Se um problema afetar vários serviços ou aplicações, a solução deverá deflagrar apenas um alerta, identificando que todas as falhas fazem parte de um único problema. Deve possibilitar a detecção da causa raiz do problema através de inteligência artificial.

11.4.15. Permitir a automatização de procedimentos de escalonamento de alertas.

11.5. APIs

11.5.1. A solução deve prover uma API, de modo que suas funcionalidades possam ser acessadas por outros softwares, obrigatoriamente através de web services.

11.5.2. Todas as chamadas à API devem ser autenticadas, com fornecimento de usuário e senha, ou outro método fornecido pelo FABRICANTE.

11.5.3. A solução deve permitir auditoria das requisições feitas à sua API, permitindo identificar no mínimo, mas não apenas:

- Data e hora do acesso ao web service
- Usuário
- Endereço IP do chamado

- Web service chamado
- Resultados obtidos

11.5.4. A API deve ter documentação detalhada, disponível no site da FABRICANTE, contendo para cada webservice no mínimo as seguintes informações, mas não restrita a:

11.5.4.1. Métodos HTTP usados na requisição (GET, POST, etc).

11.5.4.2. Explicação sobre seu uso.

11.5.4.3. Ao menos 1 (um) exemplo de uso, utilizando sempre o comando *curl* do sistema operacional Linux.

11.5.4.4. Para as requisições:

- modelo da requisição (todos os argumentos possíveis de uso, com seus respectivos tipos e descrições).
- exemplo da requisição.

11.5.4.5. Para as respostas:

- status HTTP da resposta.
- modelo da resposta (todos as informações retornadas, com seus respectivos tipos e descrições), para cada status HTTP possível da resposta.
- exemplo de resposta.

11.6. OpenShift

11.6.1. A solução deve ser compatível com OpenShift, versão 4.3 e superiores.

11.6.2. Deve reconhecer os containers automaticamente e monitorar a plataforma OpenShift.

11.6.3. Deve monitorar todos os aspectos do OpenShift, da aplicação até a camada de infraestrutura, correlacionando todos os eventos, métricas e logs baseados em tags em caso de problemas.

11.6.4. Permitir a extração de labels e annotations dos containers como tags.

11.6.5. Permitir a criação manual de tags.

11.6.6. Fornecer um painel único com informações do cluster, contendo no mínimo as seguintes informações:

- uso real de CPU dos nodes de aplicação e infraestrutura (valores mínimo, máximo e médio);
- uso real de memória dos nodes de aplicação e infraestrutura (valores mínimo, máximo e médio);
- uso real de CPU dos containers nos nodes de aplicação (valores mínimo, máximo e médio);
- uso real de memória dos containers nos nodes de aplicação (valores mínimo, máximo e médio);
- recursos disponíveis de CPU para execução de containers nos nodes de aplicação (valores mínimo, máximo e médio);
- recursos disponíveis de memória para execução de containers nos nodes de aplicação (valores mínimo, máximo e médio);

11.6.7. Fornecer dados detalhados dos nodes do OpenShift, de modo a permitir a compreensão de como os nodes individuais são usados.

11.6.8. Fornecer informações de infraestrutura dos nodes de aplicação.

11.6.9. Permitir, a partir da página de detalhes de um node, *drilldown* para seus componentes, permitindo evoluir até o nível do código sendo executado dentro dos containers.

11.6.10. Deverá fornecer no mínimo as seguintes métricas relacionadas ao ambiente OpenShift:

- Infraestrutura
  - Uso de CPU
  - Uso de memória
  - Uso do espaço em disco
  - Desempenho do disco
  - Tráfego de rede
- Métricas ETCD
- Kubernetes
  - estado de containers
  - estado dos containers
  - eventos
  - volumes
  - deployments
  - replicas

- estado do daemonset
- estado dos jobs
- estado dos nodes
- resource quota
- número de containers sendo executados

11.6.11. Fornecer dashboards pré configurados para as seguintes tecnologias:

- Kubernetes
- Istio
- CRI-O

11.7. Funcionalidades gerais da solução

11.7.1. A solução deverá usar agentes instalados ou carregados nos servidores e aplicações para a coleta de métricas. O agente será responsável pela coleta de toda as informações de desempenho e disponibilidade associadas ao servidor.

11.7.2. A solução deverá um único agente, que deverá ser capaz de coletar as métricas exigidas nesta especificação. É vedada a instalação ou carga de mais de um agente no servidor ou aplicação.

11.7.3. O agente da solução deverá ser capaz de descobrir as tecnologias suportadas nos servidores onde for instalado, bem como os processos, serviços e aplicações.

11.7.4. A solução deverá monitorar fim-a-fim aplicações web, Java, PHP e Python, hospedadas na infraestrutura da SABESP. Para isso, deverá mostrar automaticamente a ligação entre a aplicação *front-end* com todas as transações executadas no *back-end*, a partir de uma ação do usuário, chegando ao nível de código, serviço e banco de dados.

11.7.5. Prover automática e dinamicamente baseline de todas as métricas para identificar desvios de comportamento, reduzir alarmes falsos e eliminar definição de parâmetros de limites estáticos.

11.7.6. A solução deverá monitorar aplicações construídas com diversidade de plataformas tecnológicas.

11.7.7. A monitoração fim-a-fim das aplicações deve ser automática e sem que seja necessária a alteração de seu código fonte.

