CONTRATO DE REFERÊNCIA DE REPRESENTAÇÃO DE CREDENCIADOS PARA FINS DE PRESTAÇÃO DE SERVIÇOS DE REDE MÓVEL VIRTUAL - CONTRATO PARA MVNO CREDENCIADA

Pelo presente instrumento particular,

XXXX, com sede na Cidade de XXXX, Estado do XXXX, com sede na XXXXXX, inscrita no CNPJ sob o nº XXXXX, neste ato representada nos termos de seus atos constitutivos, doravante denominada simplesmente **"PROPONENTE",** e

TIM S.A., com sede na Cidade do Rio de Janeiro, Estado do Rio de Janeiro, com sede na Avenida João Cabral de Mello Neto, n° 850, bloco 01, Salas 501 a 1208, Barra da Tijuca, inscrita no CNPJ/MF sob o nº 02.421.421/0001-11, neste ato representada nos termos do seu Estatuto Social, doravante denominada simplesmente "**TIM"**;

Sendo PROPONENTE e TIM, em conjunto, denominados "Partes" e, individualmente, "Parte",

CONSIDERAÇÕES:

(i) CONSIDERANDO que, em 09/02/2022, o Conselho Administrativo de Defesa Econômica (CADE) aprovou o Ato de Concentração nº 08700.000726/2021-08 mediante condições estabelecidas em Acordo de Controle em Concentrações ("ACC)", tendo a decisão transitado em julgado em 22/03/2022;

(ii) CONSIDERANDO as disposições constantes do Acórdão n.º 9, de 31 de janeiro de 2022, e do Ato n.º 4.951, de 05 de abril de 2022, expedidos pela ANATEL;

(iii) CONSIDERANDO que, dentre as condições estabelecidas nas decisões do CADE e da ANATEL, cabe à TIM disponibilizar nova Oferta de Referência destinada a Operadoras de Rede Móvel Virtual classificadas como Prestadoras de Pequeno Porte ("PPP") e que não sejam titulares de autorização de uso de radiofrequência na área pretendida de serviços, e que possuam o interesse em se tornar uma Credenciada para explorar o SMP por meio de Rede Virtual, nas áreas de outorga da TIM no território nacional. Caso a PROPONENTE não se enquadre como PPP, as PARTES poderão negociar condições específicas para prestação por meio de Rede Móvel Virtual;

(iv) CONSIDERANDO que qualquer contrato celebrado anteriormente à data da publicação da Oferta de Referência poderá ser adequado às novas condições, caso a contraparte assim tenha interesse, inclusive em relação ao prazo de vigência;

(v) CONSIDERANDO que a TIM possui outorga para a prestação do SMP em todo o território brasileiro;

(vi) CONSIDERANDO que a Agência Nacional de Telecomunicações – ANATEL aprovou em 22 de novembro de 2010 o Regulamento sobre Exploração de Serviço Móvel Pessoal – SMP por meio de Rede Virtual (Resolução n.º 550/2010), o qual sofreu alterações mediante a edição das Resoluções n.º 632, de 07 de março de 2014 (Resolução n.º 632/2012), n.º 663, de 21 de março de 2016 e n.º 735, de 03 de novembro de 2020;

(vii) CONSIDERANDO que as Partes têm o interesse em estabelecer as condições técnicas e comerciais para a implementação da operação de Credenciada de Rede Virtual pela PROPONENTE, em regime de livre pactuação e nos termos das disposições mencionadas nos Itens 'iv' e 'v' acima;

(viii) CONSIDERANDO que a PROPONENTE declara possuir viabilidade técnica, capacidade econômico-financeira, de rede e tecnológica, em conformidade com a Oferta Pública de Compartilhamento de Infraestrutura para fins de Prestação de Serviços de Rede Móvel Virtual - Modelo Credenciado ("Oferta Pública para MVNO Credenciada") para atuar na condição de Credenciada de SMP de Rede Virtual;

(ix) CONSIDERANDO que antes da adesão à Oferta Pública para MVNO Credenciada, as Partes observarão a seguinte etapa prévia à contratação.

CONDIÇÕES GERAIS PARA ESTABELECIMENTO DE PROPOSTA

A negociação e a celebração de Contratos de MVNO entre a TIM e PROPONENTES serão realizadas de acordo com o procedimento especificado abaixo, conforme previsões estabelecidas no ACC celebrado com o CADE.

a) A PROPONENTE interessada em celebrar Contrato de MVNO Credenciada deverá enviar uma solicitação de contato diretamente à TIM, por e-mail para mvno@timbrasil.com.br, em que indicará o atendimento às condições técnicas, regulatórias, financeiras e operacionais para a celebração do contrato;

b) Após o recebimento do e-mail com a solicitação enviada pela PROPONENTE, nos termos do item 'a', a TIM agendará reunião com a PROPONENTE, em até 10 (dez) dias úteis, na qual será apresentado o modelo disponibilizado pela TIM e o projeto de atuação pela PROPONENTE, dando início ao período de negociação;

c) A PROPONENTE deverá manifestar interesse em prosseguir com a negociação com a TIM em até 15 (quinze) dias corridos, contados a partir da data de realização da reunião mencionada no item "b". Não havendo manifestação de interesse dentro deste prazo, o pedido será arquivado pela TIM;

d) Iniciado o período de negociação, em até 20 (vinte) dias úteis contados a partir da manifestação de interesse por parte da PROPONENTE, a TIM e a PROPONENTE deverão firmar acordo de confidencialidade padrão, e estabelecerão os procedimentos para a troca de informações necessárias para a execução do Contrato de MVNO Credenciada, em estrito cumprimento e aderência à legislação de defesa da concorrência, regulação e guias editados pelo CADE, e melhores práticas antitruste. Dentro deste período, a PROPONENTE deverá encaminhar a documentação necessária para a continuidade da negociação, conforme o estabelecido nos itens "e", "f" e "g" abaixo, de modo a demonstrar sua capacidade técnica, financeira, operacional e regulatória para atuação no modelo de MVNO Credenciada.

e) A PROPONENTE deverá apresentar o **Plano de Negócios,** o qual deverá conter no mínimo as seguintes informações, para permitir uma análise técnica para dimensionamento dos elementos de rede da TIM para atendimento do

PROPONENTE, observando-se mecanismos de governança e protocolos de confidencialidade estabelecidos em acordos e manuais operacionais específicos:

i. Mercado alvo e abrangência geográfica de interesse;

ii. Expectativa de base de assinantes por área de registro por um período de no mínimo 24 (vinte e quatro) meses;

iii. Projeção de tráfego para serviços de voz, dados e sms segmentado por área de registro, por um período de no mínimo 24 (vinte e quatro) meses.

iv. Condições técnicas e operacionais (elementos de rede CORE);

vii. Documentos constitutivos:

- Atos Constitutivos da empresa solicitante, de acordo com o tipo de sociedade empresária (Ltda, ME, EIRELI ou S/A);
- CPF e carteira de identidade dos sócios e/ou representantes legais;
- Relação atualizada de Clientes, se houver;
- Business Presentation – somente se a empresa já se encontrar em funcionamento;e

vii. Documentos financeiros da empresa:

- ECF – Escrituração Contábil Fiscal e/ou ECD – Escrituração Contábil Digital completo;
- Extrato de movimentação bancária, dos 03 (três) últimos meses, de conta corrente e/ou de Investimentos, em nome da empresa;
- DEFIS - Declaração de Informações Socioeconômicas e Fiscais; e,
- Imposto de Renda dos sócios dos últimos dois exercícios.

f) A PROPONENTE interessada deverá apresentar para a TIM, **Formulário de informações da PROPONENTE** anexo, preenchido com todas as informações solicitadas.

formulario Credenciada

g) A PROPONENTE deverá apresentar **Projeto** que garanta as condições mínimas de conexão e compartilhamento com a TIM, de acordo com avaliação técnica e critérios da própria TIM.

h) O prazo mencionado no item “d” poderá ser prorrogado em caso de: alterações na minuta do acordo de confidencialidade padrão; atrasos na assinatura do acordo de confidencialidade padrão por parte da PROPONENTE e atrasos no envio da documentação necessária por parte da PROPONENTE.

i) Caso ultrapassados mais de 15 (quinze) dias corridos contados do envio pela TIM da minuta do acordo de confidencialidade padrão e da solicitação para apresentação da documentação necessária sem que haja resposta ou manifestação por parte da PROPONENTE, o pedido será arquivado.

i) Uma vez firmado o acordo de confidencialidade padrão e recebida toda a documentação exigida, encaminhada pela PROPONENTE, a TIM deverá apresentar resposta formal acerca da suficiência dos documentos e quanto ao prosseguimento da negociação em até 30 (trinta) dias corridos de seu recebimento.

i) Se a documentação enviada pela PROPONENTE for insuficiente para permitir o prosseguimento da negociação, a TIM poderá solicitar sua complementação, caso em que os prazos subsequentes estabelecidos no processo de negociação serão suspensos, inclusive o prazo da resposta formal da TIM, até a entrega da documentação complementar.

ii) Não havendo resposta por parte da PROPONENTE acerca da complementação da documentação solicitada pela TIM dentro de 30 (trinta) dias corridos da solicitação, o pedido será arquivado.

j) Em até 60 (sessenta) dias corridos da data de recebimento da documentação necessária a TIM enviará à PROPONENTE as propostas comercial e técnica para celebração do Contrato de MVNO Credenciada. O cumprimento deste prazo é condicionado à aprovação e regularidade da documentação encaminhada pela PROPONENTE.

i) Ultrapassados 30 (trinta) dias corridos contados da data de recebimento das propostas comercial e técnica sem que haja manifestação de interesse ou apresentação de resposta por parte da PROPONENTE, ou caso esta manifeste não ter mais interesse em prosseguir com a negociação, o pedido será arquivado.

k) Caso a PROPONENTE esteja de acordo com as propostas comercial e técnica e manifeste interesse em prosseguir com a negociação, a TIM deverá enviar a minuta do Contrato de MVNO Credenciada em até 20 (vinte) dias corridos para a PROPONENTE, para discussão acerca das condições contratuais que regerão o relacionamento comercial entre as Partes.

i) O prazo mencionado no item “K” poderá ser prorrogado, caso a habilitação da PROPONENTE como MVNO Credenciada seja enquadrada na condição de “Projeto Especial”.

