REDE BLOCKCHAIN BRASIL

ATA 014 DE REUNIÃO DO COMITÊ EXECUTIVO

Às 11 horas do dia 14 de dezembro de 2023, através da plataforma Teams, reuniram-se os representantes dos Partícipes Patronos e dos Partícipes Aderentes Associados da Rede *Blockchain* Brasil – RBB, conforme lista de presentes abaixo, para discussão e deliberação sobre os assuntos tratados na Ordem do Dia a seguir.

Ordem do Dia

Observadas as cláusulas do Acordo de Cooperação n° D-121.2.0014.22, celebrado entre os Partícipes para a criação e manutenção da RBB e sem prejuízo do que vier a dispor o Regulamento da RBB:

1. Apreciação sobre o Manual de Operações;

2. Apreciação sobre cronograma de implantação do piloto; e

3. Informes.

Relato

1. Apreciação sobre o Manual de Operações.

Dando continuidade à reunião anterior, o Comitê Executivo, foi convidado a apreciar o Manual de Operações, conforme comunicado por e-mail e anexo a esta ata.

A representante da PRODEMGE, Mônica Azara, esclareceu que a instituição não emitiria voto por conta de impossibilidade momentânea de participar do piloto.

A proposta foi **aprovada** com o voto dos demais representantes presentes: TCU, BNDES, CPQD e Dataprev.

Lembrando que são 6 com direito a voto no total (TCU, BNDES, CPQD, Dataprev, PRODEMGE e RNP) e os votantes superam os 50% necessários para aprovação.

2. Apreciação sobre cronograma de implantação do piloto.

Dando continuidade à decisão do Comitê Executivo na reunião anterior, o representante do BNDES, Gladstone Arantes, apresentou a proposta de cronograma apreciada pelo Comitê Técnico para a implantação do piloto da RBB. O cronograma prevê uma versão piloto inicial da RBB com a participação das seguintes instituições: BNDES; TCU; Dataprev; RNP; e CPQD; a PUC-Rio também participará do piloto inicial, sem nós núcleo, conforme a natureza de Partícipe Parceiro.

A proposta foi **aprovada**.

3. Informes.

<u>Estratégia Nacional de Governo Digital</u>

O representante do CPQD, José Reynaldo Formigoni, questionou se a RBB não deveria, através de algum representante ou do Comitê Executivo, realizar sugestões para a Estratégia Nacional de Governo Digital, cuja consulta pública está aberta até o dia 22/12. O

convidado do BNDES, Milber Bourguignon reportou que já tinha participado de uma reunião sobre o assunto. Ficou acertado que ambos fariam uma reunião para apresentação de sugestões, caso fizesse sentido, ponto que foi reforçado por alguns dos integrantes.

Comunicado do Representante da RNP

Em email encaminhado para todos os representantes do Comitê Executivo, o representante da RNP nesse Comitê, Leandro Ciuffo, comunicou sua impossibilidade de participar da presente reunião. Nesse e-mail, o representante da RNP explicitou seu posicionamento no sentido de aprovar tanto o Manual de Operações quanto o cronograma para implantação do piloto.

Reuniões com Instituições Interessadas

O representante do BNDES, Gladstone Arantes, reportou reunião recente com a ANEEL e com representantes do município de Araguaína, no Tocantins, ambos sobre a pertinência e interesse de adesão à rede. Outrossim, agradeceu à representante da Secretaria de Transparência e Controle do Maranhão, Nísia Seguins, pelo contato com o município de Araguaína, acrescentando que as conversas restaram bastante adiantadas, com forte demonstração do município em participar da rede, incluindo com a hospedagem de um nó do município.

4. Lista de presença na reunião

MEMBROS PRESENTES	
COM DIREITO A VOTO	
TCU	Rainério Rodrigues Leite
BNDES	Luciana Giuliani de Oliveira Reis Sérgio Marques de Viveiros Gladstone M Arantes Junior
CPQD	José Reynaldo Formigoni Filho
Dataprev	Claudemir Custódio Brum Felipe Braga Carneiro Leão
Prodemge	Mônica Rocha
SEM DIREITO A VOTO	
Sec. Transp. do Maranhão	Nísia Paixão Seguins Louzeiro Seabra

CONVIDADOS SEM DIREITO A VOTO	
BNDES	Milber Fernandes Morais Bourguignon
Sec. Transp. do Maranhão	Steferson Lima Costa Ferreira

ANEXO I

Manual de Operações

Manual de Operações da Rede Blockchain Brasil

1. OBJETIVOS

1.1. Este Manual de Operações tem como objetivo definir as **ATIVIDADES DE OPERAÇÃO DA RBB** (Rede Blockchain Brasil), conforme definição do **REGULAMENTO DA RBB**, nos itens 3.6 e 3.2.

