APÊNDICE 2

MATRIZ DE RISCOS DA TECNOLOGIA *blockchain*

TRIBUNAL DE CONTAS DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

José Mucio Monteiro, **Presidente**

Ana Arraes, **Vice-Presidente**
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Raimundo Carreiro
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

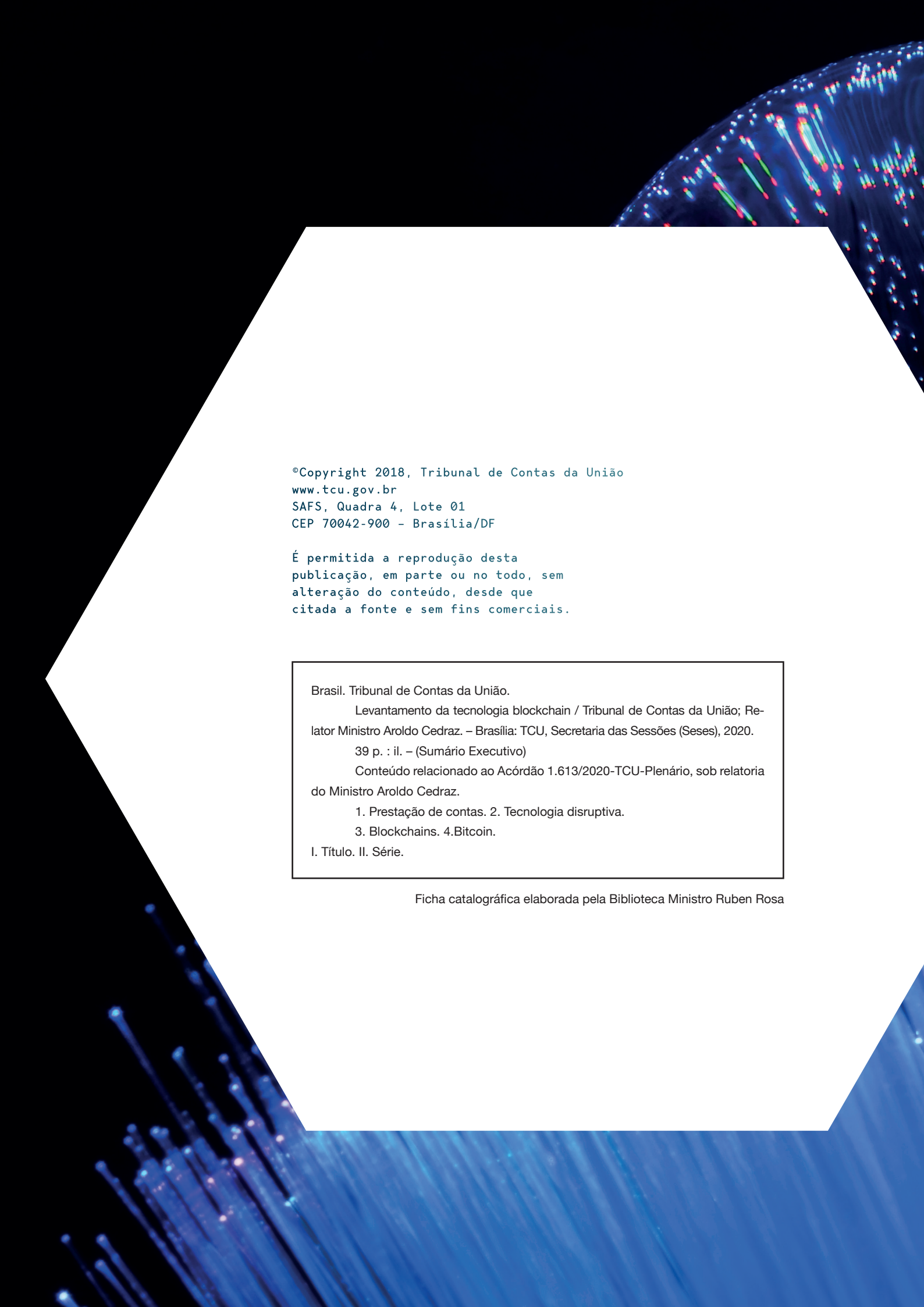
Cristina Machado da Costa e Silva, **Procuradora-Geral**
Lucas Rocha Furtado, **Subprocurador-Geral**
Paulo Soares Bugarin, **Subprocuradora-Geral**
Marinus Eduardo de Vries Marsico, **Procurador**
Júlio Marcelo de Oliveira, **Procurador**
Sergio Ricardo Costa Caribé, **Procurador**
Rodrigo Medeiros de Lima, **Procurador**

APÊNDICE 2

APLICAÇÕES *blockchain* NO SETOR PÚBLICO DO BRASIL

BRASÍLIA, 2020

TRIBUNAL DE CONTAS DA UNIÃO



Brasil. Tribunal de Contas da União.

Levantamento da tecnologia blockchain / Tribunal de Contas da União; Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria das Sessões (Seses), 2020.

39 p. : il. – (Sumário Executivo)

Conteúdo relacionado ao Acórdão 1.613/2020-TCU-Plenário, sob relatoria do Ministro Aroldo Cedraz.