ii) Por “Projeto Especial” entende-se os casos em que haja a necessidade de a TIM ou a PROPONENTE realizarem investimentos para ampliação de sua capacidade de rede disponível, adequações tecnológicas para assegurar a integração dos sistemas das empresas, modernização da infraestrutura de rede disponível, bem como quaisquer adequações de caráter técnico ou operacional não previstas inicialmente, que sejam necessárias para assegurar a habilitação da PROPONENTE como MVNO Credenciada e a continuidade da prestação dos serviços de telecomunicações da PROPONENTE.

l) Havendo concordância entre a TIM e PROPONENTE quanto aos termos e condições contratuais aplicáveis, será celebrado o Contrato de MVNO Credenciada entre as Partes.

i) Assinado o Contrato e cumpridas todas as obrigações regulatórias por parte da Proponente, a TIM e a PROPONENTE agendarão reunião para discutir a implementação do projeto e adotarão todas as medidas necessárias para esta finalidade

ii) A TIM deve submeter à ANATEL o Contrato de MVNO Credenciada firmado com a PROPONENTE, em até 30 (trinta) dias corridos após sua celebração, para homologação.

iii) Decorridos 30 (trinta) dias sem manifestação da Anatel, considerar-se-á homologado o Contrato de MVNO Credenciada, nos termos da Resolução nº 550/2010.

iv) Após a homologação do Contrato de MVNO Credenciada, em caso de ausência de manifestação, pela Anatel, em prazo superior a 30 (trinta) dias, a TIM e a PROPONENTE agendarão reunião para discutir a implementação do projeto e adotarão todas as medidas necessárias para esta finalidade.

m) O lançamento comercial da PROPONENTE estará condicionado a:

i. Apresentação da Garantia Financeira descritas nos termos do ANEXO III;

ii. Conclusão da integração técnica com aceite da PROPONENTE formalizado por e-mail.

n) Solicitações Judiciais, emitidas por autoridades competentes, que envolvam informações necessárias, que não estejam disponíveis para a TIM nas plataformas da CREDENCIADA, deverão ser objeto do Anexo VI, a ser previamente celebrado entre as Partes, para a definição de procedimentos e responsabilidades.

o) As Partes se comprometem a se reunir com vistas a detalhar um manual operacional no prazo de até 90 (noventa) dias após a assinatura do Contrato de MVNO Credenciada.

p) Para fins de esclarecimento, a PROPONENTE poderá acionar o Trustee de Monitoramento, nos termos do ACC celebrado com o CADE, para dar início a procedimento de mediação, conforme procedimento estabelecido no ACC. Ademais, a PROPONENTE poderá iniciar procedimento arbitral privado para buscar a solução de conflitos relacionados a questões comerciais, nos termos expressamente previstos no ACC.

q) Para fins de esclarecimento, os prazos aqui definidos poderão ser prorrogados: (i) diante da ocorrência de fato fortuito ou eventos de força maior, conforme definidos pelo art. 393 do Código Civil, que comprovadamente impossibilitem seu cumprimento; (ii) de comum acordo entre as Partes no âmbito das negociações para celebração do Contrato de MVNO; (iii) mediante solicitação fundamentada da TIM ou da PROPONENTE ao Trustee de Monitoramento; ou (iv) por qualquer impossibilidade técnica, legal, regulatória ou financeira que impeça o seu cumprimento.

1. OBJETO E DOS DOCUMENTOS INTEGRANTES

1.1. O presente Contrato para MVNO Credenciada destina-se exclusivamente ao atendimento de Prestadoras de Pequeno Porte (PPP) para permitir a habilitação de MVNOs na modalidade Credenciada na rede móvel da TIM, de modo que a PROPONENTE possa estabelecer o início das atividades na condição de exploradora do Serviço Móvel Pessoal (SMP) por meio de rede virtual em todo território nacional.

1.2. A Oferta Pública de Referência e o presente Contrato destinam-se exclusivamente ao atendimento de Prestadoras de Pequeno Porte (PPP), que não possuam direito de uso de radiofrequência, que têm como objetivo de estabelecer o início das atividades na condição de exploradora do Serviço Móvel Pessoal por meio de rede virtual em todo território nacional. As atuais MVNOs Credenciadas da TIM poderão aderir à nova Oferta Pública de Referência publicada pela TIM.

1.2.1. Cada Parte responderá pelas contratações e despesas que assumir ou incorrer para custeio de estudos, assessoria ou consultoria decorrente da elaboração, negociação, análise e definição de seu Modelo de Negócios, não restando qualquer direito a reembolso, compensação ou abatimento decorrente de tais despesas.

1.3. Não integra o presente Contrato para MVNO Credenciada a disponibilização pela TIM dos direitos decorrentes de acordos de roaming nacional e/ou internacional e de radiofrequência firmados com outras operadoras ou acordos de interconexão e transporte, quaisquer que sejam.

1.4. Integram este Contrato os seguintes Anexos, cujas disposições produzem efeito entre as Partes:

Anexo I – Definições

Anexo II – Condições Comerciais e Remuneração

Anexo III – Garantia Financeira

Anexo IV – Técnico de Segurança

Anexo V – Práticas de Antifraude

Anexo VI – Interceptação Legal

1.5. O presente Contrato e seus respectivos Anexos constituem partes integrantes e únicas do documento que respaldará a relação entre as Partes e deverão ser interpretados de forma harmônica e complementar. Ocorrendo discrepância ou conflito entre o presente Contrato e qualquer um de seus Anexos, as Partes acordam que prevalecerá a redação estabelecida no Contrato.

2. OBRIGAÇÕES DAS PARTES

2.1. **OBRIGAÇÕES DA PROPONENTE**:

2.1.1. A PROPONENTE deverá cumprir integralmente as condições acordadas com a TIM;

2.1.2. A PROPONENTE será responsável por apresentar, renovar ou recompor, as garantias financeiras nos prazos e condições estipulados pela TIM nos termos do ANEXO III;

2.1.3. A PROPONENTE será responsável pelo cumprimento de todas as suas obrigações regulamentares junto à ANATEL, incluindo, mas não se limitando, às dispostas na Resolução n.º 550/2010 e na Resolução n.º 632/2012, bem como em relação aos direitos de seus Clientes.

2.1.4. A PROPONENTE se compromete a elaborar, independentemente do regime jurídico a que esteja sujeita, balanço e demonstrações financeiras levantadas ao final de cada exercício social, observadas as disposições da legislação vigente e regulamentação da ANATEL.

2.1.5. A PROPONENTE observará o disposto no Anexo II deste Contrato na elaboração de planos e ofertas.

2.1.6. Para que haja uso apropriado e seguro dos recursos compartilhados, sem comprometer a eficiência e segurança das redes das Partes e nem prejudicar o sistema como um todo, garantindo a continuidade dos serviços aos clientes, trimestralmente a PROPONENTE deverá informar, mediante envio de relatório técnico de dimensionamento, as seguintes informações, respeitando-se as regras de governança e protocolos de confidencialidade previstos na Cláusula 7.5 abaixo:

- A previsão anual de Clientes, com detalhamento da quantidade de novos Clientes, quantidade de cancelamentos e a base total;

- Volume de tráfego de dados e voz, segmentados por área de registros e municípios; e

- Outras informações técnicas razoavelmente solicitadas pela TIM.

2.1.7. Os relatórios terão a finalidade de permitir à TIM análise eminentemente técnica das informações acima indicadas, respeitando-se as regras de governança e protocolos de confidencialidade previstos na Cláusula 7.5 abaixo, no sentido de avaliar e garantir o preparo e dimensionamento técnicos e adequados de sua rede e infraestrutura de telecomunicações. Os relatórios indicados na Cláusula 2.1.8 terão seu formato definido no MPPO, bem como servirão para informar à PROPONENTE eventuais restrições, se a análise de dimensionamento resultar neste sentido.

2.1.8. A PROPONENTE se compromete a criar e atualizar constantemente mecanismos de prevenção e combate à utilização fraudulenta, indevida e

irregular da rede de telecomunicações da TIM, responsabilizando-se exclusivamente por prejuízos causados à TIM e/ou terceiros.

2.1.9. A PROPONENTE se compromete a utilizar apenas equipamentos com certificação emitida ou reconhecida pela ANATEL, conforme regulamentação aplicável, inclusive observando suas condições de funcionamento.

2.1.10. A PROPONENTE deve informar, com uma antecedência de até 120 (cento e vinte) dias, à TIM quaisquer medidas que possam influenciar e/ou degradar a performance da rede, de acordo com o Anexo IV e V;

2.1.11. A PROPONENTE será responsável por cadastrar no sistema indicado pela TIM os clientes do SMP atendidos por meio de Representação, conforme previsto na regulamentação, e manter atualizada a base de dados cadastrais destes Usuários, zelando também por sua integridade, tanto do ponto de vista de segurança como de combate à fraude.

2.1.12. A PROPONENTE deve informar a TIM sobre os dados cadastrais dos Usuários do serviço SMP prestado por meio de Representação;

2.1.13. A PROPONENTE deve manter registros contábeis separados para a atividade de Representação na Prestação do SMP caso realize alguma atividade distinta.

2.1.14. A PROPONENTE deve manter todas as condições para que seja possível a Portabilidade numérica dos Usuários do SMP prestado por meio de Representação do Credenciado;

2.1.15. A PROPONENTE deve Informar à TIM qualquer alteração ocorrida nas informações fornecidas em seu plano de negócios, respeitando-se as regras de governança e protocolos de confidencialidade previstos na Cláusula 7.5 abaixo;

2.1.16. A PROPONENTE deve prover toda infraestrutura de tecnologia da informação para suporte dos serviços disponibilizados;

2.1.17. A PROPONENTE deverá definir e gerir, de forma independente, todas as ações e canais de Vendas, Marketing, Comunicação, Atendimento e Mídia;

2.1.18. A PROPONENTE custeará todo o SAC (que podem incluir, mas não estão limitados a aquisição de produtos e serviços, comunicação, atendimento, subsídio de aparelhos, produção de SIM Cards, inadimplência, armazenamento de informações, entre outras);

2.1.19. A PROPONENTE será exclusivamente responsável pelo atendimento ao seu cliente (vendas e SAC), devendo observar todas as regras vigentes sobre o referido atendimento.;

2.1.20. As Partes poderão acordar diferentes formas de atendimento mediante a termo aditivo a este Contrato.

2.1.21. A PROPONENTE deverá gerir e custear toda produção e logística de SIM Cards;

2.1.22. A PROPONENTE se compromete a arcar com os custos derivados da hipótese de descontinuidade de tecnologias empregadas pela TIM ou do surgimento de novas tecnologias atreladas ao SMP a serem adotadas pela TIM, inclusive, mas não se limitando aos custos vinculados à substituição de Estações Móveis de seus Clientes, a comunicação e cessação de serviços.