1.2. Conforme os itens 4.1.2.2, 4.1.5.1 e 4.3.2.1, este Manual de Operações foi inicialmente proposto pelo **COMITÊ TÉCNICO DA RBB** e foi aprovado pelo **COMITÊ EXECUTIVO DA RBB**, podendo ter sua atualização delegada ao **COMITÊ TÉCNICO DA RBB**.

1.3. Neste Manual de Operações, o Acordo de Cooperação nº D-121.2.0014.22 passa a ser denominado apenas de "**ACORDO**". Também serão utilizados os termos mais diretos: **REGULAMENTO, COMITÊ EXECUTIVO** e **COMITÊ TÉCNICO**.

2. ABRANGÊNCIA E ESCOPO

2.1. Este Manual se aplica a todos os **PARTÍCIPES** da **RBB**, atuais e futuros.

2.1.1. Nos casos em que houver diferenciação das regras de acordo com a função do **PARTÍCIPE** (a saber: **PATRONOS, ASSOCIADOS** ou **PARCEIROS**), será explicitamente especificado.

2.2. As definições delegadas para o Comitê Técnico por esse Manual de Operações serão incorporadas no Anexo do Manual de Operações, cuja atualização não requer aprovação pelo Comitê Executivo.

3. DEFINIÇÕES OU ABREVIATURAS

3.1. SLA (*Service Level Agreement* ou Acordo de Nível de Serviço) – Acordo estabelecido entre prestador(es) de serviços e seu(s) cliente(s), definindo níveis de desempenho e qualidade na prestação destes serviços.

3.2. OLA (*Operational Level Agreement* ou Acordo de Nível Operacional) – Acordo estabelecido entre prestadores de serviços que colaboram para a entrega de um serviço acerca dos níveis de desempenho e qualidade dos serviços operacionais prestados entre eles de tal forma a buscar manter os SLAs com os clientes finais.

3.3. Horário de Serviço (*Service Hours*) – Faixa de horário dentro da qual a rede buscará estar disponível para execução de seus serviços.

3.3.1. Todos os SLAs e/ou OLAs mencionados nesse Manual de Operações deverão valer apenas dentro do Horário de Serviço.

4. SOBRE A FASE PILOTO

4.1. A RBB será considerada inicialmente em estado de piloto. Enquanto em piloto, valerão as seguintes premissas:

4.1.1. Todos os nós da RBB serão operados por instituições partícipes do Acordo.

4.1.2. Todas as transações a serem enviadas para a RBB serão assinadas por um servidor (serviço *backend*) sob a responsabilidade de um dos partícipes do Acordo.

4.1.3. Serão estabelecidos níveis de serviço mais simples e mais facilmente alcançáveis, com foco especial em segurança da informação e menos foco em disponibilidade dos serviços.

4.1.4. Fica definido o seguinte Horário de Serviço (ou *Service Hours*): dias úteis entre 9h e 18h.

4.1.4.1. Feriados locais são considerados fora do Horário de Serviço.

5. SERVIÇOS E PAPÉIS NA FASE PILOTO

5.1. Os seguintes tipos de Serviço existem na RBB: Serviços de DLT (*Distributed Ledger Technology*) e Serviços de Suporte.

5.1.1. Serviços de Suporte são fornecidos entre Partícipes da RBB com o objetivo de garantir o adequado funcionamento, operação ou evolução dos Serviço de DLT.

5.2. Os seguintes papéis existirão durante a fase de Piloto da RBB:

5.2.1. Provedores de Serviço de DLT - São todos os partícipes do Acordo que possuam nós de quaisquer tipos compondo a rede.