1. Prestação de contas. 2. Tecnologia disruptiva.
3. Blockchains. 4.Bitcoin.
I. Título. II. Série.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

Tema: 1 - Riscos tecnológico	
Categoria de risco: Funcionamento e desempenho da rede	
Risco específico	
Não satisfação dos requisitos da aplicação pelo algoritmo de consenso escolhido	
Controles possíveis	**Critérios**
Garantir que todos os requisitos das partes interessadas sejam identificados, priorizados e registrados, com a finalidade de validar se o algoritmo de consenso escolhido atende às necessidades dos diferentes participantes da rede	COBIT BAI02 - *Managed Requirements Definition* / COBIT BAI03 - *Managed Solutions Identification and Build* / IN SGD 1/2019, art. 16, incisos I e II
Identificar qual é a topologia de rede do sistema e verificar se os nós que poderão participar do consenso são confiáveis ou não e se a organização ou o consórcio possui a quantidade suficiente de nós para executar o protocolo de consenso	
Identificar as necessidades do caso de uso quanto aos requisitos de consistência de seu estado (*safety*) e o progresso do sistema (*liveness*), considerando o Teorema CAP	
Identificar as necessidades do caso de uso quanto aos requisitos de escalabilidade, segurança e descentralização, considerando o Trilema da Escalabilidade (ou Trilema de Vitalik)	
Entender o funcionamento, os incentivos, as vantagens e desvantagens de cada um dos algoritmos de consenso disponíveis para uso pela plataforma utilizada	
Avaliar a forma como os algoritmos de consenso disponíveis previnem o *double spent attack*, *51% attack* e outros ataques relacionado	
Risco específico	
Dimensionamento incorreto dos requisitos de escalabilidade e desempenho	
Controles possíveis	**Critérios**
Contabilizar a quantidade de nós e as transações por segundo (tps) esperadas pela aplicação	COBIT BAI02 - *Managed Requirements* Definition / COBIT BAI03 - *Managed Solutions Identification and Build* / COBIT BAI04 - *Managed Availability and Capacity;* IN SGD 1/2019, art. 16, inciso II
Identificar as necessidades referentes à taxa de transferência (*throughput*) e ao intervalo de transmissão à rede de transações, incluindo tempo máximo e médio de uma transação	
Verificar se o tamanho e formato do bloco são compatíveis com as necessidades da aplicação e suportados pela plataforma utilizada	
Avaliar a possibilidade de utilizar outras tecnologias que operam sobre as plataformas *blockchain*, como canais *off-chain*, para dar maior vazão à solução	
Testar a aplicação, considerando a carga máxima esperada pela rede	
Risco específico	
Definição incorreta dos direitos de acesso ao livro-razão	
Controles possíveis	**Critérios**
Definir quem são os nós validadores da rede (*commit*), ou seja, quem participa do mecanismo de consenso	COBIT DSS06 - *Managed Business Process Control*
Identificar quais são os tipos de transações, quem pode realizar essas transações (*write*), bem como quem pode visualizar (*read*) e auditar os dados da *blockchain*	
Risco específico	
Inconsistências, devido ao problema de forks, criando duas ou mais versões do livro-razão	
Controles possíveis	**Critérios**
Estabelecer a quantidade mínima de confirmações da rede que um bloco precisa para ser considerado válido pela aplicação	COBIT BAI02 - *Managed Requirements Definition*
Risco específico	
Variações excessivas dos custos associados ao uso da rede (*transaction fees*)	
Controles possíveis	**Critérios**
Estimar e incluir o valor referente às taxas de transação de *blockchain* no orçamento de TI	COBIT APO06 - *Managed Budget and Costs* / IN SGD 1/2019, art. 11, inciso IV

Categoria de risco: Integração e interoperabilidade	
Risco específico	
Problemas de desempenho e integração com sistemas *off-chain*	
Controles possíveis	**Critérios**
Identificar e mensurar o impacto da aplicação *blockchain*/DLT nos sistemas existentes, como, por exemplo, a necessidade de desenvolvimento de adaptadores de acesso	BAI03 - *Managed Solutions Identification and Build*
Verificar se a plataforma *blockchain*/DLT utilizada tem capacidade de se comunicar com outros sistemas externos: interfaces de usuário, gerenciamento de chaves criptográficas, integração da internet das coisas e de bancos de dados	
Utilizar plataformas *blockchain*/DLT que utilizem padrões de mercado. Exemplo: acesso via REST, conectores de banco de dados etc.	
Definir estratégia de realização de testes de integração com sistemas existentes	
Verificar se os sistemas *off-chain* têm desempenho compatível com a aplicação *blockchain*/DLT, a fim de atender o número esperado de requisições	
Risco específico	
Incompatibilidade entre diferentes redes *blockchain* (*Hyperledger, Corda, Quorum, ethereum* etc.)	
Controles possíveis	**Critérios**
Identificar os mecanismos disponíveis de interoperabilidade entre plataformas	BAI03 - *Managed Solutions Identification and Build*
Avaliar se a plataforma utilizada tem funcionalidade nativa para integração com outras plataformas e redes DLTs, como, por exemplo, integração *side-chain* ou método de *atomic swap*	
Verificar se o sistema DLT deve ter APIs padronizadas, como serviços de acesso, dicionário de dados, protocolo de comunicação, algoritmo de criptografia e teste do sistema, para que possa haver fornecedores que ofereçam serviços compatível	
Categoria de risco: Construção, implantação, suporte e manutenção da rede	
Risco específico	
Abandono de suporte da plataforma blockchain pelo fabricante ou consórcio de empresas responsáveis pelo desenvolvimento, pela evolução e pela manutenção do projeto	
Controles possíveis	**Critérios**
Acompanhar os repositórios de desenvolvimento (SLACK e GITHub). O acompanhamento deve ser feito pelos profissionais da organização	COBIT APO07 - *Managed Human Resources* / COBIT APO10 - *Managed Vendors*
Avaliar o nível de utilização e dominância de mercado da plataforma *blockchain* escolhida	
Risco específico	
Falha ou interrupção do projeto *blockchain*/DLT da organização	
Controles possíveis	**Critérios**
Avaliar a possibilidade de se adotar plataformas de código aberto e conduzir projeto-piloto com escopo reduzido para validar o caso de uso e os requisitos de negócio	COBIT APO04 - *Managed Innovation*
Adquirir percentual mínimo de *software* e *hardware*, necessário apenas para atender o projeto-piloto	
Risco específico	
Escolha inadequada da plataforma *blockchain*/DLT a ser utilizada pela organização ou pelo consórcio	
Controles possíveis	**Critérios**
Definir os requisitos funcionais e não funcionais relacionados ao caso de uso	COBIT BAI02 - *Managed Requirements Definition* / COBIT BAI03 - *Managed Solutions Identification and Build* / IN SGD 1/2019, art. 11, inciso II, e art. 16, inciso II
Entender os objetivos de *design*, a finalidade e a forma de funcionamento das plataformas disponíveis	
Comparar diferentes plataformas, com base na análise e avaliação das funcionalidades de cada uma	
Executar prova de conceito (POC) com as plataformas de blockchain/DLT disponíveis, inclusive as de código aberto, para avaliar qual é a mais adequada ao caso de uso, considerando os requisitos de descentralização definidos	