11.7.8. Ao detectar um problema na aplicação ou na experiência do usuário, a solução deverá:

- identificar automaticamente e com uso de inteligência artificial todas as métricas afetadas pelo problema, de modo a possibilitar a identificação da causa raiz do problema;
- correlacionar o problema com os componentes da aplicação ou da infraestrutura que que está degradando o desempenho, incluindo suas métricas de negócio;
- a correlação deve fornecer uma visão fim a fim da transação, identificando os tempos totais e parciais de cada componente envolvido;
- permitir acessar o caminho completo da transação de usuários afetados.

11.7.9. Acrescentar um overhead máximo de 3% ao consumo de recursos de servidores onde o agente for instalado. Para este cálculo, será usada a média de consumo de recursos dos últimos 30 (trinta) dias.

11.7.10. Permitir selecionar o período de tempo com base no qual as informações serão mostradas na ferramenta. Por exemplo, mas não restrito a: tempo real, 15 minutos, últimas 24 horas, última semana.

11.7.11. Possuir retenção de até 1 (um) ano de histórico das métricas coletadas, com granularidade mínima de 15 (quinze) segundos, sem efetuar qualquer tipo de consolidação dos dados.

11.7.12. Os agentes da solução devem ser compatíveis com os seguintes sistemas operacionais:

- AIX versão 7.1 e superiores
- CentOS versão 6 e superiores
- Microsoft Windows 10
- Microsoft Windows Server 2008 e superiores
- Red Hat Enterprise Linux versão 6 e superiores
- SuSE Linux Enterprise versão 11 e superiores

11.7.13. Deve permitir o monitoramento de dispositivos via SNMPv2 e SNMPv3.

11.7.14. É vedado que a solução dependa de qualquer tipo de extensão ou integração para seu funcionamento, em qualquer de suas camadas, como por exemplo, mas não restrito a servidores, aplicações e navegadores.

11.7.15. É permitido o uso de extensões ou integrações, desde que ela seja desenvolvida, mantida e suportada pelo FABRICANTE, nos mesmos termos que a solução, nesta especificação. A comprovação se dará via documentação oficial do FABRICANTE.

11.7.16. A solução deve permitir a criação de SLAs, SLOs e SLIs.

11.8. Dashboards

11.8.1. A solução deverá fornecer uma plataforma para criação de *dashboards* customizáveis.

11.8.2. Os dashboards deverão ser baseados em métricas e outras informações fornecidas pela solução, correlacionando-as ao comportamento da aplicação.

11.8.3. Deverá ser possível incluir nos dashboards qualquer informação ou métrica fornecida pela solução.

11.8.4. É vedada a construção ou customização de dashboards através de desenvolvimento de código ou uso de APIs.

11.8.5. Os dashboards devem ser dinâmicos, de acordo com filtros aplicados a eles. Por exemplo, um dashboard sem filtros mostra os tempos de resposta mais alto de todas as aplicações monitoradas; se aplicado um filtro para uma aplicação, apenas os dados desta aplicação serão considerados.

11.8.6. Para a aplicação de filtros, é obrigatório que eles sejam informados no próprio dashboard, sendo vedada a edição ou alteração do dashboard para que as novas informações sejam mostradas.

11.8.7. Permitir a filtragem de dados utilizando as tags disponíveis.

11.8.8. Permitir que as tags sejam informadas de maneira informativa, a partir de uma lista. Quando uma tag for selecionada, os valores disponíveis para ela devem poder ser selecionados, de forma que o usuário não precise digitar nenhuma informação para compor o filtro.

11.8.9. Mostrar métricas do APM, logs, experiência do usuário infraestrutura e rede correlacionadas.

11.9. Monitoração de Aplicações

11.9.1. A solução deve descobrir automaticamente a arquitetura das aplicações, identificando todos os componentes com as quais ela interage, como por exemplo, mas não restrito a: servidores, bancos de dados e chamadas a serviços externos.

11.9.2. A descoberta automática deverá permitir o correlacionamento automático das informações dos componentes, mesmo que sejam de diferentes tecnologias.

11.9.3. Deverão ser descobertos no mínimo os elementos a seguir, mas não restrito a eles:

- conexões HTTP/HTTPS;
- web services;
- bancos de dados;
- serviço de mensageria ActiveMQ;
- serviços de cache;
- chamadas a serviços externos;
- chamadas a outros servidores.

11.9.4. Deverá ser apresentado um mapa da aplicação, a partir do qual os componentes mostrados poderão ser acessados.

11.9.5. Permitir que a partir de um componente selecionado, seja possível exibir todos os demais componentes relacionados a ele. Por exemplo: selecionando um banco de dados, deve ser possível visualizar todas as aplicações que o utilizam.

11.9.6. A monitoração da aplicação deverá ser iniciada no momento da inicialização do servidor de aplicações onde está hospedada.

11.9.7. A solução deve apresentar graficamente, para cada aplicação:

11.9.7.1. um mapa, a partir do qual os componentes mostrados poderão ser acessados, e que deverá ser atualizado dinamicamente, de forma automática, no caso de a aplicação ser alterada;

11.9.7.2. a visibilidade fim-a-fim, mostrando os diversos estágios das aplicações sem a necessidade de instalação de agentes adicionais;

11.9.7.3. um gráfico com a distribuição de frequência dos tempos de resposta das chamadas para componentes e serviços externos;

11.9.7.4. visão pré-definida das principais métricas e análises fornecidas pela solução. Deverá permitir a criação e customização de painéis, gráficos ou mapas com a inclusão ou retiradas de informações disponibilizadas pela solução;

11.9.7.5. mapa com a análise de desempenho da aplicação, identificando os serviços e infraestrutura utilizada por ela, bem como informações a respeito dos acessos de origem das transações, como navegador e visão geográfica dos acessos;

11.9.7.6. mapa apresentando o volume de execuções e tempos médios de resposta entre todos

os componentes da aplicação, de acordo com a escala e período de tempo indicado;

11.9.7.7. visualização de desvios da baseline da aplicação.