2.1.21.1 Não haverá cobrança associada ao projeto técnico necessário para implementação de novas tecnologias, nos termos da descritos na cláusula 2.1.21, sendo os custos provenientes dos elementos de rede exclusivamente de responsabilidade da PROPONENTE.

2.1.23. A PROPONENTE deve preservar e guardar por 5 (cinco) anos todas as informações relativas as reclamações e contratações de seus clientes, seja no atendimento dos canais de vendas ou SAC, bem como os seus dados cadastrais com o objetivo de garantir a ampla defesa das PARTES em eventuais questionamentos por parte das autoridades administrativas e judiciais.

2.1.24. Se em decorrência da prestação dos Serviços, existir a necessidade de trânsito e/ou circulação dos profissionais da PROPONENTE nas dependências e instalações da TIM e/ou necessidade de acesso, por quaisquer desses profissionais, a quaisquer sistemas, aplicativos, banco de dados e/ou qualquer informação fixada em qualquer suporte da TIM ou de terceiros, a PROPONENTE se obriga a observar e cumprir, por si e por seus profissionais, as normas, políticas e procedimentos da TIM relativos a (i) segurança, (ii) higiene do trabalho, (iii) segurança do trabalho, (iv) NBR ISO IEC 27001, (v) PRIVACIDADE, acesso a sistemas e aplicativos, dentre outros.

2.1.25. Permitir que a TIM, observando as obrigações de confidencialidade estabelecidas na Cláusula 7 abaixo, a seu livre e exclusivo critério, realize análises de segurança e vistorias nas instalações da PROPONENTE onde é(são) prestado(s) o(s) Serviços. Referidas vistorias, desde que dentro do horário comercial e previamente informadas à PROPONENTE.

2.1.26. A eventual realização de análises de segurança e vistorias pela TIM e/ou seus representantes, não implicará em qualquer prejuízo ou diminuição das responsabilidades da PROPONENTE, não a eximindo das obrigações ora assumidas. Neste sentido, a PROPONENTE se compromete a possibilitar à TIM o uso de mecanismos que esta entenda necessários para a perfeita realização das vistorias, com o objetivo de comprovar que todos os requisitos e cláusulas de segurança estão sendo seguidas pela PROPONENTE. A vistoria poderá ser realizada de forma online ou presencialmente e a PROPONENTE se compromete a comprovar, através de evidências, a existência de todos os requisitos de segurança exigidos pela TIM.

2.1.27. A PROPONENTE, em virtude dos riscos identificados pela TIM quando das análises de segurança e vistorias acima referidas, se obriga a desenvolver e aplicar um plano de tratamento de riscos, tendo por base as solicitações exigidas por estas para a melhoria na prestação dos serviços ora contratados. Nesse sentido, a PROPONENTE compromete-se a

envidar seus melhores esforços no sentido de aplicar de maneira efetiva o plano de tratamento de riscos elaborado, responsabilizando-se pela veracidade de todas as informações e evidências que transparecer a TIM sobre esse mérito.

2.1.28. A PROPONENTE deverá ainda, comunicar a TIM imediatamente e no prazo máximo de 24h (vinte e quatro horas), assim que identificado, quaisquer incidentes de segurança que possam prejudicar e/ou reduzir a atuação da PROPONENTE na prestação de serviços objeto deste Contrato.

2.2. **DAS OBRIGAÇÕES DA TIM:**

2.2.1. A TIM será responsável pelo cumprimento de suas obrigações junto à ANATEL, enquanto Prestadora de Origem.

2.2.2. A TIM será responsável pela prestação do serviço SMP, nos termos da Resolução n.º 550/2010.

2.2.3. A TIM realizará o credenciamento da PROPONENTE junto à ANATEL, mediante ao cumprimento dos requisitos expostos no âmbito deste Contrato.

2.2.4. A TIM proporcionará à PROPONENTE as mesmas condições empregadas na prestação de serviços a seus próprios usuários.

2.2.5. Comunicar previamente em até 30 (trinta) dias aos Usuários da PROPONENTE a rescisão ou extinção da relação entre Prestadora Origem e Credenciado, explicando o motivo, disponibilizando, aos Usuários, alternativas de adesão a um de seus Planos de Serviço, para garantia da continuidade da prestação sem alteração do código de acesso, sendo assegurado, caso opte pela rescisão do contrato, que esta não lhe acarrete qualquer ônus;

2.2.6. Informar à ANATEL qualquer rescisão ou extinção de relação entre as Partes, acompanhada da motivação para tal, bem como as providências a serem tomadas com relação aos Usuários atendidos por meio de Representação da PROPONENTE;

2.2.7. Assegurar o cadastramento dos Usuários do SMP prestado por meio de Representação, conforme previsto na regulamentação, com permanente atualização da base de dados cadastrais desses Usuários e sua integridade, tanto do ponto de vista de segurança, como de combate à fraude;

2.2.8. Manter controle da quantidade e do cadastro de Usuários do SMP prestado por meio de Representação da PROPONENTE;

2.2.9. Encaminhar à ANATEL, mensalmente, relatório com a quantidade de Usuários do SMP cadastrados, por plano de serviço;

2.2.10. Realizar quebra de sigilo, nos termos da legislação, atendendo as solicitações das autoridades competentes relativas ao fornecimento de dados cadastrais, bem como as demandas de quebra de sigilo telefônico e

telemático, incluindo a identificação das antenas utilizadas, fluxo de chamada, dados, SMS/MMS e a identificação de IPs, além de realizar as programações de interceptação telefônica e telemática a serem implementadas na rede da TIM relativos aos usuários de sua responsabilidade;

2.2.11. Informar, em prazo razoável, a PROPONENTE das futuras alterações em sua rede, em especial aquelas que impactem na Prestação do SMP por meio de Rede Virtual;

2.2.12. Ceder a base de Usuários atendidos pelo Credenciado em caso de migração deste para outra Prestadora Origem ou de obtenção de Autorização para Prestação do SMP por meio de Rede Virtual; e

2.2.13. Colaborar com o Credenciado de Rede Virtual para a implementação das ações versando sobre segurança pública, conforme deliberações do Grupo Técnico de Suporte à Segurança Pública.

2.3. **DAS OBRIGAÇÕES COMUNS (PARTES)**

2.3.1. Para a implementação do objeto previsto neste Contrato, as Partes se comprometem a trabalhar em conjunto e fornecer todas as informações necessárias, sejam elas de cunho financeiro, técnico, jurídico ou de qualquer outra natureza, respeitando-se as regras de governança e protocolos de confidencialidade previstos na Cláusula 7.5 abaixo.

2.3.2. Cada uma das Partes deve designar, no prazo máximo de 30 (trinta) dias da obtenção da homologação pela TIM, uma equipe formada por pessoas com conhecimento necessário para a adequada implementação deste Contrato, sempre em conformidade com a legislação e regulamentação vigentes.

2.3.3. A TIM deverá indenizar a PROPONENTE de forma proporcional à sua responsabilidade por multas, sanções ou condenações individuais ou coletivas, que a PROPONENTE venha a sofrer, desde que tais fatos sejam comprovados e oriundos de falhas nas obrigações da TIM. Da mesma forma, a PROPONENTE deverá indenizar a TIM de forma proporcional por quaisquer multas, sanções ou condenações, individuais ou coletivas, que a TIM venha a sofrer, desde que tais fatos sejam oriundos de falhas comprovadas nos serviços e/ou obrigações da PROPONENTE.

3. CONDIÇÕES COMERCIAIS E REMUNERAÇÃO

3.1. As condições comerciais e de remuneração resultantes da parceria entre a TIM e a PROPONENTE são definidas no Anexo II deste Contrato.

4. DA VIGÊNCIA E RESCISÃO

4.1. O presente Contrato é firmado em caráter irretratável e irrevogável pelo período inicial de XXXXXXX anos (“Prazo Inicial”), contados a partir da data de assinatura

do Contrato, podendo ser encerrado antecipadamente caso: i) a TIM não obtenha a homologação deste Contrato perante a Anatel, ii) a autorização da Prestadora Origem para a prestação do SMP (serviço móvel pessoal) seja extinta pelo Poder Concedente ou sofra restrição regulatória que inviabilize a manutenção do presente Contrato, iii) o Contrato seja denunciado (independentemente de qualquer motivo), por qualquer das Partes, mediante notificação prévia, com antecedência mínima de 180 (cento e oitenta) dias.

4.2. Após o decurso do Prazo Inicial, o Contrato será renovado automaticamente por períodos sucessivos de 02 (dois) anos ("Prazo de Renovação").

4.3. O presente Contrato também poderá ser rescindido nos casos abaixo definidos:

a) Por qualquer das Partes, quando observado o inadimplemento das obrigações estabelecidas no presente Contrato, após o não atendimento de notificação concedendo o prazo de 30 (trinta) dias para que a obrigação inadimplida seja sanada pela Parte Infratora;

b) Requerimento de recuperação judicial ou extrajudicial ou decretação de falência de qualquer uma das Partes;

c) Por acordo mútuo entre as Partes;

d) Por não apresentação, recomposição ou renovação das garantias solicitadas, conforme regras definidas no Anexo III;

e) Por ocorrência de fato que, por sua natureza e gravidade, incidam sobre a confiabilidade e moralidade de qualquer das Partes ou que seja suscetível de causar danos ou comprometer, mesmo que indiretamente, a imagem da outra Parte;

f) alteração societária da PROPONENTE ou cessão de parte de seus ativos;

4.3.1. As Partes acordam, desde já, que, em qualquer caso de extinção do presente Contrato, a PROPONENTE terá direito ao pagamento, pela TIM, do comissionamento das recargas (definido no Anexo II) até o efetivo término do Contrato, sendo certo que a PROPONENTE deverá manter seus canais de recarga ativos até lá.