Risco específico	
Imaturidade das redes e plataformas de *blockchain*/DLT existente	
Controles possíveis	**Critérios**
Avaliar a possibilidade de utilizar outras soluções, tais como banco de dados distribuídos e APIs REST	COBIT BAI03 - *Managed Solutions Identification and Build*
Verificar a possibilidade de implementar uma camada de abstração para acesso aos recursos da plataforma nativa de *blockchain*	
Aguardar e monitorar evoluções tecnológicas que possam apoiar ou impactar no alcance dos objetivos de negócios	

Categoria de risco: Armazenamento de informações on-chain e *off-chain*	
Risco específico	
Inadequação do conteúdo do bloco ou das transações a serem gravados na *blockchain*	
Controles possíveis	**Critérios**
Definir quais informações e seus respectivos estados devem ou não ser armazenados na *blockchain*	COBIT BAI02 - *Managed Requirements Definition* / COBIT APO14 - *Managed Data*
Validar se o caso de uso implementado está aderente aos requisitos de negócio da organização ou do consórcio e se a execução das transações atinge o resultado esperado	
Risco específico	
Não validação da entrada de dados a serem registrados, considerando o caráter imutável de uma blockchain	
Controles possíveis	**Critérios**
Identificar quem é o responsável ou dono da informação que é registrada na blockchain, de forma a definir os critérios de validação	COBIT APO14 - *Managed Data* / *ABNT NBR ISO*/ IEC 27002:2013 – 12.4.4
Definir estratégia de como corrigir dados registrados incorretamente na *blockchain,* como, por exemplo, transações de estorno ou correção	
Selecionar um serviço de carimbo eletrônico de tempo confiável	
Risco específico	
Inviabilidade de armazenamento do tamanho da *blockchain* em um nó da rede	
Controles possíveis	
Verificar a possibilidade de mover dados que não são mais usados de forma ativa para um dispositivo de armazenamento separado, destinado à retenção por longo prazo	COBIT BAI04 - *Managed Availability and Capacity*
Definir o tamanho do bloco e da transação, considerando a capacidade de armazenamento dos nós participantes e vazão da rede	

Tema: 2 - Riscos de negócio e da governança da rede	
Categoria de risco: Necessidades de negócio da organização ou do consórcio	
Risco específico	
Inadequação do caso de uso para utilização de uma *blockchain*/DLT ou não alinhamento da solução blockchain aos objetivos estratégicos da organização ou do consórcio – adoção por “modismo tecnológico” ou influência de fornecedores	
Controles possíveis	**Critérios**
Identificar qual é o problema que a organização ou o consórcio está tentando resolver, bem como onde será criado valor com a utilização de uma solução *blockchain*/DLT (redução de custos, experiência do cidadão/ usuário, desintermediação etc.)	COBIT APO01 - *Managed I&T Management Framework* / COBIT APO02 - *Managed Strategy* / COBIT APO08 - *Managed Relationships* / IN SGD 1/2019, art. 11, inciso II / Acórdão 2.569/2014-TCU-Plenári
Utilizar um modelo de avaliação para determinar se o caso de uso da organização ou do consórcio demanda a utilização da arquitetura distribuída P2P ou pode se beneficiar da descentralização e/ou eliminação de intermediários	
Identificar como a solução *blockchain*/DLT pode beneficiar os diferentes participantes da rede	
Verificar se as partes interessadas definiram os requisitos de negócio e revisaram e aprovaram a documentação do projeto	
Elaborar estudo de viabilidade técnica para analisar se a adoção de uma blockchain/DLT é a melhor tecnologia entre as possibilidades existentes, identificando os benefícios e custos de cada solução disponível, considerando outros modelos de integração, como o uso de APIs e Dados Abertos	

Risco específico	
Resistência da organização ou do consórcio em utilizar uma solução inovadora, como a tecnologia *blockchain*/DLT	
Controles possíveis	**Critérios**
Obter engajamento da alta administração no incentivo à adoção de soluções inovadoras dentro da organização	COBIT EDM05 - *Ensured Stakeholder Engagement* / COBIT APO02 - *Managed Strategy* / COBIT APO04 - *Managed Innovation* / COBIT APO08 - *Managed Relationships*
Estimar o período em que a iniciativa apresentará resultados significativos para o negócio e começar com uma abordagem de projeto-piloto	
Mensurar o impacto pretendido com a iniciativa em termos qualitativos e quantitativos e conscientizar a alta administração sobre os benefícios da tecnologia	
Conscientizar a alta administração de que novas formas de relacionamento e cooperação aumentam a inovação e melhoram a eficiência dos serviços prestados pelas organizações públicas	