11.9.8. A solução deve identificar automaticamente transações de negócio, iniciadas no mínimo, mas não restrita, pelas seguintes tecnologias:

- protocolos HTTP/HTTPS;
- web services;
- serviços de mensageria;
- chamadas externas;
- servidores remotos.

11.9.9. A solução deve identificar para cada transação de negócio:

- a satisfação do usuário segundo o padrão APDEX;
- mapa da topologia da transação, com as mesmas funcionalidades do mapa da aplicação;
- o fluxo e a arquitetura completa da transação.

11.9.10. A solução deve monitorar 100% (cem por cento) das execuções das transações de negócio, mostrando no mínimo as seguintes métricas:

- quantidade de execuções;
- tempos de resposta;
- volume de erros.

11.9.11. A solução deve permitir classificar e quantificar as execuções das transações, de acordo com seu tempo de resposta, tipo de erro e volume de erros. A classificação e quantificação deverá permitir a estratificação no mínimo por:

- aplicação;
- transação de negócio;
- servidor de aplicação.

11.9.12. A solução deve permitir executar *drilldown* detalhado do código executado (classes, métodos e instruções SQL) para 100% (cem por cento) das transações executadas nos servidores de aplicação, de forma automática e sem intervenção manual.

11.9.13. Quando um problema for detectado, a solução deverá:

- detalhar todas as informações do problema;
- identificar os serviços, aplicações e componentes da infraestrutura afetados, representando-os visualmente e os correlacionando;
- correlacionar automaticamente o problema com as métricas afetadas;
- identificar o número de usuários reais afetados;
- gravar o comportamento e a evolução do problema, identificando quando os principais eventos ocorreram e serviços impactados.

11.9.14. A solução deve permitir agrupar os problemas de mesma causa e efeitos, em tempo real e mantendo o histórico.

11.9.15. A solução deve detectar eventos ocorridos na aplicação, como por exemplo, mas não restrito a reimplantação e reinicialização.

11.9.16. Permitir a análise e comparação de métricas de diferentes versões da solução.

11.9.17. A solução deve identificar sem intervenção manual, o baixo desempenho ou travamento dos seguintes componentes:

- transações de negócio
- instruções SQL
- backends

11.9.18. A solução deve identificar automaticamente o baseline de novos componentes monitorados, sem intervenção manual.

11.9.19. Monitorar classes e métodos das aplicações.

11.9.20. Monitorar fim a fim as aplicações, registrando e analisando no mínimo:

- a requisição do usuário no navegador (por exemplo, mas não apenas cliques, rage cliques, links acessados e carga de páginas);
- execução de códigos nos servidores de aplicação, identificando webservices e chamadas a serviços externos de suas transações;
- instruções SQL.

11.9.21. Permitir a monitoração de aplicações implantadas pelo menos nos seguintes ambientes de nuvem:

- Amazon Web Services (AWS)
- Google Cloud
- Microsoft Azure

11.9.22. A monitoração de aplicações implantadas em ambiente de nuvem deve ter as mesmas funcionalidades da monitoração de aplicações implantadas na infraestrutura própria da SABESP.

11.9.23. A solução deverá permitir a captura de informações de chamadas a APIs REST. Deve ser possível capturar, no mínimo, mas não restrito a:

- método utilizado;
- recurso chamado;
- parâmetros informados na URL;
- formato de retorno;
- conteúdo da resposta;
- status HTTP da resposta.

11.10. Monitoração de Rede

11.10.1. Coletar informações de desempenho de rede e network flows.

11.10.2. Realizar a verificação automática de desempenho e disponibilidade da rede por processo (JVM, .NET etc.), coletando e exibindo, no mínimo, mas não restrito às métricas de rede a seguir:

- informações de tráfego de entrada e saída;
- disponibilidade;
- taxa de transmissão e retransmissão;
- erros e perdas de pacotes das interfaces de rede.

11.10.3. Realizar a verificação automática de desempenho e disponibilidade da rede por host monitorado, correlacionando problemas de rede a problemas em aplicações.

11.10.4. Identificar dispositivos, *data centers* e regiões geográficas com baixo desempenho de rede, correlacionando-os com problemas em aplicações.

11.10.5. Para os hosts monitorados, fornecer as seguintes informações, para a origem e destino de cada conexão:

- protocolo (pelo menos, mas não restrito aos protocolos TCP e UDP);
- endereço IP;
- porta;
- direção (entrada ou saída);
- volume dos dados enviados;
- throughput dos dados enviados;
- volume dos dados recebidos;
- throughput dos dados recebidos;
- número de frames TCP retransmitidos;
- latência das conexões TCP;
- RTT variance.

11.10.6. Além das informações exigidas no item anterior, se uma conexão tiver como origem ou destino um container, deverá identificar também:.

- ID do container;
- nome do container;
- nome da imagem;
- tag da imagem;
- implantações realizadas no container;
- namespace;
- nome do container.