4.4. Em caso de rescisão contratual por culpa da TIM nos termos do item 4.3, "a", a TIM deverá arcar com os reais custos da migração, devidamente comprovados, da PROPONENTE para outra operadora de SMP, limitados ao valor máximo de R$ 1.500.000,00 (um milhão e quinhentos mil reais).

4.5. Sem prejuízo da rescisão contratual prevista na cláusula 4.3 "a", em caso de saída imotivada ou rescisão do Contrato por culpa da PROPONENTE, toda base de assinantes da PROPONENTE, assim como a base de assinantes das eventuais Credenciadas que estejam sob sua estrutura, será notificada pela TIM do desligamento do serviço com antecedência mínima de 45 (quarenta e cinco) dias. Diante disso, a TIM está desde já autorizada a notificar os Clientes da PROPONENTE por meio de SMS e/ou outros meios de comunicação quanto ao desligamento do Serviço da PROPONENTE e as alternativas de adesão a um dos Planos de Serviço da TIM ou outra operadora, resguardada a possibilidade de solicitação de portabilidade. A notificação poderá ser diária até a data de

desligamento do serviço, respeitada a regulamentação vigente, de modo a minimizar os impactos ao usuário final e garantir a continuidade e fruição dos serviços contratados.

4.5.1 Ocorrendo o encerramento do Contrato nos termos previstos no item 4.5. acima, a PROPONENTE deverá pagar multa equivalente ao somatório de:

4.5.1.1 Valor fixo de R$ 1.500.000,00 (um milhão e quinhentos mil) de reais, corrigidos pelo índice aplicável ao presente Contrato;

4.5.1.2 A PROPONENTE deverá pagar uma multa equivalente ao somatório de 30% (trinta por cento) do compromisso de receita bruta mínima anual (definido conforme Anexo II) remanescente, até o fim da vigência do Contrato.

4.5.2 Durante o período de migração mencionado na cláusula 4.5, nos termos deste Contrato, não será possível, a solicitação de novas ativações pela PROPONENTE.

4.6. Em qualquer hipótese de rescisão ou término da vigência deste Contrato, as Partes deverão garantir a continuidade dos serviços durante o prazo de aviso prévio, para a base de Clientes existentes à época do término, bem como para novos Clientes que venham a contratar os serviços até que se obtenha uma solução para a migração de tais Clientes.

4.7. Os valores previstos no itens 4.4 e 4.5.1 acima serão reajustados anualmente com base na variação do IPCA, ou por outro índice que eventualmente venha a substituí-lo.

4.8. Os valores descritos no item 4.4 deverão ser pagos pela TIM no prazo máximo de 60 (sessenta) dias contados da comprovação da migração total prevista, bem como os valores descritos nos itens 4.5.1 e deverão ser pagos pela PROPONENTE no prazo máximo de 60 (sessenta) dias contados da data do recebimento da notificação de rescisão. Após os prazos descritos acima, a Parte que deverá receber o valor da rescisão poderá tomar as medidas administrativas e judiciais cabíveis para cobrança, caso necessário.

5. PUBLICIDADE

5.1. As Partes não poderão produzir, publicar ou distribuir folheto de divulgação ou qualquer outra publicação relativa à outra Parte, às suas coligadas ou a este Contrato, sem autorização prévia, por escrito, da outra Parte.

6. CONFIDENCIALIDADE

6.1. As Partes, seus funcionários e seus subcontratados não deverão divulgar qualquer documento ou Informação à qual tenham acesso, em relação ao objeto do presente Contrato. A divulgação e/ou reprodução, seja total ou parcial, de qualquer Informação, relativa a este Contrato ou de qualquer detalhe sobre sua evolução, deverá ser feita apenas mediante consentimento prévio, por escrito, da outra Parte, respeitando-se sempre os limites legais, as melhores práticas e documentos normativos da PARTE FORNECEDORA relativos à segurança e privacidade.

6.2. Cada Parte (doravante “Parte Receptora”) deverá manter todas as informações fornecidas pela outra Parte (doravante “Parte Fornecedora”) no mais estrito sigilo e não poderá divulgá-las a terceiros sem o consentimento prévio, por escrito, da Parte Fornecedora. As Informações não poderão ser utilizadas pela Parte Receptora para outra finalidade além da execução deste Contrato. As obrigações acima descritas não se aplicarão a qualquer Informação que:

(i) já forem de domínio público à época em que tiverem sido reveladas;
(ii) passarem a ser de domínio público após sua revelação, sem que a divulgação seja efetuada em violação ao disposto neste Acordo;
(iii) forem legalmente reveladas a qualquer das Partes, às suas Afiliadas ou aos seus Representantes por terceiros que, até onde a Parte receptora, suas Afiliadas ou Representantes tenham conhecimento, não estejam violando, em relação às informações fornecidas, qualquer obrigação de confidencialidade;
(iv) devam ser reveladas pela Parte Receptora, em razão de uma ordem emitida por órgão administrativo ou judiciário com jurisdição sobre referida Parte, somente até a extensão de tal ordem; ou
(v) forem independentemente obtidas ou desenvolvidas por qualquer das Partes sem qualquer violação das obrigações previstas neste Acordo, exceto quando tais informações forem desenvolvidas tendo como base as Informações Confidenciais.

6.3. A Parte receptora das Informações Confidenciais deverá comunicar à Parte FORNECEDORA tão logo o saiba, qualquer solicitação daquelas informações por quaisquer autoridades públicas competentes ou por meio de qualquer processo judicial, de forma que a Parte FORNECEDORA seja capaz de tomar as medidas legais que julgar cabíveis.

6.4. As Partes estão cientes de que cada uma delas faz parte de uma organização de várias entidades legais em diversas jurisdições (empresas “Associadas”), e que poderá ser necessário ou adequado fornecer Informações a empresas Associadas. Por esta razão, cada Parte (ambas em condição de Parte Fornecedora e Parte Receptora conforme este Contrato) está de acordo com o fato de que:

(i) A Parte Receptora poderá fornecer Informações a uma empresa Associada, mas apenas pela necessidade de a última tomar conhecimento dessas informações a fim de realizar as finalidades prevista neste Contrato, respeitando-se as diretrizes legais vigentes e nos limites do consentimento fornecido pelo titular dos dados; e
(ii) Cada Parte garante o cumprimento e a confidencialidade adequada, por parte de suas empresas Associadas, dos termos e condições desta Cláusula.

6.5. Cada Parte deverá limitar o acesso às Informações a seus funcionários, representantes, contratados ou consultores a quem este acesso seja razoavelmente necessário ou apropriado para o exclusivo propósito de garantir a adequada execução do presente Contrato.

6.5.1. TIM se obriga a instituir mecanismos de governança e protocolos de confidencialidade estabelecidos em acordos e manuais operacionais específicos para analisar as informações da PROPONENTE que sejam imprescindíveis para avaliações técnicas, de impacto e de dimensionamento de rede exclusivamente relacionadas à apropriada execução e implementação deste Contrato.

6.6. O dever de Confidencialidade abrange as Informações recebidas pelas Partes, de forma oral ou escrita, através de diversos procedimentos de comunicação, tais como telefone, fac-símile e mídias digitais, de cujo sigilo uma Parte tenha sido alertada pela outra, por qualquer meio.

6.7. A não observância de qualquer das disposições estabelecidas nesta Cláusula sujeitará a Parte infratora aos procedimentos judiciais e administrativos competentes, de ordem civil e criminal, inclusive tutela antecipada, medidas liminares e indenização por perdas e danos que possam advir à outra Parte.

6.8. A obrigação de confidencialidade é em caráter irrevogável e irretratável, devendo ser observada mesmo após o encerramento do presente Contrato.

6.9. Todas as Informações Confidenciais transmitidas ou divulgadas à Parte Receptora devem ser devolvidas à Parte Fornecedora ou destruídas pela Parte Receptora de forma irrecuperável, tão logo tenha terminado a necessidade de seu uso pela Parte Receptora ou tão logo solicitado pela Parte Fornecedora e, em qualquer caso, na hipótese de término deste Contrato. A pedido da Parte Fornecedora, a Parte Receptora deverá se responsabilizar pelo transporte das informações solicitadas e prontamente emitir uma declaração a ser assinada por seu representante legal, confirmando que toda a Informação não retornada para a Parte Fornecedora foi inteiramente destruída.

6.10. O descumprimento da presente cláusula acarreta a imediata rescisão do presente Contrato, independentemente de prévia notificação.

7. PROPRIEDADE INTELECTUAL

7.1. Os direitos de propriedade intelectual e industrial das obras criadas, desenvolvidas ou modificadas durante a vigência deste Contrato permanecerão como propriedade individual de cada uma das Partes, responsável pela criação, desenvolvimento ou modificação.

7.2. Nenhum direito de propriedade intelectual e industrial atualmente existente, ou que venha a ser adquirido ou licenciado por uma Parte, será outorgado à outra Parte.

7.3. Salvo autorização expressa em contrário, nenhuma Parte poderá publicar ou usar logotipo, marcas e patentes registradas pela outra Parte.

7.4. As marcas registradas por qualquer das Partes para identificar seus produtos e serviços, bem como o(s) logotipo(s) registrado(s) pelas Partes são de propriedade de cada uma delas.

7.5. A outra Parte, seus empregados ou entidades terceirizadas não terão quaisquer direitos, relativamente a essas marcas ou logotipos, exceto na medida expressamente estabelecida no presente Contrato e conforme especificado por escrito.

8. INEXISTÊNCIA DE VÍNCULO

8.1. Este Contrato não cria qualquer responsabilidade trabalhista e/ou previdenciária entre as Partes, os administradores, empregados, funcionários e consultores de cada uma e/ou terceiros por elas contratados que executarem o Objeto deste instrumento, sendo de exclusiva responsabilidade de cada uma das Partes o pagamento de todos os encargos aplicáveis, incluindo, sem limitação, os de natureza trabalhista, previdenciária e referentes a acidentes de trabalho.

8.2. Qualquer reclamação trabalhista ou outro tipo de ação que venha a ser apresentada por funcionários, prepostos ou agentes de uma das Partes, será de responsabilidade única e exclusiva da mesma, a qualquer tempo, ainda que após o término do presente Contrato, as quais assumirão integralmente a questão, respondendo pelo pagamento de indenizações, multas, honorários advocatícios, custas processuais e todos e quaisquer outros encargos que houver, independentemente de qualquer notificação, intimação, comunicação ou aviso. Se por qualquer motivo a parte inocente arcar com condenações, custas judiciais, despesas processuais, multas ou honorários advocatícios em processos trabalhistas judiciais ou administrativos de responsabilidade da outra parte, esta última deverá indenizar a primeira pelo valor despendido no prazo de 60 (sessenta) dias, contados da notificação

8.3. Cada Parte é exclusivamente responsável por seus funcionários e prepostos designados para as atividades objeto deste Contrato.