Risco específico	
Estabelecimento de empecilhos, por parte da organização ou do consórcio, para adoção de uma solução *blockchain*/DLT, por receio de perder poder sobre determinado processo/informação ou deixar de exercer uma função de negócio que atualmente desempenha ou ter prejuízo com a adoção da tecnologia distribuída, sem avaliar ameaças externas, como a implementação da solução por organizações ou consórcios concorrentes	
Controles possíveis	**Critérios**
Fornecer à alta direção uma perspectiva holística da tecnologia, levando em consideração fatores estratégicos e técnicos	COBIT EDM05 - *Ensured Stakeholder Engagement* / COBIT APO02 - *Managed Strategy* / COBIT APO04 - *Managed Innovation* / COBIT APO08 - *Managed Relationships*
Mapear as ameaças de organizações ou consórcios concorrentes e alertar a alta direção sobre os riscos de não implementação da solução	
Repensar onde a organização poderá acrescentar valor no novo processo que será executado, sem necessidade de autoridade central	
Detalhar os reais ganhos em relação à eficiência, à redução de custos e ao combate a fraude e corrupção	

Categoria de risco: Governança da rede

Risco específico	
Inadequação da estrutura de governança do consórcio ou falta de interesse de colaboração de determinados participantes	
Controles possíveis	**Critérios**
Realizar a qualificação das partes interessadas, com o intuito de identificar o ecossistema de atores vitais à solução e as áreas importantes para cooperação	COBIT EDM05 - *Ensured Stakeholder Engagement* / COBIT APO08 - *Managed Relationships*
Definir a forma de atuação dos participantes do consórcio, incluindo atividades de supervisão, controle e gerenciamento das informações registradas na *blockchain*	
Garantir que os participantes do consórcio concordem sobre as principais decisões do projeto e regras de funcionamento e governança	
Definir as diretrizes de colaboração, incluindo papéis e responsabilidades dos participantes e comitês, bem como aspectos quanto ao investimento de recursos públicos	
Avaliar quais são os incentivos à participação na rede, tais como compartilhamento de informações, aumento da celeridade e desburocratização de processos ou serviços	
Avaliar se são necessárias mudanças hierárquicas ou normativas na organização, para permitir a obtenção dos benefícios com transações distribuídas	

Categoria de risco: Recursos humanos

Risco específico
Pouco conhecimento sobre a tecnologia ou inexistência, na organização, de número suficiente de profissionais capacitados para executar o projeto pretendido

Controles possíveis	Critérios
Desenvolver estratégia para capacitar os profissionais em relação a sistemas distribuídos, arquitetura de redes, criptografia, processos de negócio e linguagens de programação para desenvolvimento de contratos inteligentes	COBIT APO07 - *Managed Human Resources*
Capacitar recursos humanos com aspectos multidisciplinares, como a escolha de uma plataforma DLT apropriada, incentivos dos mecanismos de consenso e design de governança	
Verificar se os profissionais envolvidos estão familiarizados com os padrões de mercado, a exemplo dos critérios estabelecidos pelo *Focus Group on Application of Distributed Ledger Technology do International Telecommunication Union* (ITU FG DLT) e pelo comitê técnico da Organização Internacional de Normalização (*International Organization for Standardization* – ISO/TC 307), relacionados às tecnologias DLT	
Assegurar que os profissionais envolvidos tenham consciência dos riscos e benefícios da tecnologia, bem como dos desafios da computação distribuída e das redes P2P	
Conhecer a experiência de outros órgãos em relação à implantação de projetos de *blockchain*/DLT	

Categoria de risco: Custos associados ao projeto

Risco específico
Desconhecimento do custo do projeto de implantação da solução distribuída

Controles possíveis	Critérios
Elaborar o custo total de propriedade do projeto, incluindo custos de aquisição de ativos (*hardware* e *software*), insumos, licenciamentos, pessoal e serviços, bem como possíveis despesas fixas após a implantação da solução, tais como garantia, suporte técnico e manutenção corretiva	COBIT APO06 - *Managed Budget and Costs* / IN SGD 1/2019, art. 11, incisos II, alínea "a", e I
Identificar outras entidades da administração pública que implantaram projeto blockchain/DLT e comparar os custos envolvidos	

Risco específico
Variações dos custos associados ao uso da rede

Controles possíveis	Critérios
Estimar as quantidades de transações *on-chain* e definir limites claros com despesas referentes às taxas de transação	COBIT APO06 - *Managed Budget and Costs* / IN SGD 1/2019, art. 11, inciso IV
Estimar e incluir o valor referente às taxas de transação de *blockchain*, bem como o custo de escrita, leitura e execução de contratos inteligentes, no orçamento de TI	

Risco específico
Significativo custo agregado de leitura e escrita de informações por meio da tecnologia *blockchain*, dada a necessidade de desenvolvimento de *software* de acesso aos dados da *blockchain*, o que requer conhecimento da API de acesso da plataforma *blockchain*

Controles possíveis	Critérios
Fornecer *software* de acesso às informações ("fachada") na *blockchain* permissionada. O fornecimento deve ser feito pelo gestor da aplicação, para levar a tecnologia aplicada na *blockchain* aos demais órgãos participantes. Exemplo: API, interface *web* ou outro tipo de interface visual etc.	COBIT BAI03 - *Managed Solutions Identification and Build*
Obter apoio de organizações ou órgãos mais experientes na tecnologia *blockchain*, para auxiliar o desenvolvimento interno de uma API de acesso	

Tema: 3 - Riscos na execução de contratos inteligentes (*smart contracts*) e aplicações descentralizadas (dApps)

Categoria de risco: Desenvolvimento de código e execução de aplicações

Risco específico
Imprevisibilidade lógica do contrato inteligente

Controles possíveis	Critérios
Identificar e validar condições de interrupção e término do contrato, para assegurar a resiliência do código	COBIT BAI03 - Managed Solutions Identification and Build / ABNT NBR ISO/IEC 27002:2013 – 14.2
Conduzir revisões e aceitação rigorosas de código, para garantir que o estado final dos dados na *blockchain* seja entre os participantes, tanto para condições esperadas do negócio quanto para exceções	