11.10.7. Apresentar graficamente um mapa dinâmico, de todas as conexões de rede monitoradas. A partir do mapa deverá ser possível:

- selecionar qualquer uma das conexões;
- isolar conexões com problemas de performance;
- diagnosticar problemas em balanceamento de carga entre os containers de um cluster;
- identificar serviços, incluindo aplicações, responsáveis por tráfego de alto volume;

11.11. Monitoração de Logs

11.11.1. Permitir a análise dos logs das aplicações, serviços e infraestrutura permitindo criar alertas quando da ocorrência de palavras ou grupos de palavras existentes nos logs.
11.11.2. Permitir o uso de uso de expressões regulares para a análise dos logs.
11.11.3. Permitir que sejam geradas métricas a partir de logs, de modo que seja possível manter as informações por um período prolongado de tempo.
11.11.4. Permitir a consulta em tempo real dos logs, sejam eles indexados ou não.
11.11.5. Acessar logs associados a partir de uma métrica monitorada.
11.11.6. A partir de um log, acessar o dashboard com as métricas do host.
11.11.7. A partir de um log, acessar o dashboard com as métricas da aplicação.
11.11.8. Permitir filtrar quais entradas do log devem ser indexadas.
11.11.9. Permitir filtrar quais entradas do log serão visualizadas.
11.11.10. Permitir processar automaticamente os logs dos componentes monitorados pela solução.

11.12. Monitoração da Experiência do Usuário

11.12.1. A solução deverá monitorar a experiência dos usuários finais de aplicações para ambiente web e aplicações para dispositivos móveis.
11.12.1.1. Em aplicações para ambiente web, é vedada qualquer tipo de alteração manual nas aplicações, para obter a monitoração. Entretanto, é permitida a inserção automática de *snippets* JavaScript pela solução nas aplicações.
11.12.1.2. Em aplicações para dispositivos móveis, é permitida a alteração da aplicação, mas apenas para configurar a monitoração.
11.12.1.3. A monitoração deverá monitorar aplicativos sendo executados no mínimo, mas não restrito, nos seguintes sistemas operacionais móveis:
- iOS 12 e superiores;
- Android 9 e superiores.

11.12.2. A solução deverá permitir a captura de dados na página executada no navegador do usuário. Deve ser possível capturar, no mínimo, mas não restrito a:
- Meta tags (nativamente);
- Parâmetros informados na URL (nativamente);
- Variáveis de JavaScript (nativamente ou por instrumentação do código fonte);
- Dados de formulários (nativamente ou por instrumentação do código fonte).

11.12.3. A solução permitir a identificação e coleta de todas as ações realizadas pelo usuário na página da aplicação, tais como cliques e "*rage clicks*", mesmo que estas ações não façam chamadas aos servidores de aplicação.
11.12.4. Realizar a verificação do desempenho das ações dos usuários exibindo no mínimo, na linha do tempo, as informações abaixo:
- quantidade de ações;
- duração das ações;
- resultado (por exemplo: sucesso, erro, timeout, etc.);
- tempo de execução.

11.12.5. Apresentar ao menos as seguintes informações para cada ação de usuário nas aplicações:
- falhas e erros de JavaScript ocorridos;
- origem geográfica das ações;
- navegador de origem;
- duração;
- distribuição da quantidade de ações por duração;
- chamadas a serviços de terceiros por períodos de tempo histórico.

11.12.6. Apresentar, para os erros de JavaScript encontrados nas aplicações, as seguintes informações do cliente , indicando a quantidade de erros para cada uma delas:
- sistema operacional;
- navegador, incluindo sua versão;
- localidade;
- ação que gerou o erro;

11.12.7. Identificar, para cada requisição web, a satisfação do usuário segundo o padrão APDEX.
11.12.8. Mostrar tempos de carga de páginas, erros de frontend e duas dependências, para os ambientes web e móvel.
11.12.9. Permitir filtrar erros .

11.13. Integração com bancos de dados

11.13.1. É vedada a instalação de agentes nos servidores de bancos de dados, bem como a alteração de qualquer parâmetro dos bancos e servidores, para sua monitoração.

11.13.2. Verificar o desempenho de todas as chamadas a bancos de dados feitas pelas aplicações e serviços.

11.13.3. Suportar no mínimo os seguintes bancos de dados:

- DB2
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP Hana
- SQL Server

11.13.4. Exibir no mínimo as seguintes informações para as conexões com os bancos de dados:

- Taxa de falhas
- Tempo médio de resposta
- Quantidade de conexões por período de tempo

11.13.5. Exibir, para todas as instruções SQL executadas:

- quantidade de execuções, taxa de falha, o tempo de resposta médio;
- permitir a identificação de qual serviço ou aplicação fez a chamada, independentemente da plataforma tecnológica de origem;

11.14. Inteligência Artificial (IA) e Machine Learning (ML)

11.14.1. Dispor de motor de IA e ML atuando em todos os itens monitorados simultaneamente

11.14.2. O motor de IA e ML deve prover funcionalidades de correlação de eventos, devendo suportar os seguintes tipos de correlação:

- deduplicação - quando múltiplos eventos repetitivos são recebidos para o mesmo incidente de um mesmo elemento de infraestrutura, devendo registrar o evento apenas uma vez;
- topologia - suprimir os eventos gerados a partir de elementos relacionados entre si, onde um destes elementos é o causador do incidente.

11.14.3. Oferecer algoritmos para detecção de anomalias, entre eles, mas não apensa:

- Forecast;
- Outliers;
- Correlations;
- Anomaly Detection.

11.14.4. Oferecer algoritmos com *Continuous Scan* de métricas para detecção automática de anomalias, sem a necessidade de criação de alertas para cada métrica coletada.