9. ISENÇÃO DE RESPONSABILIDADE

Cada Parte será a única e exclusiva responsável por seus negócios, tais como: (i) atividade desempenhada por suas controladoras, controladas, coligadas, empregados, funcionários e/ou prestadores de serviços em função deste Contrato; (ii) violação ou inadimplemento de qualquer disposição deste Contrato, salvo se a violação ou inadimplemento ocorreu por ato ou fato de responsabilidade exclusiva da Parte contrária e que venha impactar diretamente a operação da outra Parte; e/ou (iii) ação, procedimento ou demanda promovida por terceiros relacionada a qualquer dos eventos previstos nos itens (i) e (ii), acima, isentando a Parte prejudicada, suas controladoras, controladas, coligadas e/ou fornecedores de quaisquer danos diretos comprovadamente resultantes dos eventos descritos acima.

9.1. Nenhuma das Partes responderá por insucessos comerciais, danos emergentes, lucros cessantes ou danos indiretos da outra Parte em decorrência de imperfeita execução do presente Contrato, ressalvadas as hipóteses de multa contratual e/ou responsabilidade expressamente previstas neste Contrato.

9.2. O presente Contrato não confere a qualquer das Partes poderes para assumir ou criar qualquer obrigação, expressa ou implícita, em nome de outra Parte, nem representar essa outra como agente, funcionário, representante ou qualquer outra função, permanecendo cada qual como inteiramente independente da outra.

9.3. As Partes declaram e garantem que:

i. os seus representantes que firmam o presente Contrato, possuem plena capacidade para celebrá-lo e realizar todas as operações aqui previstas, independentemente de qualquer outra autorização, tendo tomado todas as

medidas de natureza societária e outras eventualmente necessárias para autorizar a sua celebração; e que,

ii. a celebração deste Contrato e o cumprimento das obrigações aqui previstas, não violam ou violarão qualquer disposição dos seus documentos societários ou das disposições de qualquer Contrato ou instrumento que tenham celebrado, não infringem ou infringirão qualquer disposição de lei, decreto, norma, ordem administrativa ou judicial ou regulamento aos quais esteja o presente Contrato sujeito, e não exigem ou exigirão qualquer consentimento, aprovação ou autorização de, aviso a, ou arquivamento ou registro junto a qualquer pessoa física ou jurídica, tribunal ou autoridade governamental.

10. DO CASO FORTUITO OU FORÇA MAIOR

10.1. As Partes não terão qualquer responsabilidade caso não cumpram quaisquer das disposições do presente Contrato em virtude da ocorrência de casos fortuitos ou de força maior, nos termos do Artigo 393 do Código Civil, desde que a(s) Parte(s) que se veja(m) impossibilitada(s) de cumprir com suas obrigações notifique à(s) outra(s) Parte(s), imediatamente, a respeito de tal circunstância.

10.2. A Parte que for afetada por caso fortuito ou motivo de força maior envidará seus melhores esforços para que cessem seus efeitos com a maior brevidade possível, não sendo isto possível, as Partes poderão rescindir o presente Contrato sem quaisquer ônus.

10.3. Cessados os efeitos de caso fortuito ou motivo de força maior, a situação original e regular de cumprimento das obrigações contratuais, quando possível e havendo consenso mútuo, deverá ser imediatamente restabelecida.

10.4. Se a ocorrência de caso fortuito ou motivo de força maior prejudicar apenas parcialmente a execução das obrigações oriundas deste Contrato, por uma das Partes, a Parte afetada deverá cumprir as obrigações que não tiverem sido afetadas pela ocorrência do caso fortuito ou motivo de força maior, em sua maior extensão possível.

10.5. Quaisquer das PARTES poderá extinguir o Contrato na ocorrência de caso fortuito e/ou força maior que afete a sua execução, e o mantenha suspenso por mais de 90 (noventa) dias corridos, bem como se for comprovada a impossibilidade de cumprir o seu objeto.

11. ANTICORRUPÇÃO E ÉTICA NOS NEGÓCIOS

11.1. Neste ato, as PARTES declaram possuir:

i. códigos próprios de conduta que contemplam as diretrizes e os princípios de comportamento ético, íntegro e transparente a que se subordinam os seus administradores, empregados e colaboradores; e,

ii. programas de compliance que visam garantir:

(a) o cumprimento da legislação, códigos, regulamentos, regras, políticas e procedimentos de anticorrupção de qualquer governo ou autoridade

competente, considerando a jurisdição onde os negócios e serviços serão conduzidos ou realizados nos termos deste Contrato – em especial, a Lei nº 12.846/2013, o Decreto nº 8.420/2015 e a Lei dos Estados Unidos da América contra práticas de corrupção no exterior ("FCPA") –; e,

(b) a identificação de desvios de conduta de seus administradores, empregados e demais colaboradores, direta ou indiretamente vinculados.

11.2. Nesse sentido, a PROPONENTE declara e garante que:

11.3. Visando garantir a efetividade do seu Programa de Compliance, dissemina e treina seus empregados, subcontratados, consultores, agentes e/ou representantes acerca do tema anticorrupção;

11.4. Tem conhecimento que a TIM pauta seus negócios e sua atuação na observância da ética e pelo desenvolvimento e crescimento sustentável, razão pela qual se compromete a respeitar e a proteger os direitos humanos, o direito do trabalho, os princípios da proteção ambiental e da luta contra todas as formas de corrupção, à luz dos princípios do Pacto Global das Organizações das Nações Unidas;

11.5. Reconhece que estão publicados no site da TIM os termos do seu Código de Ética e Conduta, da Política Anticorrupção e da Política de Conflito de Interesses disponíveis em http://www.tim.com.br/ri > ESG > Regulamentos e Políticas > Sobre a TIM > Sustentabilidade > O Nosso Modelo para Sustentabilidade, cujas diretrizes são amplamente divulgadas e disseminadas no âmbito da companhia, ao mercado e à sociedade;

11.6. Cumprirá e fará com que todos os seus empregados, subcontratados, consultores, agentes e/ou representantes que estejam relacionados ao escopo do presente Contrato, ainda que de forma indireta, cumpram o Código de Ética e de Conduta, a Política Anticorrupção e de Conflito de Interesses da TIM, mencionado no item 12.5;

11.7. Tem conhecimento que a TIM repudia e condena atos de corrupção em todas as suas formas, inclusive suborno, extorsão e propina, em especial, os previstos na Lei nº 12.846/2013 e no "FCPA", o financiamento ao terrorismo, o trabalho infantil, ilegal, forçado e/ou análogo ao escravo, bem como todas as formas de exploração de crianças e adolescentes e todo e qualquer ato de assédio ou discriminatório em suas relações de trabalho, inclusive na definição de remuneração, acesso a treinamento, promoções, demissões ou aposentadorias, seja em função de raça, origem étnica, nacionalidade, religião, sexo, identidade de gênero, orientação sexual, idade, deficiência física ou mental, filiação sindical ou que atente contra:

i. os direitos humanos e/ou impliquem ou resultem em torturas, físicas ou mentais;
ii. a saúde e a segurança pessoal e/ou do ambiente de trabalho;
iii. o direito de livre associação dos colaboradores;
iv. os direitos ambientais e de sustentabilidade; e,
v. a valorização da diversidade.

11.8. Não foi condenada por qualquer ato lesivo à administração pública, nem foi ou está listada por qualquer governo ou agência pública (tal como Nações Unidas ou

Banco Mundial) como excluída, suspensa ou está indicada para exclusão e/ou suspensão ou inelegível para programas de licitação do governo.

11.9. Considerando a responsabilidade estabelecida pelo artigo 2º da Lei nº 12.846/2013, a PROPONENTE não praticará qualquer ato lesivo previsto na referida lei - em especial, não ofereceu pagar, nem pagou, não pagará, oferecerá, prometerá ou dará, direta ou indiretamente, qualquer valor ou coisa de valor, incluindo quaisquer eventuais valores a ela pagos pela TIM, a qualquer funcionário ou oficial de um governo, empresa ou sociedade controlada pelo governo ou de propriedade do mesmo, partido político, candidato para cargo político, ou a qualquer outra pessoa estando ciente de ou acreditando que tal valor ou item de valor será transmitido a alguém para influenciar qualquer ação, omissão ou decisão por tal pessoa ou por qualquer órgão governamental com a finalidade de obter, reter ou conduzir negócios para si e/ou para a TIM - bem como em violação aos preceitos contidos no "FCPA", em interesse e/ou em benefício, exclusivo ou não, da TIM.

11.10. Além disso, a PROPONENTE declara tomar, neste ato, conhecimento do Canal de Denúncias da TIM, disponível em http://www.tim.com.br/canal-denuncia/?origin=RI, e se compromete a, sempre que possível, submeter ali toda e qualquer tentativa e/ou prática a que for submetida, tomar conhecimento, ou contra qual for investida que enquadre-se nas condutas descritas na Lei nº 12.846/2013 e/ou violem as normativas internas da TIM, em especial, mas não se limitando, ao Código de Ética e Conduta, a Política Anticorrupção, a Política de Conflito de Interesses e/ou legislações vigentes.

11.11. A TIM poderá, independentemente de qualquer disposição contrária contida neste Contrato e mediante notificação prévia, suspender e/ou rescindir este Contrato em caso de comprovada violação de qualquer declaração e/ou garantia estabelecida na presente Cláusula.

11.12. A PROPONENTE indenizará e isentará a TIM de e contra qualquer perda, reivindicação, custa ou despesa incorrida pela TIM, baseadas em ou decorrentes de qualquer violação das declarações e garantias estabelecidas na presente Cláusula ou em razão de qualquer violação ao disposto na legislação supra citada decorrente de qualquer ato, ativo ou omissivo, da PROPONENTE e/ou de seus Conselheiros, diretores, funcionários e/ou representantes.