Documentar as situações esperadas de sucesso e insucesso dos contratos inteligentes (requisitos de negócio) por meio de testes automatizados	
Risco específico	
Erros na escrita do código fonte dos contratos inteligentes, decorrentes de falhas no *design* do *software* e entendimento dos requisitos da aplicação	
Controles possíveis	**Critérios**
Criar novos símbolos de Linguagem Unificada de Modelagem (*Unified Modeling Language* – UML), para desenho dos diagramas de solução *blockchain* e seus *patterns*, como, por exemplo, símbolos que representem aplicações híbridas, *on-chain* e *off-chain*	COBIT BAI02 - *Managed Requirements Definition* / COBIT BAI03 - *Managed Solutions Identification and Build*
Definição de *design patterns*, boas práticas de desenvolvimento e geração automática de código, baseados em modelos testados	
Utilização de *design patterns* para evolução de contratos inteligentes, como, por exemplo, *proxy*, que faz indireção à real implementação do contrato inteligente	
Uso de ferramentas de análise de código e métodos formais de testes	
Risco específico	
Erros do usuário no uso de dApps. Como, em geral, as aplicações *blockchain* permitem que o próprio usuário realize diretamente suas transações, não é difícil que um usuário leigo ou pouco experiente se confunda na manipulação de chaves públicas e privadas e envie transações para endereços inválidos, errando o endereço (chave pública) do participante ou confundindo-o entre várias chaves	
Controles possíveis	**Critérios**
Educar os usuários e descrever os procedimentos sobre a correta utilização de soluções dApps/*blockchain*	COBIT BAI02 - *Managed Requirements Definition* / COBIT BAI03 - *Managed Solutions Identification and Build*
Melhorar a usabilidade de *frontends* de dApps, para evitar que os usuários cometam erros	
Divulgar, para a comunidade usuária da aplicação, melhores práticas no uso da dApps, por meio de avisos e ajudas on-line	
Risco específico	
Perda de transações enviadas à blockchain que é acessada pela dApp. O nó *blockchain* que recebe a requisição do frontend da dApp pode estar indisponível, por ter tido o endereço trocado, ou, simplesmente, o *software* do nó pode não executar a transação por algum motivo	
Controles possíveis	**Critérios**
Fornecer, nos dApps, *frontends* robustos, que informem ao usuário a realização ou não de uma transação na *blockchain*	COBIT BAI02 - Managed Requirements Definition / COBIT BAI03 - Managed Solutions Identification and Build
Categoria de risco: Serviço de oráculo	
Risco específico	
Indisponibilidade do serviço de oráculo	
Controles possíveis	**Critérios**
Utilizar, como alternativa, múltiplas fontes de verdade, o que aumenta, inclusive, a confiança da informação gerada	COBIT BAI04 - *Managed Availability and Capacity* COBIT APO14 - *Managed Data* / ABNT NBR ISO/IEC 27002:2013 – 17.2
Conduzir revisões e aceitação rigorosas de código, para garantir que o estado final dos dados na *blockchain* seja entre os participantes, tanto para condições esperadas do negócio quanto para exceções	
Determinar a governança dos serviços de oráculo, com gerência de configuração definida: controle de versões, *pipeline* de publicação, custodiantes dos serviços definidos etc.	
Monitorar a disponibilidade dos serviços de oráculo	
Risco específico	
Violação de dados *off-chain* durante uma invocação ou um retorno do serviço de oráculo	

Controles possíveis	Critérios
Usar oráculos descentralizados e confiáveis	COBIT APO14 - *Managed Data*
Utilizar, como alternativa, soluções baseadas em múltiplas fontes de verdade (oráculos), de forma a obter um consenso sobre a informação recuperada	
Usar serviços de verificação de oráculos, que coordenam a chamada a vários oráculos, devolvendo a informação de consenso. Por exemplo, o acesso a uma informação meteorológica, para execução de um contrato inteligente, poderia se dar por meio de um serviço de verificação que pesquisasse em vários serviços de meteorologia *on-line* e entregasse a informação com maior prevalência	

Tema: 4 - Riscos de segurança da informação

Categoria de risco: Algoritmos criptográficos, gerenciamento de chaves criptográficas e assinaturas digitais

Risco específico
Quebra de primitivas criptográficas, em razão da escolha de chaves ou algoritmos fracos

Controles possíveis	Critérios
Desenvolver e implementar, caso não exista, política voltada ao uso de controles criptográficos para proteção da informação	COBIT APO13 - *Managed Security* / ABNT NBR ISO/IEC 27002:2013 – 10.1.1 e 10.1.2
Estabelecer processo de garantia da validade das chaves públicas utilizadas que verifique as propriedades matemáticas das chaves, evitando, assim, o uso de chaves fracas ou corrompidas, bem como assegurar que a aplicação utiliza números geradores aleatórios, seguros e confiáveis	
Selecionar tamanhos de chave apropriados, considerando a vida útil esperada do sistema e quaisquer dados protegidos por ele	
Selecionar algoritmos e tamanhos de bloco de acordo com os requisitos de temporalidade, eficiência e segurança, inclusive para os algoritmos de *hash*, os quais são usados na produção de blocos	
Realizar revisões periódicas para determinar se as equivalências precisam ser revisadas (por exemplo, se os tamanhos das chaves precisam ser aumentados) e os algoritmos continuam seguros	
Selecionar algoritmos de acordo com o procedimento computacional, uma vez que, eventualmente, alguns são mais eficientes a depender da função a ser executada	
Conhecer as leis ou as regulamentações e restrições nacionais e exteriores aplicáveis ao uso de técnicas criptográficas	