12. Homologação

12.1. O primeiro colocado será convocado e deverá fornecer o ambiente de homologação, demonstrando as capacidades técnicas, funcionalidades e comportamentos previstos na especificação técnica.

12.2. As atividades deverão contemplar no mínimo os seguintes procedimentos:

12.2.1. Realização de reunião de *kick-off* para validação do escopo e requisitos para as atividades.
12.2.2. Configuração da solução de acordo com as melhores práticas do fabricante.
12.2.3. Criação de usuário para administração do ambiente, sendo ele o administrador principal da solução.
12.2.4. Criação de usuários para acesso a solução de APM.
12.2.5. Instalação dos agentes nos servidores definidos na reunião de kick-off.
12.2.6. Acompanhamento do restart, das máquinas físicas/virtuais após a instalação dos agentes.
12.2.7. Configuração das aplicações, definidas na reunião de kick-off, a serem monitoradas pela solução de APM.
12.2.8. Configuração do controle de sessões de usuários que serão monitoradas para cada uma das aplicações elencadas na reunião de kick-off.
12.2.9. Criação de até um parâmetro para coleta de informações que estão trafegando por uma transação.
12.2.10. Criação e customização de ao menos 1 (um) dashboard, de acordo com as métricas, filtros e tags definidos pela SABESP.
12.2.11. Configuração de recebimento de e-mail, para envio de alertas da solução de APM.

12.3. Deverá ser avaliado se a solução:
12.3.1. Possui interface de operação e administração, exclusivamente WEB.
12.3.2. Permite a monitoração de aplicações hospedadas em ambiente próprio da SABESP.
12.3.3. Não apresenta incompatibilidades apesar da diversidade de plataformas tecnológicas, versões e distribuições providas por fornecedores de marcas variadas, tanto de hardware quanto de software.
12.3.4. Permite verificar o acompanhamento da experiência do usuário final no acesso às aplicações.
12.3.5. Realiza a verificação da performance e disponibilidade das seguintes plataformas tecnológicas:
- Aplicações do tipo Web (HTTP e HTTPS);
- Linguagem Java;
- Servidores de aplicação JBoss e Tomcat;
- Bancos de dados ORACLE;

12.3.6. Identifica problemas ocorridos no ambiente, de forma automática e inteligente, verificando, além do impacto do problema, a causa raiz do mesmo, em tempo real e mantendo o histórico do diagnóstico.
12.3.7. Realiza o monitoramento fim-a-fim de aplicações, registrando e avaliando, no mínimo, se:
- A requisição feita pelo usuário no navegador (click e carga de páginas);
- A execução do código nos servidores de aplicação;
- As consultas aos servidores de banco de dados;
- O retorno do resultado ao navegador do usuário;
- E identificando webservices e chamadas a serviços externos das transações de uma aplicação.

12.3.8. É capaz de realizar a correlação de eventos e análise aprofundada do desempenho e disponibilidade de aplicações, podendo chegar até o nível de classes e métodos da aplicação.
12.3.9. É capaz de correlacionar automaticamente e de forma gráfica, todos os componentes descobertos incluindo, hosts, processos, serviços e aplicações e suas dependências.

12.4. A equipe avaliadora da SABESP terá autonomia técnica para avaliar cada quesito constante nesta especificação, podendo decidir se a demonstração feita pela licitante atende aos itens solicitados. No caso de não atendimento, a equipe avaliadora justificará sua decisão.
12.5. As atividades serão realizadas de maneira remota, utilizando a plataforma Microsoft Teams.
12.6. As atividades ocorrerão dentro de um prazo máximo de 5 (cinco) dias corridos a partir da aceitação da proposta do primeiro colocado.
12.7. A SABESP definirá qual ambiente (servidores e aplicações) serão usadas para as atividades.
12.8. Em caso de necessidade decorrente da falta de escopo da(s) aplicação(ões) para demonstração de atendimento de algum requisito, será permitido que o licitante demonstre o item em ambiente diferente do usado para o teste. Neste caso:
- a demonstração deverá ser on-line e estar operacional;
- não será permitido em hipótese alguma o uso de documentação, print de tela ou apresentações;
- este recurso somente poderá ser utilizado por decisão exclusiva da SABESP, quando entender que a impossibilidade de comprovação do item é culpa exclusiva dos dados, da aplicação ou do ambiente interno.

12.9. Em hipótese alguma será gerado algum custo para a SABESP, decorrente da execução destas atividades.

12.10. Para a verificação dos requisitos técnicos, capacidades e comportamentos, a SABESP avaliará individualmente os requisitos técnicos. Para isso, poderão ser realizados testes de performance na aplicação, alterações no ambiente da aplicação, desligamento pontual da aplicação, novos *deploys*, bem como utilizar de outras ferramentas para aferir e comparar os resultados ou solicitar demonstrações onde seja necessária a reconfiguração ou reinstalação de algum componente da solução.

12.11. Todos os requisitos deverão ser atendidos simultaneamente, ou seja, não será permitido que para atendimento de algum item, a solução deixe de atender outro item previsto.

12.12. Caso não sejam comprovados todos os itens previstos na especificação técnica, o licitante primeiro colocado será desclassificado e será convocado o segundo colocado, assim sucessivamente.

12.13. Ao final das atividades, a solução deverá estar totalmente operacional coletando e avaliando a performance da(s) aplicação(ões) definidas. Os dados coletados e as análises feitas pela solução serão utilizados para demonstração das capacidades, funcionalidades e comportamentos.