11.13. A PROPONENTE se compromete a, sempre que solicitada, prestar (i) declaração de conformidade com as obrigações assumidas na presente cláusula e/ou (ii) esclarecimento acerca de eventual questionamento referente à fato ou evento relacionado às obrigações contidas na presente cláusula, compartilhando eventuais documentos solicitados.

11.14. Por fim, a TIM declara que as disposições deste Contrato foram negociadas à luz e em estrita observância ao seu Código de Ética e de Conduta e à legislação de proteção ao meio ambiente, demonstrando seu compromisso com o desenvolvimento sustentável e na manutenção do equilíbrio dos ecossistemas, conforme Política Ambiental disponível em http://ri.tim.com.br/ - > ESG > Regulamentos e Políticas. Além disso, no que se refere às disposições contidas na presente Cláusula, a PROPONENTE, na qualidade de fornecedora e/ou parceira comercial, se compromete a observar e difundir em sua cadeia de negócios os princípios e valores éticos e sociais supramencionados, bem como o de concorrência.

12. RESPONSABILIDADE DE ATENDIMENTO AO CLIENTE

12.1. A responsabilidade de atendimento aos seus usuários é única e exclusiva da TIM, que deverá seguir todas as obrigações, prazos e regras estabelecidas pela ANATEL órgãos de defesa do consumidor e demais autoridades administrativas e judiciais, bem como a legislação vigente pertinente.

12.2. A TIM deverá indicar, em instrumento específico, a descrição do sistema de atendimento ao Usuário e o modo de proceder em caso de solicitações ou reclamações.

13. COBERTURA DO SERVIÇO

13.1. A PROPONENTE tem ciência que a Área de Cobertura da TIM está divulgada no Mapa de Cobertura no site da TIM (www.tim.com.br), e atende às localidades onde a PROPONENTE terá atuação.

13.2. Nos casos de necessidade de implementação de cobertura outdoor e indoor, para atender suas necessidades de negócio, não previstas na proposta e durante o processo de negociação, caberá a PROPONENTE arcar com os custos de equipamentos, sempre respeitando as premissas de fornecedores homologados/certificados pela TIM.

14. PROTEÇÃO DE DADOS

14.1. Para os fins deste Contrato, são considerados:

(a) “DADOS PESSOAIS”: qualquer informação obtida em meio online ou offline e capaz de identificar ou tornar identificável uma pessoa natural singular (“TITULAR ou TITULAR DOS DADOS”), incluindo informações que possam ser combinadas com outras para identificar um indivíduo, e/ou que se relacionem com a identidade, características ou comportamentos de um indivíduo ou influenciem na maneira como tal indivíduo é tratado ou avaliado; por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica (tais como cookies, beacons e tecnologias correlatas) ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular. A definição de Dados Pessoais também inclui o conceito de DADOS PESSOAIS SENSÍVEIS;

(b) “TRATAMENTO” (e os termos relacionados “TRATAR” e “TRATADOS”): qualquer operação ou conjunto de operações efetuadas com Dados Pessoais ou com conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. A PROPONENTE declara que o tratamento aqui definido será realizado no Brasil;

(c) “BASE LEGAL”: requisitos para o tratamento de Dados Pessoais definidos nos artigos 7º e 11 da Lei nº 13.709/2018. A identificação da base legal para cada dado pessoal a ser coletado pela PROPONENTE será realizada pela

PROPONENTE, cabendo a esta a obrigação de apontar qual a base legal que deseja utilizar para legitimar cada operação de tratamento de cada dado pessoal a ser tratado pela TIM;

(d) "CONTROLADOR": parte a quem competem as decisões referentes ao tratamento de Dados Pessoais, inclusive quanto à determinação das finalidades e dos meios de tratamento;

(e) "OPERADOR": parte que trata Dados Pessoais de acordo com as instruções do CONTROLADOR e em seu nome;

(f) "INCIDENTE": incidente de segurança ocorrido no contexto do tratamento de Dados Pessoais e que possa acarretar risco ou dano relevante aos seus titulares, inclusive hipóteses de tratamento indevido de Dados Pessoais.

14.2. As Partes declaram, por este Instrumento, que cumprem toda a legislação aplicável sobre privacidade e proteção de dados, inclusive (sempre e quando aplicáveis) a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet (Lei Federal n. 12.965/2014), seu decreto regulamentador (Decreto 8.771/2016), a Lei Geral de Proteção de Dados (Lei Federal n.13.709/2018), e demais normas setoriais ou gerais sobre o tema, inclusive as estrangeiras.

14.3. As Partes reconhecem que, em virtude da celebração desse Contrato, podem ser realizadas operações de tratamento de Dados Pessoais. Em especial, concordam as Partes que, para os fins da legislação relacionada à proteção de Dados Pessoais aplicável, no âmbito do Contrato, a PROPONENTE e a TIM devem ser consideradas como Controladora de Dados Pessoais, caracterizando uma controladoria conjunta entre as Partes.

14.3.1. As Partes declaram e garantem que cumprem e que continuarão cumprindo toda e qualquer obrigação legal aplicável relacionada à privacidade e à proteção de Dados Pessoais em decorrência do exercício de suas atividades no contexto do Contrato, sendo certo que manterão em segurança todos e quaisquer Dados Pessoais a que tiverem acesso em virtude da relação estabelecida em decorrência do Contrato.

14.3.2. Concordam as Partes que todos os Dados Pessoais tratados no contexto deste Contrato, inclusive todos os Dados Pessoais disponibilizados para tratamento em conexão com a prestação dos serviços objeto deste Contrato pela TIM, serão fornecidos, compartilhados e/ou disponibilizados pela própria PROPONENTE e/ou pelos terceiros por ela designados para tal finalidade, sem qualquer ingerência da TIM nesse sentido.

14.3.3. Para fins de esclarecimento, concordam as Partes que não constitui uma obrigação da TIM sob o Contrato o fornecimento, o compartilhamento e/ou de qualquer forma a disponibilização de acesso a quaisquer Dados à PROPONENTE ou a terceiros, exceto aqueles necessários para garantir o cumprimento das obrigações da TIM expressamente previstas no item 2.3 deste Contrato.

14.4. As Partes declaram e garantem que toda e qualquer operação de coleta, uso, tratamento e armazenamento de Dados Pessoais no âmbito do Contrato será

realizada única e exclusivamente de forma a cumprir as finalidades relacionadas à execução do objeto deste Contrato e nos estritos limites das atribuições de cada Parte, conforme os termos do Contrato e da Resolução nº 550/2010 da Anatel, observados os princípios de proteção de dados e sempre utilizando uma Base Legal válida para tal Tratamento, podendo ser, por exemplo, por meio do consentimento livre, informado e inequívoco do titular dos Dados Pessoais, exclusivamente para a realização de finalidades determinadas, ou mesmo por meio da necessidade do atendimento de interesse legítimo das Partes e/ou de terceiros com quem as Partes mantenham relação jurídica, desde que dentro das legítimas expectativas dos respectivos titulares dos Dados Pessoais objeto do tratamento.

14.4.1. Sem prejuízo das demais disposições do Contrato, ficam vedadas quaisquer operações de tratamento de Dados Pessoais que sejam discriminatórios e proibidas pela legislação de privacidade e proteção de dados aplicável, ou incompatíveis com a natureza do dado pessoal tratado.

14.4.2. Qualquer tratamento de Dados Pessoais realizado pelas Partes que extrapole as finalidades previstas neste Contrato será de responsabilidade exclusiva da Parte que o realizar, obrigando-se tal Parte a indenizar a outra Parte por todo e qualquer dano e prejuízo eventualmente causado em razão de tal tratamento não autorizado.

14.5. No contexto do tratamento de Dados Pessoais pela PROPONENTE em conjunto a terceiros, incluindo, mas não se limitando aos seus fornecedores, fica estabelecido que todas as disposições estabelecidas nesta cláusula serão aplicáveis a tais terceiros, sendo a PROPONENTE a única e exclusiva responsável perante a TIM por quaisquer perdas e danos causados à TIM e/ou a terceiros por tais terceiros em razão de eventual violação desta cláusula ou da legislação aplicável por tais terceiros e/ou pela PROPONENTE no contexto do tratamento de Dados Pessoais.

14.6. As Partes garantem que as informações tratadas no âmbito do Contrato estarão armazenadas em ambiente seguro, em servidores localizados no Brasil ou no exterior, observado o estado da técnica disponível, valendo-se de políticas e tecnologias de segurança como criptografia, controles de acesso e certificações de segurança específicos, e somente poderão ser acessadas por pessoas qualificadas e autorizadas pelas Partes, responsabilizando-se cada Parte por todo e qualquer acesso indevido a que tenha dado causa. Cada Parte se compromete a imediatamente informar a outra Parte em caso de suspeita ou de efetiva perda, destruição, alteração, divulgação e acesso e/ou tratamento ilegal ou não autorizado dos Dados Pessoais, a fim de protegê-los contra violações, em desrespeito aos termos deste Contrato, da legislação aplicável, para evitar eventuais danos e prejuízos às Partes e a terceiros.

14.7. A TIM não será responsabilizada, em nenhuma hipótese, por eventuais ações, omissões, falhas ou erros da PROPONENTE e/ou de quaisquer funcionários, prepostos, representantes ou terceiros por ela contratados, incluindo, mas não se limitando aos seus fornecedores, no contexto do tratamento de quaisquer Dados Pessoais sob este Contrato, bem como por quaisquer perdas consequenciais ou decorrentes do tratamento direto ou indireto dos Dados Pessoais, devendo a PROPONENTE indenizar e manter a TIM isenta de qualquer responsabilidade

nesse sentido, independentemente de existência ou ausência de comprovação de dolo ou culpa por parte da TIM.

14.7.1. Fica assegurado às Partes, nos termos da lei, o direito de regresso em face da Parte responsável diante de eventuais danos causados por esta em decorrência do descumprimento das obrigações legais, regulatórias ou contratuais, por ação ou omissão, em relação à proteção dos Dados Pessoais tratados no âmbito deste Contrato, no valor integral das perdas e danos sofridos, incluindo sanções administrativas, eventuais condenações, acordos, termos de ajuste de conduta, custas processuais, honorários advocatícios, honorários periciais e demais despesas decorrentes de tal descumprimento, em linha com a cláusula 2.3.3, sem prejuízo das demais penalidades previstas neste Contrato.