5.2.2. Consumidores de Serviços de DLT – Pessoas físicas ou jurídicas que utilizem um dos serviços disponibilizados.

5.2.3. Uma instituição partícipe do Acordo pode ser, ao mesmo tempo, Provedor e Consumidor de Serviço de DLT.

5.3. Sobre os Consumidores de Serviço:

5.3.1. Consumidores Permissionados são aqueles que possuem permissão expressa de um Provedor para o uso de um serviço.

5.3.2. Consumidores Públicos são aqueles que não precisam da permissão de nenhum dos Provedores de Serviço para o consumo dos serviços.

5.4. Os seguintes Serviços de DLT serão disponibilizados pela RBB durante o piloto:

5.4.1. Processamento de transações distribuídas – Serviço através do qual uma pessoa física ou jurídica, possuidora de um endereço no padrão da rede envia uma transação para ser processada pela rede, conforme os padrões definidos para redes compatíveis com o ecossistema Ethereum.

5.4.2. Acesso de leitura à blockchain (*ledger*) – Serviço através do qual uma pessoa física ou jurídica executa seu próprio nó Hyperledger Besu ou qualquer outro que atenda aos protocolos subjacentes e conecta-se a um nó de um Provedor de Serviço da RBB para ter acesso completo ao conteúdo da blockchain.

5.5. Denomina-se Item de Configuração da RBB a um componente, processo, repositório de dados ou de parâmetros ou qualquer outro elemento envolvido no provimento dos serviços oferecidos pela rede.

5.5.1. Denomina-se Configuração da RBB o conjunto de Itens de Configuração da rede.

6. INFRAESTRUTURA E NÍVEIS DE SERVIÇO

6.1. Os Partícipes do Acordo comprometem-se a disponibilizar os componentes de infraestrutura de TI com os níveis de desempenho e volumes necessários para garantir o adequado funcionamento da RBB.

6.1.1. O funcionamento adequado da RBB compreende tanto fornecimento dos Serviços de DLT dentro dos SLAs adequados quanto os Serviços de Suporte dentro dos OLAs adequados.

6.1.2. O Comitê Técnico será responsável pela definição dos Serviços de Suporte, assim como de seus OLAs.

6.2. Como princípio geral, o Comitê Técnico deve buscar concentrar-se na definição de protocolos, Serviços, SLAs e OLAs, evitando arbitrar características da infraestrutura interna dos Partícipes.

6.2.1. Os Partícipes devem ter a liberdade de compor suas infraestruturas internas, ajustando o desempenho e volumes dos seus componentes de acordo com suas realidades específicas, desde que atendam os protocolos, Serviços, SLAs e OLAs.

6.2.2. Exceções a essa regra geral devem ser aprovadas pelo Comitê Executivo, em especial se implicarem a possibilidade de verificação da infraestrutura interna de um Partícipe por parte dos outros Partícipes ou seus indicados.

6.3. O Comitê Técnico deverá definir boas práticas quanto aos componentes de infraestrutura a serem utilizados, assim como seus desempenhos e volumes, de tal forma a facilitar a composição das infraestruturas internas pelos Partícipes.

6.3.1. A definição dos componentes tecnológicos necessários, seus desempenhos desejáveis e volumes são apresentados no anexo desse Manual.

6.3.2. Os níveis de desempenho e volume a serem especificados dependem dos componentes específicos, podendo se referir, por exemplo, a desempenho de CPU, *throughput* de canais de comunicação, *volume* de armazenamento de dados (*storage)* dos nós, número de conexões dos coletores de monitoração, entre outros.

7. PERMISSIONAMENTO E RESPONSABILIZAÇÃO

7.1. Sobre permissionamento para uso de serviços da RBB:

7.1.1. O Serviço de Processamento de Transações Distribuídas (seção 5.4.1) só estará disponível para Consumidores Permissionados.

7.1.2. O Serviço de Acesso de Leitura à Blockchain estará disponível para Consumidores Públicos.

7.2. Os Consumidores Permissionados deverão realizar um cadastro antecipado perante um Provedor de Serviço através do qual enviarão transações para a RBB.

7.3. É de inteira responsabilidade do Provedor de Serviço armazenar *off chain* (ou seja, fora da blockchain) as informações cadastrais de todos os Consumidores Permissionados que houver permissionado, incluindo todo o histórico cronológico dos permissionamentos, em conformidade com a LGPD.