Risco específico
Ausência de estratégia do ciclo de vida das chaves

Controles possíveis	Critérios
Definir requisitos para o gerenciamento de chaves criptográficas ao longo de todo seu ciclo de vida, incluindo procedimentos e métodos seguros para gerar e obter certificados de chaves públicas, distribuir chaves para os usuários devidos, armazenar chaves, mudar ou atualizar chaves, revogar chaves, recuperar chaves perdidas ou corrompidas, realizar cópias de segurança, arquivar chaves, destruir chaves, manter registro e auditoria das atividades relacionadas ao gerenciamento das chaves	COBIT APO13 - *Managed Security* / ABNT NBR ISO/IEC 27002:2013 – 10.1.1 e 10.1.2
Definir papéis e responsabilidades relacionados ao gerenciamento de chaves	
Avaliar a estratégia de armazenamento das chaves criptográficas, considerando os métodos "*cold wallet*" ou "*hot wallet*"	

Risco específico
Perda acidental de chaves criptográficas

Controles possíveis	Critérios
Definir requisitos para o gerenciamento de chaves criptográficas ao longo de todo seu ciclo de vida, incluindo procedimentos e métodos seguros para gerar e obter certificados de chaves públicas, distribuir chaves para os usuários devidos, armazenar chaves, mudar ou atualizar chaves, revogar chaves, recuperar chaves perdidas ou corrompidas, realizar cópias de segurança, arquivar chaves, destruir chaves, manter registro e auditoria das atividades relacionadas ao gerenciamento das chaves	COBIT APO13 - *Managed Security* / COBIT DSS05 - *Managed Security Services* / ABNT NBR ISO/IEC 27002:2013 – 10.1
Definir papéis e responsabilidades relacionados ao gerenciamento de chaves	

Avaliar a estratégia de armazenamento das chaves criptográficas, considerando os métodos "*cold wallet*" ou "*hot wallet*	
Risco específico	
Perda acidental de chaves criptográficas	
Controles possíveis	**Critérios**
Definir procedimentos para revogação de chaves e comunicação do evento	COBIT APO13 - *Managed Security* / COBIT DSS05 - *Managed Security Services* / ABNT NBR ISO/IEC 27002:2013 – 10.1
Utilizar técnicas de backup das chaves, como o método de *12-word phrase*, bem como técnicas de "*social key recovery*"	
Risco específico	
Exposição indevida das chaves criptográficas dos nós especializados da rede a terceiros	
Controles possíveis	**Critérios**
Utilizar senhas para criptografar chaves em armazenamento local	COBIT APO13 - *Managed Security* / COBIT DSS05 - *Managed Security Services* / ABNT NBR ISO/IEC 27002:2013 – 10.1
Limitar o período pelo qual uma chave está no formato *plaintext*	
Estabelecer mecanismos de auditoria para registrar todos os acessos às chaves e usos delas	
Definir procedimentos para registro e identificação de todas as assinaturas que podem ser inválidas, devido ao comprometimento de uma chave	
Definir critérios de acesso lógico para determinar o pessoal autorizado a utilizar e gerenciar as chaves	
Utilizar mecanismos de *multisignature* para impedir que transações sejam assinadas com uma única chave roubada	
Risco específico	
Inadequação do período de tempo de guarda das chaves ou dos certificados para verificação de assinatura digital	
Controles possíveis	**Critérios**
Definir procedimentos para registro histórico e identificação das assinaturas digitais, considerando o período pelo qual a identidade do originador das informações protegidas pela chave criptográfica correspondente precisa ser verificada, ou seja, a fonte de informações precisa ser autenticada	COBIT APO13 - *Managed Security* / COBIT DSS05 - *Managed Security Services* / ABNT NBR ISO/IEC 27002:2013 – 10.1
Categoria de risco: Segurança de frontends de contratos inteligentes (*smart contracts*) e aplicações centralizadas (dApps)	
Risco específico	
Injeção de software malicioso (*phishing*), no *frontend* ou no dispositivo que executa o *frontend* da dApp, em que o usuário é ludibriado a enviar suas credenciais ou informações sensíveis	
Controles possíveis	**Critérios**
Utilizar técnicas *anti-phishing*, como não abrir *e-mails* suspeitos ou clicar em *links* em textos e imagens de *e-mails* de quem não se conhece	COBIT APO13 - *Managed Security* / ABNT NBR ISO/IEC 27002:2013 – 12.2
Verificar endereços de origem e destino das transações	
Autenticar *endpoints* com a utilização de certificados digitais aderentes aos padrões da ICP-Brasil ou certificados *Secure Sockets Layer (SSL)*	
Risco específico	
Exposição do código fonte do contrato inteligente. Devido ao caráter contratual, que envolve várias partes, a exposição do código fonte do contrato inteligente pode ser necessária. Pessoas mal-intencionadas podem utilizar essa exposição para atacar a aplicação	

Controles possíveis	Critérios
Para aplicações ou redes permissionadas, adotar acordos de confidencialidade (*Non Disclosure Agreement* – NDA), de modo a ratificar a necessidade de não divulgação do código fonte a pessoas não autorizadas ou envolvidas no contrato	COBIT APO13 - *Managed Security* / ABNT NBR ISO/IEC 27002:2013 – 7 e 18

Risco específico
Risco no gerenciamento de chaves pelos usuários, tendo em vista que podem armazenar suas chaves de forma inadequada, compartilhá-las com terceiros, ser roubados (*hack*), ser persuadidos por alguém a informá-las ou perdê-las

Controles possíveis	Critérios
Educar os usuários e descrever os procedimentos sobre a correta utilização de soluções dApps/*blockchain*	COBIT APO13 - *Managed Security* / ABNT NBR ISO/IEC 27002:2013 – 7 e 18
Melhorar a usabilidade de *frontends* de dApps, para evitar que os usuários cometam erros	
Divulgar, para a comunidade usuária da aplicação, melhores práticas no uso da dApps, por meio de avisos e ajudas *on-line*	

Categoria de risco: Nós e componentes da rede

Risco específico
Problemas relacionados à visibilidade dos nós e componentes participantes da rede