12.14. O licitante avaliado será desclassificado no teste de conformidade se:

- não iniciar o teste dentro do prazo estabelecido;
- deixar de atender qualquer requisito previsto;
- não apresentar profissionais especializados na Solução, durante a realização do teste de conformidade ou quando solicitado pela SABESP, para o esclarecimento de dúvidas que porventura surgirem durante as atividades.

12.15. Ocorrendo alguma situação excepcional que ocasione o adiamento de qualquer das datas das atividades, o licitante será devidamente comunicado e convocado para nova data.

12.16. A SABESP emitirá o parecer de validação, com o embasamento da aprovação ou não da licitante avaliada. Caso aprovada no teste de conformidade, o pregoeiro a declarará como vencedora, procedendo à abertura do prazo recursal e demais trâmites licitatórios legais.

12.17. Desclassificado o primeiro colocado, a segunda colocada será convocada para apresentação dos documentos de habilitação, proposta de preços e para participação da prova de conceito.

12.18. O ambiente de testes deverá ser mantido até o final da fase de recursos do pregão.

12.19. O ambiente de testes não poderá ser utilizado para a implantação da solução definitiva.

13. Qualificação técnica

13.1. O Proponente deverá apresentar todos os documentos listados abaixo.

13.2. Declaração, emitida pelo FABRICANTE ou REPRESENTANTE LEGAL no Brasil, atestando que o Proponente é parceiro autorizado e está apto a comercializar e prestar os serviços previstos na presente especificação. Caso o proponente seja o FABRICANTE, não precisará apresentar esta declaração.

13.3. Atestado(s) de execução bem sucedida de prestação de serviços e consultoria, emitido(s) em nome do proponente e fornecido(s) por pessoa jurídica, que comprove o suporte técnico e consultoria bem sucedidos na solução proposta, de no mínimo 100 (cem) horas.

13.4. Atestado(s) fornecidos por pessoa jurídica e emitido(s) em nome do(s) profissional(is) que será(ão) responsável(is) pelos serviços de consultoria, comprovando a experiência bem sucedida desse(s) profissional(is) na prestação de serviços de consultoria na solução proposta, em quantidade não inferior a 50% (cinquenta por cento) do objeto licitado.

13.5. Registro em carteira profissional, contrato de prestação de serviço, pré-contrato ou contrato social comprovando o vínculo do(s) profissional(is) com o Proponente.

13.5.1. O pré-contrato a que se refere este subitem deve vincular o(s) profissional(is) ao Proponente, devendo
esta vinculação ser condicionada à assinatura do Contrato entre o Proponente e a SABESP.

13.5.2. No caso de funcionários, devem ser fornecidas as guias quitadas do FGTS.

13.6. Observações:

- O proponente poderá apresentar um ou mais atestados para comprovar a experiência na execução dos serviços de consultoria.
- Em caso de somatório dos atestados, deverá ficar comprovada a execução de horas em quantidade suficiente para comprovar o quantitativo mínimo exigido na especificação.
- É permitido que na declaração de execução de serviços em nome da proponente, o nome do profissional
  também seja especificado. Neste caso, a apresentação de um único atestado será considerada válida.
- Para a autorização de comercialização, será aceita a autorização com data de emissão até 30

(trinta) dias anteriores à data do pregão.

13.7. Todos os certificados devem ser fornecidos por Órgãos da Administração Pública ou Entidades Privadas, devidamente assinados, carimbados e em papel timbrado da empresa ou órgão tomador.

13.8. Todas as comprovações devem ser apresentadas à SABESP até a data de assinatura do contrato.

13.9. A falta dos documentos e exigências descritas nos itens acima implicará na inabilitação imediata do licitante.

13.10. A SABESP poderá promover a qualquer tempo diligência para verificar a veracidade das informações para confrontação do detalhamento das especificações desta contratação.

Anexo I – Glossário

No âmbito desta especificação, as seguintes definições devem ser utilizadas:

- AIOps - Inteligência Artificial para Operações de TI.
- APDEX - Application Performance Index, é um padrão aberto que define um método para reportar, comparar e medir todos os aspectos relativos aos tempos de resposta da aplicação. Disponível em https://www.apdex.org.
- Extensão - qualquer peça de software (como por exemplo, mas não restrito a bibliotecas, agentes e scripts), utilizados para adicionar funcionalidades à solução padrão.
- Incidente – qualquer evento que pode levar a uma parada ou perda de desempenho ou disponibilidade nos
  serviços da empresa.
- Monitor – métrica sobre a qual podem ser aplicados *thresholds*, que se forem ultrapassados devem emitir alertas no próprio software, ou em outro software a ele integrado.
- OpenShift – refere-se ao software Red Hat OpenShift Container Platform.
- PI – Application Programming Interface. Conjunto de rotinas e padrões estabelecidos por um software para a utilização das suas funcionalidades por aplicativos externos, que apenas usarão seus serviços.
- Rage click – Cliques de raiva. Ação do usuário em clicar repetidamente sobre um ponto de uma página web, normalmente quando a resposta da página está lenda.
- SaaS – Software as a Service.
- Serviço - num servidor, é qualquer funcionalidade disponibilizada, como um servidor de aplicações sendo executado.
- SLI – Service Level Indicator, são métricas que indicam como está o desempenho dos serviços.
- SLO – Service Level Objective , são objetivos que definem um nível de serviço a ser atingido. Um SLO é composto de um ou mais SLIs. Normalmente são expressos como uma percentagem num período de tempo.
- SLA – Service Level Agreement, acordo entre um fornecedor e um cliente, ou entre duas áreas da mesma organização. Mostram o que o cliente pode esperar do serviço prestado.
- Tag – também chamadas etiquetas ou marcadores, são informações disponíveis nos itens monitorados, usados para organizar, agrupar e filtrar (entre outras operações) as informações disponíveis.
- Thresholds – limites máximo e mínimo do valor de uma métrica, que causará o disparo de um alerta.