7.4. O Provedor de Serviço precisará permissionar o Consumidor Permissionado através do uso de um ou mais contratos inteligentes (*smart contracts*) disponibilizados para tal e denominados, em conjunto, de Contrato Inteligente de Permissionamento.

7.4.1. Tal procedimento deve ocorrer mesmo no caso de o Consumidor Permissionado ser o próprio Provedor de Serviço.

7.5. O Contrato Inteligente de Permissionamento deverá permitir e o Provedor de Serviço deverá:

7.5.1. Armazenar contas (endereços) de todos os Provedores de Serviço responsáveis por realizar permissionamento, denominadas Contas Administradoras (pelo menos, uma por Provedor de Serviço).

7.5.2. Armazenar as contas (endereços) de todos os Consumidores Permisionados.

7.5.3. Armazenar e informar, para cada conta de um Consumidor Permissionado, qual a Conta Administradora que o permissionou, garantindo o não repúdio da informação.

7.5.4. Manter uma prova criptográfica vinculada a cada conta de Consumidor Permissionado para validar a integridade dos dados cadastrais fornecidos pelo Provedor de Serviço no ato de permissionamento, garantindo a verificação inequívoca de que os dados apresentados a qualquer momento correspondem exatamente aos originalmente cadastrados.

7.5.4.1. Tal prova criptográfica também deverá provar inequivocamente a ciência do Consumidor Permissionado acerca da realização do cadastro e das responsabilidades daí decorrentes.

7.5.4.2. A implementação da prova criptográfica, assim como de todas as funcionalidades aqui demandadas precisa aderir aos ditames da LGPD.

7.5.5. No início da fase piloto, antes da implementação das funcionalidades necessárias no Contrato Inteligente de Permissionamento para garantir a viabilidade das cláusulas 7.5.4 e 7.5.4.1, assume-se que o Consumidor Permissionado será sempre o próprio Provedor de Serviço que passa a assumir todas as responsabilidades daí decorrentes.

7.5.6. Após a implementação das referidas funcionalidades, os Consumidores Permissionados que também forem Provedores de Serviço deverão realizar o

cadastro através do Contrato Inteligente de Permissionamento da mesma forma que quaisquer outros Consumidores Permissionados.

7.6. Toda e qualquer atividade ilegal originada a partir de uma transação enviada à rede será de inteira responsabilidade do Consumidor Permissionado que detém a conta signatária da referida transação.

7.6.1. Na eventualidade de o Provedor de Serviço falhar em divulgar as informações cadastrais da conta originadora da transação sob escrutínio legal, ou em comprovar a integridade e consentimento do Consumidor Permissionado, conforme estabelecido nas cláusulas 7.5.4 e 7.5.4.1, ou ainda, na situação prevista na cláusula 7.5.5, o Provedor de Serviço assumirá responsabilidade solidária por quaisquer atos ilícitos consequentes de transações enviadas pela conta permissionada e será sujeito a responder legalmente.

8. MONITORAÇÃO

a) Definições.

8.1. Monitoração - No contexto desse Manual de Operações, monitoração é a atividade de coletar informações sobre os serviços e a infraestrutura da RBB com o objetivo de acompanhar seu funcionamento e permitir a tomada de ações para garantir o funcionamento adequado destes serviços.

8.1.1. Monitoração local - Refere-se à monitoração coletada por um partícipe sobre seus próprios nós da RBB.

8.1.2. Monitoração descentralizada ou federada – Refere-se à monitoração coletada por um partícipe sobre os nós de outros partícipes da RBB.

b) Protocolos para monitoração.

8.2. A monitoração da RBB será descentralizada ou federada. Assim todos os partícipes deverão disponibilizar informações dos seus nós para a monitoração federada a ser realizada pelos outros partícipes.

8.2.1. O Comitê Técnico poderá definir exceções.

8.3. A disponibilização das informações se dará através de protocolo técnico definido pelo Comitê Técnico, incluindo requisitos de autenticação.

8.4. O conjunto de informações a serem compartilhadas entre os partícipes será definido pelo Comitê Técnico.

8.5. O Comitê Técnico deve buscar definições técnicas que minimizem tanto os riscos de segurança quanto o consumo de recursos da monitoração descentralizada.

8.6. As especificações técnicas definidas pelo Comitê Técnico constarão no Anexo desse Manual de Operações.

9. INCIDENTES

a) Definições.