15. DISPOSIÇÕES FINAIS

15.1. Alteração. Qualquer alteração dos termos e condições deste Contrato somente será considerada válida se formalizada por escrito, em instrumento próprio, assinado por todas as Partes.

15.2. Natureza Vinculante. As Partes estabelecem, de forma irrevogável e irretratável, que se comprometem, desde já, a cumprir integralmente, o presente Contrato o qual é acordado de forma vinculante.

15.3. Renúncia. A tolerância de qualquer das Partes a um determinado inadimplemento de outra Parte não afetará ou prejudicará os direitos da Parte tolerante com relação a qualquer inadimplemento subsequente desta ou de outra natureza; nem o atraso ou omissão de qualquer das Partes no exercício de qualquer direito afetará ou prejudicará quaisquer direitos que a Parte inadimplente possa ter com relação a este ou qualquer futuro inadimplemento.

15.4. Nulidade Parcial. Se qualquer disposição deste Contrato for considerada inválida ou inexequível por qualquer motivo, tal invalidade não afetará a validade das demais disposições deste instrumento, e as Partes substituirão mediante acordo a disposição inválida por outra válida que mais se aproximar da intenção e do efeito econômico da disposição inválida.

15.5. Avisos. Todos os avisos que qualquer uma das Partes deva ou pretenda enviar à(s) outra(s) serão enviados por escrito e entregues pessoalmente para seus representantes legais. Qualquer aviso entregue será considerado dado somente após o comprovante de recebimento de fato das Partes a serem notificadas.

15.6. Cessão ou Transferência. O presente Contrato obriga as Partes, seus sucessores a qualquer título, tendo automaticamente sua titularidade transferida à entidade superveniente, e eventuais cessionários autorizados, sendo que qualquer outra alteração ou modificação contratual só terá validade mediante a celebração de termo aditivo, o qual deverá ser devidamente assinado pelos representantes legais das Partes.

15.7. Solução de conflitos. As Partes se comprometem em boa-fé empreender os melhores esforços para dirimir eventuais conflitos oriundos do presente Instrumento.

15.7.1. Caso haja conflito de interesses entre as Partes, o mesmo poderá ser submetido Processo de Resolução de Conflitos por meio de requerimento dirigido à ANATEL.

15.8. Este Contrato contém o compromisso integral entre as Partes com relação ao seu objeto e substitui todo e qualquer instrumento contratual ou acordo anterior, escrito ou oral, com relação a todas as questões cobertas por este Contrato ou nele mencionadas.

15.9. Este Contrato não cria qualquer tipo de sociedade, associação, joint venture ou qualquer outra relação de natureza semelhante entre as Partes, não sendo permitido qualquer das Partes agir em nome da outra.

15.10. As Partes reconhecem expressamente que todas as disposições deste Contrato foram integralmente negociadas e aceitas com o respaldo de seus consultores jurídicos, refletindo, portanto, a boa-fé subjetiva das Partes nesta contratação.

15.11. Quaisquer valores e penalidades previstos e oriundos do presente Contrato serão considerados dívidas líquidas e certas, servindo, para tanto, o presente instrumento, como título executivo extrajudicial, nos termos do art. 784, III do Código de Processo Civil.

15.12. As Partes reconhecem e anuem expressamente a veracidade, autenticidade, integridade, validade e eficácia deste Contrato nos termos dos artigos 104 e 107 do Código Civil, assinado pelas Partes em formato eletrônico e/ou por meio de certificados eletrônicos, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

16. FORO E LEIS APLICÁVEIS

16.1. O presente Contrato será regido pela lei brasileira. Fica eleito o foro da Comarca da Capital do Estado de São Paulo para solucionar qualquer controvérsia oriunda deste instrumento, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

E, por estarem assim justos e acordados, as Partes firmam o presente Contrato em 2 (duas) vias de igual forma e teor, na presença das testemunhas abaixo identificadas.

Rio de Janeiro, XX de XXXXXXX de 20XX.

_____	_____
TIM S.A.	**PROPONENTE**

Testemunhas:

_____	_____
Nome:	Nome:
CPF:	CPF:

ANEXO I

DEFINIÇÕES

Aplicam-se as seguintes definições para os fins deste Contrato, além das previstas na regulamentação vigente e, em especial, no Regulamento do Serviço Móvel Pessoal:

a) **Cliente**: usuários provenientes da parceria firmada por meio deste Contrato de Agente Credenciado.

b) **Credenciamento**: é o Contrato de representação, objeto de livre negociação, entre o Credenciado e a Prestadora de Origem, cuja eficácia depende de homologação pela ANATEL, nos termos da Resolução ANATEL nº 550/2010.

c) **Credenciado de Rede Virtual (Credenciado)**: é a pessoa jurídica, credenciada junto à Prestadora Origem, apta a representá-la na Prestação do Serviço Móvel Pessoal, devendo ser empresa constituída segundo as leis brasileiras, com sede e administração no País, , nos termos da Resolução ANATEL nº 550/2010;

d) **Dados:** é o valor pago pela utilização do tráfego de dados. O valor será cobrado por megabyte trafegado na rede TIM;

e) **Inadimplemento substancial**: considera-se inadimplemento substancial qualquer fato que venha a inviabilizar a operação, seja oriundo de práticas espontâneas da parte que deu causa, seja oriundo de caso fortuito ou força maior.

f) **MVNO**: Mobile Virtual Network Operator;

g) **MVNO Credenciada da TIM:** Operadora Móvel Virtual (MVNO) credenciada pela TIM;

h) **MVNE**: Mobile Virtual Network Enabler;

i) **MVNA**: Mobile Virtual Network Aggregator;

j) **Prestadora Origem**: é a Autorizada do Serviço Móvel Pessoal com a qual o Credenciado de Rede Virtual possui relação para a exploração de SMP por meio de Rede Virtual;

k) **Projeto Técnico:** Valor aplicado pela TIM para elaboração e implementação do projeto técnico de compartilhamento Sistemas (topologia, requisitos funcionais e técnicos), incluindo investimentos, adaptações tecnológicas e integrações técnicas necessárias para permitir o funcionamento da PROPONENTE. O pagamento do Projeto Técnico ocorrerá 30 (trinta) dias a após sua entrega. Para fins de recebimento de valores referentes a projeto técnico, a TIM deverá encaminhar a MVNO a Nota Fiscal, com a antecedência mínima de 05 (cinco) dias úteis da data do respectivo vencimento. Os custos serão devidamente justificados e apresentados pela TIM à PROPONENTE.

l) **Rede Virtual no Serviço Móvel Pessoal (Rede Virtual)**: é o conjunto de processos, sistemas, equipamentos e demais atividades utilizadas pelo Credenciado de Rede Virtual para a exploração de SMP por meio da rede da Prestadora Origem, nos termos da Resolução ANATEL nº 550/2010;

m) **Representação**: é a atividade desenvolvida pelo Credenciado com o objetivo de compor, juntamente com a Prestadora Origem, etapas da Prestação do SMP, podendo, inclusive, agregar valor a essa Prestação, não se confundindo com a Representação Comercial, de que trata a Lei nº 4.886, de 09 de dezembro de 1965, nos termos da Resolução ANATEL nº 550/2010.

n) **SMP**: Serviço Móvel Pessoal;

ANEXO II

CONDIÇÕES COMERCIAIS E REMUNERAÇÃO

1. CONDIÇÕES COMERCIAIS

1.1. O presente Contrato tem como objeto a disponibilização, pela TIM, em caráter isonômico e não discriminatório, da infraestrutura de Rede de Acesso necessária para permitir a habilitação de MVNOs em sua rede móvel, devendo a PROPONENTE comprovar sua capacidade econômica, financeira e técnica para prestação dos serviços, de modo que a PROPONENTE forneça aos seus Clientes os serviços de Voz, Dados e SMS em todas as tecnologias disponíveis e em uso pela TIM, na localidade em questão, tais como:

a) 2G - utilização de Voz e Mensagem de Texto em CS (Circuit Swichting), Dados em GPRS e EDGE;
b) 3G - utilização de Voz e Mensagem de Texto em CS (Circuit Swichting), Dados em UMTS e WCDMA;
c) 4G - utilização de Voz em PS (Packet Swichting - VoLTE) e Dados em LTE, incluindo M2M e IoT; e
d) 5G - utilização de Voz em PS (Packet Swichting - VoLTE) e Dados em DSS, Non Standalone e Standalone, incluindo M2M e IoT.

1.2. Em observância aos custos de Projeto Técnico, conforme definido no Anexo I, para implementação do serviço de MVNO Credenciada, a PROPONENTE se compromete a pagar o valor de **R$ 1.500.000,00 (um milhão e quinhentos mil reais, líquido de impostos)**, em até 30 (trinta) dias após a finalização do credenciamento junto à ANATEL, sob pena de extinção deste Contrato. Os custos serão devidamente justificados e apresentados pela TIM à PROPONENTE.

1.2.1. Para fins de recebimento de valores referentes a projeto técnico, a TIM deverá encaminhar a PROPONENTE a Nota Fiscal, com a antecedência mínima de 05 (cinco) dias úteis da data do respectivo vencimento. Sendo o faturamento processado pela filial da TIM situada à Av. Alexandre de Gusmão, nº 29, Bloco B, Vila Homero Thon, Santo André/SP, inscrita no CNPJ/MF sob o nº 02.421.421/0231-62 e com Inscrição Municipal sob o nº 249349.

1.2.2. Para as PROPONENTES que já possuam acordo de MVNO com a TIM e estejam totalmente integradas, não será aplicada cobrança de Projeto Técnico, exceto nos casos que demandar investimentos para adaptações tecnológicas e integrações técnicas necessárias para permitir o funcionamento da PROPONENTE em novos serviços e tecnologias.

1.3. A PROPONENTE também se compromete a gerar a receita bruta mínima (somatório de todas as recargas de seus clientes) anual, de forma progressiva e nunca menor que no ano antecessor, conforme listada na tabela abaixo:

COMPROMISSO DE RECEITA BRUTA MÍNIMA ANUAL

ANO	Valor
1	R$ 7.500.000 (sete milhões e quinhentos mil reais)
2	R$ 10.000.000 (dez milhões de reais)
3	R$ 20.000.000 (vinte milhões de reais)
4	R$ 30.000.000 (trinta milhões de reais)
5	R$ 40.000.000 (quarenta milhões de reais)

1.4. Caso a PROPOENTE não atinja o compromisso de receita bruta mínima anual, a TIM realizará a cobrança do valor remanescente (diferença entre o valor do compromisso anual, subtraído do valor arrecadado no ano em questão) em até 30 (trinta) dias após o período de apuração anual, correspondente ao aniversário do lançamento comercial.