Controles possíveis	Critérios
Estabelecer um processo formal de aprovação, registro e cancelamento dos nós, para permitir atribuição dos direitos de acesso	COBIT DSS05 - *Managed Security Services* / COBIT DSS06 - *Managed Business Process Controls* / ABNT NBR ISO/IEC 27002:2013 – 9
Definir restrições no acesso à solução *blockchain* (escrita, validação e visualização), de acordo com as necessidades da aplicação, com o intuito de impedir que dados sensíveis de *blockchains* permissionadas sejam descobertos sem autorização explícita	
Verificar como o sistema habilita os desenvolvedores, bem como especificar a autorização e confidencialidade dos contratos inteligente	

Risco específico
Ataques aos nós especializados da rede

Controles possíveis	Critérios
Implementar segurança de terminal adequada, que inclui desenho, implementação e manutenção de controles que garantam a segurança na prestação de serviços, como, por exemplo, controles preventivos de acesso e *firewalls*, e medidas para identificar a ocorrência de um incidente, como, por exemplo, monitoramento de rede e sistema	COBIT DSS05 - *Managed Security Services*

Risco específico
Vulnerabilidades no código-fonte da plataforma *blockchain*/DLT

Controles possíveis	Critérios
Garantir que existam controles de segurança adequados para repositórios de códigos, como, por exemplo, segregação de funções, processo de aprovação de alterações, controles de acesso	COBIT DSS05 - *Managed Security Services* / ABNT NBR ISO/IEC 27002:2013 – 12.6
Conduzir testes de penetração extensivos na aplicação *blockchain*	
Monitorar as vulnerabilidades de *blockchain*, como, por exemplo, ataque de 51%, ataque de gasto duplo, contratos inteligentes maliciosos, ataque de negação de serviço (DoS), ataque *Sybil*, farejamento de pacotes	

Risco específico
Ataques em que uma interface se faz passar por uma entidade oficial e simula executar as transações ou requisições desejadas pelo usuário, como ataques do tipo *Man-in-the-Middle* (MITM)

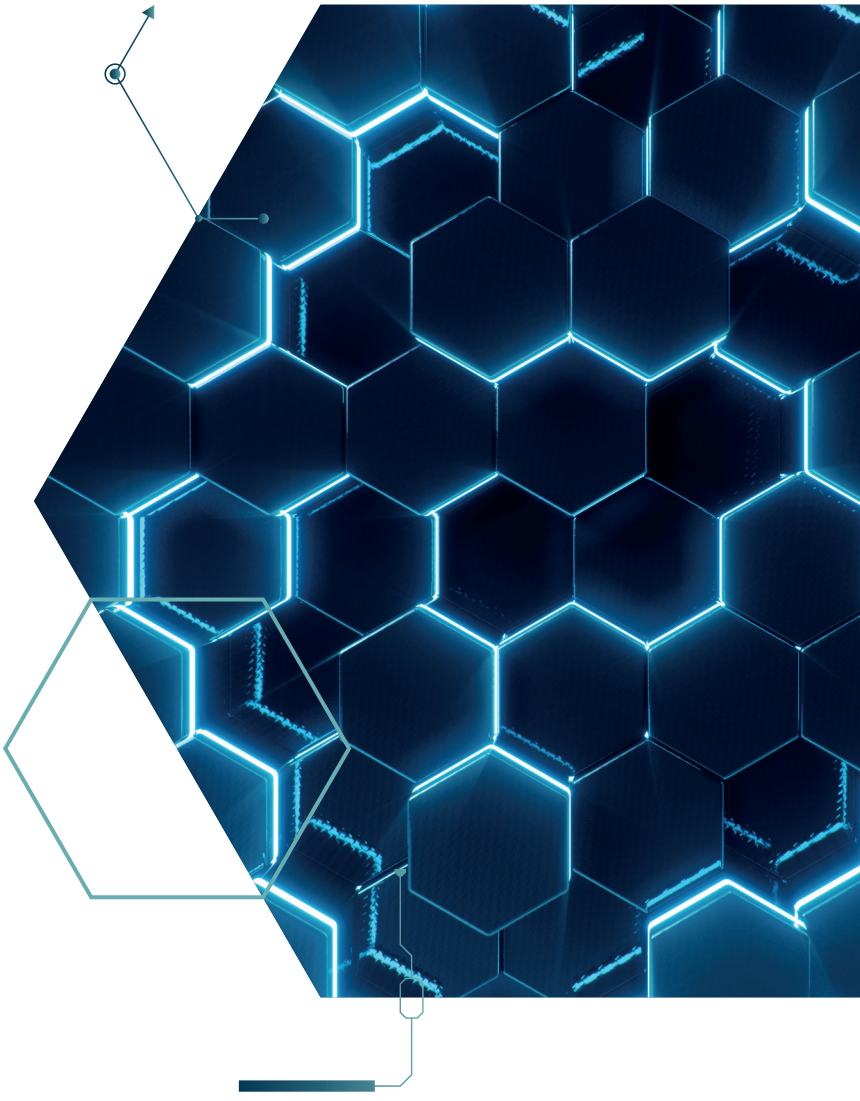
Controles possíveis	Critérios
Utilizar protocolos de autenticação de *endpoint* e implementar *virtual private networks* (VPNs)	COBIT DSS05 - *Managed Security Services* / ABNT NBR ISO/IEC 27002:2013 – 14.1.2 / Medida Provisória 2.200-2, de 24 de agosto de 2001
Avaliar a possibilidade de implementar técnicas de segurança para se prevenir ataques de DNS *spoofing*, ARP *spoofing* e IP *spoofing*	
Autenticar *endpoints*, com utilização de certificados digitais aderentes aos padrões da ICP-Brasil ou certificados *Secure Sockets Layer* (SSL)	