9.1. Incidente – Evento não planejado que cause impacto na disponibilidade ou qualidade do serviço.

9.2. Incidente crítico – Tipo de incidente com potencial de dano maior, que possa afetar a confidencialidade, privacidade ou integridade das informações, a imagem pública das instituições, ou que cause maior impacto na disponibilidade ou qualidade do serviço. Demanda atenção mais urgente de tratamento.

9.2.1. O Comitê Técnico poderá definir os critérios para classificar um incidente como crítico, desde que não conflitem com as definições deste Manual de Operações.

9.3. Causa raiz – Subconjunto de características da RBB que são a causa, mesmo que indiretamente, de um ou mais incidentes. Uma causa raiz poderá gerar diversos incidentes se seu estado não for alterado.

9.4. O tratamento de um incidente resulta no restabelecimento do funcionamento adequado dos componentes afetados, mas nem sempre implica a solução da causa raiz do incidente.

b) Protocolo para tratamento de incidentes.

9.5. Os membros do Comitê Executivo, representando cada partícipe, deverão definir Gestores de Incidentes do partícipe que representam.

9.5.1. Para cada partícipe, será necessário haver a previsão de, pelo menos, um Gestor de Incidentes disponível para ser acionado durante todo o Horário de Serviço.

9.5.2. Havendo substituição de um Gestor de Incidentes, tal ocorrência deverá ser comunicada a todos os Partícipes através do canal definido no item 9.6.

9.6. Os Gestores de Incidentes de todos os partícipes se comunicarão através de uma ou diversas ferramentas de comunicação a serem definidas pelo Comitê Técnico.

9.6.1. Será mantido um canal de comunicação exclusivo, em separado, para avisos de incidentes críticos.

9.7. No caso de identificação de um incidente por um partícipe, um Gestor de Incidentes deste poderá comunicar a ocorrência na ferramenta de comunicação de incidentes, buscando a colaboração com os diversos partícipes na sua correção, identificação ou caracterização.

9.7.1. É esperado que os Gestores de Incidente das diversas instituições colaborem com seus pares da RBB para a saúde geral da rede, inclusive realizando consultas, alinhamentos e interlocuções com os outros funcionários das suas instituições que possam auxiliar no intento.

9.7.2. Deve-se manter o canal de incidentes críticos exclusivo para comunicação de incidentes críticos para os quais se acredite que a participação dos outros Gestores de Incidentes seja necessária para sua correção.

9.8. No caso da comunicação de ocorrência de incidentes críticos por um Gestor de Incidentes no canal exclusivo para tal fim, cada Gestor de Incidentes tem as seguintes obrigações:

9.8.1. Responder à mensagem original e estar disponível em até 2 horas (dentro do Horário de Serviço) para trabalhar no tratamento do incidente crítico.

9.8.1.1. Nos casos em que a comunicação de incidente crítico fizer referência a um problema na infraestrutura de um subconjunto de partícipes, o OLA acima só se aplica aos Gestores de Incidentes destes partícipes.

9.8.2. Manter os esforços necessários para o tratamento do incidente crítico.

9.8.3. No caso de necessidade de realização de ações síncronas ou semissíncronas entre os partícipes que sejam essenciais para o tratamento de Incidentes Críticos (restart dos validadores, por exemplo), os partícipes se comprometem a:

9.8.3.1. Realizar a atividade em até 16h (dentro das Horas de Serviço).

10. SEGURANÇA

a) Definições.

10.1. Segurança na RBB – A RBB será considerada segura se todos os acessos a informações, funcionalidades, administração e infraestrutura subjacente (incluindo outras infraestruturas dos partícipes não obrigatoriamente ligadas à RBB) estiverem garantidamente disponíveis apenas às pessoas físicas ou jurídicas adequadas, impedindo acessos espúrios, tanto propositais quanto acidentais, além de mau funcionamento provocado por ações deliberadas.

10.1.1. A definição de Segurança, no contexto da RBB, está diretamente associada ao conceito de cyber-segurança e de segurança da informação, conceitos muito usados no mercado.

10.2. Incidente de Segurança – Incidente em que ocorra a quebra da segurança da RBB.

10.3. Exploração de Segurança – Ação proposital de agente malicioso buscando quebrar a segurança da RBB.

10.4. Vulnerabilidade de segurança – Situação em que o estado ou uma característica da RBB permite uma Exploração de Segurança da rede.