Anexo II – Acordo de confidencialidade

ACORDO DE CONFIDENCIALIDADE

Pelo presente instrumento particular, <Informar_Razão_Social>, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob nº <Informar_CNPJ>, com sede em <Informar_Cidade/UF>, neste ato representada por seu
<Informar_Representante_legal>, doravante denominada simplesmente <Informar_Empresa>, e

SABESP DISTRIBUIÇÃO S/A, pessoa jurídica de direito privado, sociedade por ações, subsidiária integral da Companhia Paranaense de Energia – SABESP com sede no Município de Curitiba, Estado do Paraná, na Rua José Izidoro Biazetto, nº 158, Bloco A, Mossunguê, CEP 81.200 -240, neste ato representada pelo seu
<Informar_Representante_legal>, doravante denominada simplesmente "**SABESP DIS**",

SABESP Geração e Transmissão S/A, pessoa jurídica de direito privado, sociedade por ações, subsidiária integral da Companhia Paranaense de Energia – SABESP com sede no Município de Curitiba, Estado do Paraná, na Rua José Izidoro Biazetto, nº 158, Bloco A, Mossunguê, CEP 81. 200-240, neste ato representada pelo seu

<Informar_Representante_legal>, doravante denominada simplesmente “**SABESP GeT**”,

SABESP Comercialização S/A, pessoa jurídica de direito privado, sociedade por ações, subsidiária integral da Companhia Paranaense de Energia – SABESP com sede no Município de Curitiba, Estado do Paraná, na Rua José Izidoro Biazetto, nº 158, Bloco A, Mossunguê, CEP 81.200 -240, neste ato representada pelo seu
<Informar_Representante_legal>, doravante denominada simplesmente “**SABESP COM**”,

SABESP Holding S/A, pessoa jurídica de direito privado, sociedade por ações, subsidiária integral da Companhia Paranaense de Energia – SABESP com sede no Município de Curitiba, Estado do Paraná, na Rua José Izidoro Biazetto, nº 158, Bloco A, Mossunguê, CEP 81.200-240, neste ato representada pelo seu
<Informar_Representante_legal>, doravante denominada simplesmente “**SABESP HOL**”,

<Informar_Empresa> e **SABESP DIS, SABESP GeT, SABESP COM, SABESP HOL** doravante também denominadas individualmente “Parte” e, em conjunto, “Partes”.

CONSIDERANDO QUE:

A <Informar_Empresa> necessita realizar acesso remoto ao ambiente de TI das Partes SABESP, resolvem estas celebrar o presente Acordo de Confidencialidade (“Acordo”), como condição para a liberação do acesso remoto, que se regerá pelas cláusulas e condições a seguir descritas:

OBJETO

Constitui objeto do presente Acordo de Confidencialidade, a obrigação de sigilo e confidencialidade em relação às informações que forem fornecidas e utilizadas pelas Partes durante o período de disponibilização da rede via acesso remoto.

INFORMAÇÕES CONFIDENCIAIS

Para os propósitos do presente instrumento, o termo “Informações Confidenciais” significa toda informação relacionada a produtos, operações reveladas ou de qualquer outra maneira tornadas disponíveis por uma das Partes, incluindo, porém sem se limitar a dados técnicos, econômicos, comerciais, jurídicos, contratuais, “know- how”, informações de clientes, declarações financeiras e contábeis, dados de empregados e diretores, gerenciamento, planejamento estratégico, políticas adotadas, informações técnicas e todas as cópias e derivados contendo tais Informações Confidenciais, ainda que não tenham sido identificadas como tal.

As Informações Confidenciais poderão ser fornecidas através dos seguintes meios, porém não se limitando a estes: mídias eletrônicas, desenhos, modelos, dados, especificações, relatórios, compilações, programas de computador, patentes, aspectos financeiros e econômicos de clientes e fornecedores, potenciais concorrentes, questões contratuais, produtos existentes e/ou futuros e outros materiais quaisquer que tenham sido obtidos e/ou conhecidos antes e/ou depois da vigência deste instrumento.

Não são consideradas Informações Confidenciais as que:

a) Sejam ou venham a ser identificadas como de domínio público;
b) Sejam expressamente identificadas pelas Partes como “não confidenciais”;

c) Devam ser divulgadas por força de lei, decisão em processo judicial ou administrativo.

USO DAS INFORMAÇÕES CONFIDENCIAIS

As Partes concordam em não revelar as Informações Confidenciais a qualquer pessoa ou entidade, sem o prévio consentimento, por escrito, da outra Parte.

As Partes não utilizarão e nem permitirão que outros utilizem quaisquer Informações Confidenciais, para qualquer outro propósito, que não aquele para o qual foram reveladas.

As Partes não poderão adulterar, alterar, reprojetar, transmitir as Informações Confidenciais sem prévia autorização, por escrito, da outra Parte.

As Partes asseguram que as Informações Confidenciais não serão mecanicamente copiadas e/ou de outra maneira reproduzidas, divulgadas, publicadas, nem serão circuladas sem prévia permissão, por escrito, da outra Parte.