Tema: 5 - Riscos regulatório	
Categoria de risco: Conformidade jurídica de contratos inteligentes (*smart contracts*) e aplicações descentralizadas (dApps)	
Risco específico	
Incerteza regulatória sobre a utilização de contratos inteligentes	
Controles possíveis	**Critérios**
Provocar órgãos superiores ou legisladores para concepção de normas regulatórias	COBIT MEA03 - *Managed Compliance With External Requirements* / ABNT NBR ISO/IEC 27002:2013 – 18.1
Identificar as experiências de outros países relativas à utilização de contratos inteligentes na prestação de serviços públicos	
Controles possíveis	**Critérios**
Provocar órgãos superiores ou legisladores para concepção de normas regulatórias	COBIT MEA03 - *Managed Compliance With External Requirements* / ABNT NBR ISO/IEC 27002:2013 – 18.1
Identificar as experiências de outros países relativas à utilização de contratos inteligentes na prestação de serviços públicos	
Risco específico	
Não expressão da vontade das partes pelo contrato inteligente (mapeamento inadequado dos arranjos legais)	
Controles possíveis	**Critérios**
Identificar, revisar e documentar todos os requisitos legais, contratuais e regulatórios, incluindo regras específicas do tema relacionado ao contrato inteligente, bem como estabelecer estratégia para validação do código em relação às vontades das partes à luz da legislação vigente – *compliance by design*	COBIT BAI02 - *Managed Requirements Definition*
Realizar revisão crítica de todas as situações que resultem em reivindicações de cláusulas contratuais, considerando questões do tempo de contrato, prescrição e decadência, como, por exemplo, finalização da liquidação e resolução de litígios dos contratos	
Risco específico	
Reversão judicial de contrato inteligente por descumprimento legal	
Controles possíveis	**Critérios**
Alterar a programação de cada contrato inteligente, de forma que seja gerado, automaticamente, um arquivo para assinatura das partes, retratando com fidelidade o conteúdo do programa gerador do contrato	COBIT MEA03 - *Managed Compliance With External Requirements* / ABNT NBR ISO/IEC 27002:2013 – 18.1
Risco específico	
Falta de presunção de veracidade jurídica-legal do método de assinatura digital utilizado nos contratos inteligentes ou impossibilidade de a autenticidade das transações ser verificada fora do próprio sistema *blockchain*	
Controles possíveis	**Critérios**
Determinar os requisitos de autoria e temporalidade das transações realizadas no livro-razão distribuído	COBIT MEA03 - *Managed Compliance With External Requirements* / Medida Provisória 2.200-2, de 24 de agosto de 2001
Identificar se o caso de uso demanda a utilização de um procedimento comum de assinatura eletrônica ou uma assinatura digital qualificada. Ex. Lei exigir a assinatura como condição de validade ou eficácia de um ato ou negócio jurídico	
Utilizar assinatura digital produzida com o uso do processo de certificação digital da ICP-Brasil para garantir, concomitantemente, autoria, integridade, confidencialidade, autenticidade, temporalidade e não repúdio aos documentos, às transações e aos atos eletrônicos	
Categoria de risco: Privacidade	
Risco específico	
Armazenamento de informações sensíveis na *blockchain* ou dificuldade de implementar o mecanismo de privacidade denominado “direito a ser esquecido”	

Controles possíveis	Critérios
Assegurar que informações visíveis não violem a Lei Geral de Proteção de Dados Pessoais (LGPD)	COBIT BAI09 - *Managed Assets* / COBIT MEA03 - *Managed Compliance With External Requirements* / ABNT NBR ISO/IEC 27002:2013 – 18.1 / ABNT NBR ISO/IEC 27701 / Lei 13.709/2018 / Lei 12.527/2011
Mapear informações pessoais ou sensíveis que estão sujeitas a reivindicação do direito de esquecimento por parte dos cidadãos e, quando possível, armazená-las em banco de dados *off-chain*, utilizando apenas os hashes desses dados *on-chain*	
Assegurar que o cidadão conheça os instrumentos de política de privacidade e termos de uso e concorde com eles	
Definir e classificar o tipo de informação que pode ser armazenada na rede, de acordo com os requisitos da Lei de Acesso à Informação (LAI)	
Estudar a viabilidade de utilizar técnicas de *zero-knowledge*	
Definir estratégia de como a identidade será preservada nas transações	

Risco específico
Não verificação ou validação da identidade de usuários participantes da rede

Controles possíveis	Critérios
Avaliar se o caso de uso demanda a autenticidade para fins jurídicos-legais	COBIT DSS05 - *Managed Security Services* / COBIT MEA03 - *Managed Compliance With External Requirements* / Medida Provisória 2.200-2, de 24 de agosto de 2001
Definir estratégia para identificação primária dos usuários da rede, a fim de garantir que um cidadão é quem diz ser (*Know Your Customer – KYC)* e não realiza atividades criminosas (*Anti-Money Laudering – AML*)	
Definir processo seguro e auditável para garantir a ligação entre uma pessoa e sua chave	
Compartilhar informações biométricas dos cidadãos entre órgãos públicos	
Utilizar certificados digitais aderentes aos padrões da ICP-Brasil	



Responsabilidade pelo conteúdo
Secretaria-Geral da Presidência (Segepres)
Secretaria das Sessões (Seses)

Projeto gráfico, diagramação e capa
Secretaria de Comunicação (Secom)
Núcleo de Criação e Editoração (NCE)

Tribunal de Contas da União
Secretaria-Geral da Presidência (Segepres)
SAFS Quadra 4 Lote 1
Edifício Sede Sala 146
70.042-900, Brasília – DF
(61) 3316-5338
segepres@tcu.gov.br

Ouvidoria do TCU
0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Senge/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

_MISSÃO

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

_VISÃO

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.

www.tcu.gov.br