10.5. Vulnerabilidade Crítica de Segurança é uma Vulnerabilidade de Segurança cuja possível Exploração de Segurança pode gerar um Incidente Crítico de Segurança.

b) Atividades de Segurança da RBB.

10.6. Conforme demanda dos Comitês Executivo ou Técnico, os Partícipes deverão disponibilizar recursos humanos e de infraestrutura para a realização das seguintes atividades. Tais atividades podem ser executadas periodicamente, com periodicidade definida por um dos Comitês.

10.6.1. Estratégia Geral de Segurança – Desenvolvimento de uma estratégia conjunta para garantir a segurança da RBB, incluindo o tratamento de vulnerabilidades e incidentes de segurança.

10.6.2. Avaliação de Risco de Segurança – Atividade em que os Partícipes, em conjunto, levantam riscos de impacto na Segurança da rede.

10.6.3. Análise de Segurança – Atividade em que os Partícipes levantam o estado de Segurança da RBB, realizando atividades como varreduras de vulnerabilidade, pentest, mapeamento dos sistemas e serviços, entre outras atividades capazes de identificar possíveis brechas de Segurança.

10.6.4. Os Partícipes da RBB deverão elaborar um processo de auditoria de aceite de contratos inteligentes a serem implantados na rede.

10.6.4.1. Após sua elaboração e adoção, os Partícipes se comprometem a submeter todos os contratos inteligentes a este processo de auditoria antes de implantá-los na rede.

c) Protocolos para Incidentes de Segurança da RBB.

10.7. Uma Vulnerabilidade Crítica de Segurança pode ser, opcionalmente, tratada como Incidente Crítico.

10.7.1. Para isso, basta que um Gestor de Incidentes realize a comunicação no canal exclusivo de Incidentes Críticos.

10.7.2. Nos casos previstos nesse Manual de Operações e seus Anexos, uma Vulnerabilidade Crítica de Segurança será automaticamente considerada um Incidente Crítico de Segurança.

10.8. O Comitê Técnico deverá manter uma lista de critérios para definição dos Incidentes Críticos de Segurança.

10.9. O Comitê Técnico deverá manter um Catálogo de Incidentes Críticos de Segurança com os exemplos que servirão para uma reflexão antecipada sobre estas possíveis ocorrências.

10.9.1. Devem-se estabelecer possíveis ações necessárias para mitigação (evitar) e tratamento (após ocorrência) dos Incidentes Críticos.

10.9.2. Todos os partícipes comprometem-se a executar os procedimentos necessários para o tratamento dos Incidentes Críticos, conforme as ações previstas no Catálogo Incidentes Críticos.

10.9.3. O Catálogo de Incidentes Críticos poderá incluir Vulnerabilidades Críticas de Segurança que se julguem necessário serem tratadas com a mesma prioridade e com os mesmos mecanismos dos Incidentes Críticos.

10.9.3.1. As avaliações de severidade e potencial gravidade das Vulnerabilidades de Segurança devem considerar a CVSS (*Common Vulnerability Scoring System*).

d) Compromissos Específicos Acerca de Vulnerabilidades Críticas de Segurança.

10.10. O acesso não autorizado às chaves privadas de um nó validador ou dos endereços usados para realizar o permissionamento, conforme item 7.4 deste Manual de Operações, é considerado uma Vulnerabilidade Crítica de Segurança. Por isso, os partícipes comprometem-se a:

10.10.1. Realizar uma gestão responsável de suas chaves privadas, de tal forma a garantir a não ocorrência de vazamento.

10.10.2. Manter um conjunto separado de chaves dedicadas apenas e exclusivamente à execução das atividades de permissionamento descritas no item 7.4.

10.10.3. Responsabilizar-se pelas consequências, inclusive judiciais, das ações resultantes do vazamento de tais chaves privadas a atores maliciosos ou não.

10.11. A detecção de que o Permissionamento de Endereços se encontra desabilitado em um nó validador de um partícipe será considerada uma Vulnerabilidade Crítica de Segurança.

10.11.1. Havendo uma monitoração para detectar tal condição, os partícipes se comprometem a comunicar no canal de Incidentes Críticos o mais rapidamente possível a ocorrência do evento.