As Partes obrigam-se a:

a) manter em sigilo as Informações Confidenciais, valendo-se do mesmo grau de cuidado com relação às suas próprias informações confidenciais, impedindo qualquer uso não autorizado por meio deste contrato, sua publicação ou sua comunicação a terceiros não autorizados;

b) restringir a revelação das Informações Confidenciais somente para aqueles empregados, prepostos, conselheiros e consultores das Partes que estejam participando da atividade;

c) dar ciência a seus empregados, prepostos, conselheiros e consultores, sem se limitar a estes que tiverem conhecimento das Informações Confidenciais, das obrigações assumidas no presente Acordo e da proibição de divulgação das informações fornecidas para a outra Parte;

d) não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para uso de terceiros; e

e) não efetuar nenhuma gravação ou cópia de documentação confidencial a que tiver acesso em decorrência da conexão remota.

As Partes não se obrigarão a preservar as Informações Confidenciais que:

a) são ou tornem-se publicamente disponíveis ou tornem-se publicamente disponíveis por outra maneira que não uma revelação não autorizada; ou

b) seja requerida sua revelação por qualquer foro de jurisdição competente, lei, regulação, agência do governo, órgão de controle, administração ou ordem legal, desde que a Parte requerida a revelar a Informação forneça à outra Parte aviso prévio de tal ordem ou requerimento.

Em caso de dúvida acerca da confidencialidade de determinada informação (especificações, processos, procedimentos, desenhos, amostras, entre outros), as Partes deverão tratar a mesma sob sigilo, até que venha a ser autorizado pela Parte detentora da Informação Confidencial, por escrito, a tratá-la diferentemente. Em hipótese alguma se interpretará o silêncio das Partes como liberação de qualquer dos compromissos ora assumidos.

REVELAÇÕES ÀS ENTIDADES GOVERNAMENTAIS

Caso uma das Partes venha a ser legalmente obrigada a revelar as Informações Confidenciais por qualquer entidade governamental, administrativa ou judicial competente, a mesma enviará prontamente a outra Parte o aviso por escrito, no prazo de 05 (cinco) dias, contados da notificação da entidade governamental, permitindo a outra Parte requerer medida cautelar ou outro recurso legal apropriado.

A Parte que for obrigada, por determinação legal, revelará tão somente as informações que forem legalmente exigíveis.

CESSÃO E SUCESSÃO

1. Nenhuma das Partes cederá, transferirá ou sub-rogará este Acordo a terceiros, no todo ou em Parte, sem o prévio consentimento da outra Parte contrária, salvo em se tratando de cessão às sociedades controladas, controladoras ou sob controle comum de uma das Partes, estendendo-se a essas sociedades, as obrigações de confidencialidade conforme o presente instrumento.
2. Nenhuma cláusula contida neste Acordo será interpretada como outorga ou conferência de quaisquer direitos, por licença ou qualquer outra forma, sobre Informações Confidenciais reveladas para a outra Parte.
3. Este Acordo beneficiará e obrigará as Partes e seus sucessores e não será cedido ou de qualquer outro modo transferido.
4. O presente acordo não poderá ser aditado, modificado ou renunciado, exceto se por escrito, em separado, e assinado pelas Partes.

DANOS

A não observância de quaisquer das disposições de confidencialidade estabelecidas neste instrumento, sujeitará a Parte infratora, como também o agente causador ou facilitador, por ação ou omissão, ao pagamento de multa compensatória desde já estipulada em 100% (cem por cento) do valor do contrato.

A multa prevista no item anterior deverá ser paga pela Parte Infratora no prazo máximo de 48 (quarenta e oito) horas.

VIGÊNCIA

Este Acordo vigorará pelo prazo de 10 (dez) anos, contados a partir da sua assinatura pelas Partes.

DEVOLUÇÃO DAS INFORMAÇÕES

No término da vigência deste Acordo ou mediante requisição de uma das Partes, todas as cópias de quaisquer Informações Confidenciais e partes delas que permanecerem em posse de uma Parte deverão ser devolvidas a outra Parte ou destruídas, mediante certificação, não subsistindo nenhum outro compromisso ou responsabilidade.

DAS DISPOSIÇÕES GERAIS

O disposto no presente instrumento não obrigará, ou de qualquer outro modo, comprometerá as Partes, direta ou indiretamente, a estabelecer qualquer relação de negócio, concluir uma transação ou celebrar qualquer tipo de acordo entre si.

As partes contratantes declaram, sob as penas da Lei, que os signatários do presente instrumento são seus procuradores/representantes legais, devidamente constituídos na forma dos respectivos Contratos/Estatutos Sociais, com poderes para assumir as obrigações ora CONTRATADAs.

DO FORO

As Partes elegem o foro da Comarca de Curitiba, Estado do Paraná, para dirimir quaisquer dúvidas ou controvérsias oriundas deste instrumento, com renúncia a qualquer outro, por mais privilegiado que seja.

E por estarem assim justas e acordadas, as Partes assinam este Acordo em 02 (duas) vias, de igual forma e teor, para um só efeito, na presença de 02 (duas) testemunhas.

Curitiba, DD de MÊS de ANO.

Pela

<SABESP DISTRIBUIÇÃO S/A>

Pela

<SABESP GERAÇÂO e TRANSMISSÃO S/A>

Pela

<SABESP COMERCIALIZAÇÂO S/A>

Pela

<SABESP HOLDING S/A>

Pela

<Informar_Empresa>

Testemunha

Testemunha