10.11.2. Os partícipes com Permissionamento de Endereços desabilitado comprometem-se a ativá-lo o mais rapidamente possível.

11. UPGRADE SÍNCRONO.

11.1. *Upgrade Síncrono* - Mudança de versão (em geral, para uma mais nova) de um Item de Configuração da RBB que exija a sincronização total ou parcial entre os partícipes.

11.2. A partir da aprovação pelo Comitê Técnico de um *Upgrade Síncrono*, os partícipes se comprometem a realizar as atividades necessárias em, no máximo, duas semanas.

11.2.1. Excetuam-se os casos em que a realização de *Upgrade Síncrono* é parte do tratamento de um Incidente Crítico, caso em que são enquadrados nos termos específicos.

12. ON BOARDING.

12.1. *On Boarding* – Inclusão de um novo partícipe na rede.

12.1.1. A atividade de *On Boarding* de um partícipe implica tarefas para outros partícipes, como a abertura de regras de firewall, votação de validadores etc.

12.2. Após a aprovação da adesão de um novo partícipe pelo Comitê Executivo, o Comitê Técnico decidirá o cronograma da incorporação desse partícipe à rede.

12.2.1. A adesão efetiva do Partícipe à rede, inclusive com seus nós tem como pré-requisitos a designação de representantes no Comitê Técnico e de designação de Gerentes de Incidentes, assim como outras demandas que se fizerem necessárias nesse Manual de Operações, no Regulamento ou no Acordo.

12.2.2. No caso de haver demanda do novo Partícipe Aderente para entrada dos seus nós na rede, o Comitê Técnico deverá apreciar a demanda em, no máximo, duas reuniões.

12.2.2.1. O *On Boarding* deverá ser iniciado em, no máximo, duas semanas após a reunião de apreciação pelo Comitê Técnico.

12.2.2.2. A execução do *on boarding* só deverá ser postergada em caso de problemas concretos acima do controle de todos.

ANEXO I do Manual de Operações

1. RECOMENDAÇÕES DE INFRAESTRUTURA

1.1. Conforme instruído pela cláusula 6.3 do Manual de Operações, seguem abaixo as recomendações básicas de infraestrutura para os nós da RBB:

1.1.1. CPU: 2 virtual CPUs.

1.1.2. Memória RAM: 8 GB.

1.1.3. Hard Disk: 100 GB SSD.

1.1.4. Docker versão mínima 19.03.12.

1.2. A configuração mínima típica da infraestrutura é composta por cinco cointainers, sendo quatro nós Hyperledger Besu e um Prometheus.

1.2.1. Em geral, os containers dos nós Besu encontrar-se-ão em diferentes hosts.

1.2.2. Já o container Prometheus poderá coabitar um host ou não, de acordo com a avaliação de cada Partícipe.

Lista de Assinaturas

Assinado por: GLADSTONE MOISES ARANTES JUNIOR, 033.***.***-**, assinado em: 30/01/2024
Papel: Representante BNDES

Assinado por: SERGIO MARQUES DE VIVEIROS, 612.***.***-**, assinado em: 30/01/2024
Função: Gerente
Papel: Representante do BNDES

Assinado por: LUCIANA GIULIANI DE OLIVEIRA REIS, 813.***.***-**, assinado em: 30/01/2024
Função: Chefe de Departamento
Papel: Representante BNDES

Assinado por: FELIPE BRAGA CARNEIRO LEAO, 117.***.***-**, assinado em: 02/02/2024
Papel: Representante da Dataprev

Assinado por: JOSE REYNALDO FORMIGONI FILHO, 031.***.***-**, assinado em: 02/02/2024
Papel: Representante CPQD

Assinado por: NISIA PAIXAO SEGUINS LOUZEIRO, 001.***.***-**, assinado em: 04/02/2024
Papel: Representante da Sec Trans Maranhao

Assinado por: MONICA ROCHA DE AZARA, 046.***.***-**, assinado em: 05/02/2024
Papel: Representante da Prodemge

Assinado por: CLAUDEMIR CUSTODIO BRUM, 026.***.***-**, assinado em: 05/02/2024
Papel: Representante da Dataprev

Assinado por: RAINERIO RODRIGUES LEITE, 358.***.***-**, assinado em: 06/02/2024
Papel: Representante TCU