1.5. A PROPONENTE estará inadimplente nos termos deste Contrato, enquanto não forem quitados os valores referentes ao compromisso de receita bruta mínima anual. Não fazendo jus a qualquer remuneração prevista no item 3.2 deste Anexo II até que esteja adimplente novamente.

1.6. A TIM poderá solicitar a qualquer momento uma garantia financeira, que deverá ser apresentada no prazo, modalidade e valor estipulados pela TIM em condições estabelecidas em termo aditivo a este Contrato.

1.6.1. A apresentação da Garantia Financeira na modalidade, valor e prazo estipulados pela TIM é uma obrigação da PROPONENTE e sua não apresentação implica em inadimplemento contratual.

2. CRIAÇÃO DE PLANOS E OFERTAS

2.1. A criação de planos e ofertas será definida conjuntamente pela TIM e a PROPONENTE, assim como suas condições, facilidades e comodidades a serem ofertadas, nos termos da Resolução ANATEL nº 550/2010.

2.2. A PROPONENTE poderá oferecer somente planos pré-pagos.

2.2.1. As Partes poderão acordar a oferta de planos controle e pós-pago mediante a termo aditivo a este Contrato.

3. REMUNERAÇÃO DAS PARTES

3.1. Em contrapartida ao cumprimento das obrigações previstas neste Contrato, a PROPONENTE será paga pela TIM exclusivamente a remuneração estabelecida no item 3.2 deste Anexo II, integrante ao Contrato.

3.2. A PROPONENTE será remunerada a cada recarga efetuada por seu cliente, em sua rede própria e na rede da TIM, em um valor percentual de **7%** (sete por cento) sobre o valor bruto de recarga.

3.3. Com o objetivo de incentivar um maior número de recargas, a PROPONENTE poderá contratar um pacote de dados, com custo de atacado, a qualquer momento, para ser utilizado como bonificação aos seus Clientes, conforme a tabela abaixo:

PACOTE DE BONIFICAÇÃO	R$/MB
Até 1 TB	0,0050
1TB a 10 TB	0,0049
10 TB a 50 TB	0,0048
50 TB a 100 TB	0,0047

3.3.1. Os valores da tabela de bonificação acima são líquidos de impostos.

3.3.2. A cobrança do pacote de bonificação se dará por meio do encontro de contas, isto é, valor do comissionamento apurado no mês, subtraído do custo do(s) pacote(s) contratado(s).

4. OBSERVAÇÕES GERAIS

4.1. Os valores descritos neste anexo serão reajustados anualmente com base na variação do Índice Nacional de Preços ao Consumidor Amplo (IPCA) da Fundação Getúlio Vargas, ou por outro índice que eventualmente venha a substituí-lo.

4.2. As Partes concordam em negociar, a qualquer momento durante a vigência do Contrato, preços promocionais por tipo de serviço prestado, de acordo com a disponibilidade e/ou viabilidade, por meio de um termo aditivo a este contrato.

ANEXO III

GARANTIA FINANCEIRA

1. Para amparar financeiramente a operação descrita no presente Contrato**,** a **PROPONENTE** deverá disponibilizar, a favor da TIM, uma garantia financeira, a ser definida entre Fiança Bancária, CDB Caucionado ou Depósito Bancário (por meio de adiantamento), respeitando as seguintes premissas:

1.1. A garantia financeira será calculada conforme o volume financeiro (faturamento mensal a ser devido pela **PROPONENTE**), previsto no plano de negócio da **PROPONENTE**, a ser preparado pela **PROPONENTE** e apresentado à TIM, respeitando-se as regras de governança e protocolos de confidencialidade estabelecidos em acordos e manuais operacionais específicos, para o período de 12 (doze) meses futuros, ou conforme o compromisso financeiro assumido pela PROPONENTE para os 12 (doze) meses futuros, o que for maior;

1.2. Somente serão aceitas garantias financeiras de bancos de primeira linha, conforme definição da TIM;

1.3. O prazo para disponibilização da garantia e os dados do banco emissor deverão ser apresentados à **TIM** para sua aprovação, no prazo de 60 (sessenta) dias antes do lançamento comercial. Após aprovação, a **PROPONENTE** terá o prazo de 15 (quinze) dias para entregar à **TIM** a referida garantia emitida. O lançamento Comercial estará condicionado a disponibilização da referida garantia.

1.4. A garantia deverá possuir prazo mínimo de vigência de 12 (dose) meses, devendo a **PROPONENTE** apresentá-la à TIM, ou providenciar sua renovação, se for o caso, em até 30 (trinta) dias antes do respectivo vencimento, mantendo-a válida durante toda vigência do Contrato, sob pena de rescisão do Contrato por inadimplemento e cobrança de penalidades nos termos da cláusula 4.5 deste Contrato;

1.5. A garantia oferecida (tipo, valor, etc), poderá ser reavaliada pela TIM, a qualquer momento, havendo a possibilidade de manutenção da garantia atual, troca do

tipo de garantia, dispensa de apresentação de garantias, ou ainda, solicitação de novas garantias;

2. Em caso de inadimplemento contratual ou não pagamento pontual dos valores devidos pela **PROPONENTE** à TIM nos termos do presente Contrato, a TIM estará autorizada a executar a Garantia, independente de notificação prévia à MVNO, nos valores devidos, acrescidos dos encargos financeiros, conforme métrica abaixo:

    a) multa moratória de 2% (dois por cento) sobre o valor total do débito original, aplicável a partir do dia seguinte ao do vencimento;
    b) juros de mora de 1% (um por cento) ao mês sobre o débito, calculados pro rata temporis, contados a partir da data de vencimento do Documento de Cobrança até a efetiva liquidação do débito;
    c) atualização dos valores em atraso pelo IPCA, ou por outro índice que venha a substituí-lo, até a data da efetiva liquidação do débito total.

3. Na hipótese de inadimplência da **PROPONENTE** com relação à apresentação, renovação ou recomposição da garantia financeira, ou ao pagamento de quaisquer valores devidos pela MVNO à TIM, relacionados ao Contrato, ambos por até 30 (trinta) dias consecutivos e considerando as obrigações de continuidade na prestação do serviço aos clientes, o Contrato poderá ser rescindido a critério da TIM nos termos da cláusula 4.5 deste Contrato.

ANEXO IV

ANEXO TÉCNICO DE SEGURANÇA

Índice

OBJETIVO E CAMPO DE APLICAÇÃO

Este documento tem o objetivo de formalizar os requisitos de segurança lógica e física (doravante, Requisitos) para a proteção das informações e Ativos TIC/infraestrutura da TIM (doravante, TIM), determinando as regras a serem incluídas no anexo técnico do contrato/contrato de serviços com os fornecedores (doravante, Terceiro).

Os requisitos estão agrupados de acordo com os seguintes temas:

A	Proteção de informação
B	Requisitos de Eventos e Incidentes de Segurança
C	Segurança Física para os Escritórios de Terceiro
D	Estações de Trabalho, Servidores e demais dispositivos de terceiros
E	Sistemas de Informação de Terceiros
F	Infraestrutura de Rede de Terceiros
G	Segurança Física para os Escritórios da TIM
H	Estações de Trabalho da TIM
I	Sistemas de informação da TIM – Acesso e Uso

J	Acesso Local à Infraestrutura de Rede da TIM
K	Acesso Remoto à Infraestrutura de Rede da TIM
L	Serviço de e-mail da TIM
M	Serviço de Conexão à Internet da TIM
N	Continuidade de Negócios
O	Desenvolvimento Seguro de Aplicativos de Software
P	Avaliação de Vulnerabilidade
Q	Serviços em Cloud (Cloud Service Provider)

REQUISITOS PARA TERCEIRO

A política de segurança e outros documentos normativos da TIM devem ser seguidas por terceiro que estejam dentro das dependências da TIM. Os itens relacionados aos capítulos G, H, I, J, K, L e M representam uma parte das orientações.

A. Proteção da informação

No que diz respeito à TIM, informação significa qualquer agregação de dados que tenha um valor e um significado para a TIM, qualquer que seja a forma e as tecnologias usadas para seu processamento e armazenamento. A definição de informação inclui qualquer notícia ou comunicação em forma escrita ou verbal, ou qualquer conjunto de "dados estruturados" processados, comunicados, armazenados (manualmente ou por meios automáticos) e utilizados na execução do trabalho, bem como dados em um arquivo ou código de programa.

1) O terceiro deve garantir que as informações proprietárias da TIM sejam processadas, de acordo com os princípios de "*Need to know*" e "Segregation of Duties", exclusivamente dentro do serviço contratual, evitando a divulgação para/ou na presença

de pessoas não autorizadas.

2) O terceiro é obrigado a processar as informações da TIM, seja em TI e/ou em forma de papel, salvaguardando a sua Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade, bem como em conformidade com as leis atuais.

3) O terceiro deve ter completa rastreabilidade dos acessos realizados nas informações da TIM, com o objetivo de identificar origem, autor, data/hora e informação acessada, com tempo mínimo de retenção de 02 (dois) anos.

4) O terceiro que presta serviços, produtos ou equipamentos para à TIM deve obrigatoriamente possuir Política de Segurança Cibernética, preferencialmente, tendo seu resumo publicado em seu Web Site.

5) O terceiro que presta serviços, produtos ou equipamentos para as infraestruturas críticas da TIM deve realizar periodicamente, auditorias independentes e comprová-las de acordo com a solicitação da TIM.

6) O terceiro que manipula, armazena ou fornece informações de dados pessoais da TIM, deve obrigatoriamente, criptografar os dados em repouso e em trânsito.

B. Requisitos de Eventos e Incidentes de Segurança

1) O terceiro deve identificar, internamente, uma estrutura/figura de referência para garantir a segurança do serviço prestado, que tem a tarefa de assegurar as relações entre o terceiro e a TIM para realizar a gestão transversal de todos os aspectos de segurança, comunicando previamente a TIM.

2) O contato com a área de segurança da TIM, para todos itens abaixo, deve ser realizado através do e-mail csoc@timbrasil.com.br.

3) O terceiro, através do seu Representante de Segurança deve informar imediatamente a TIM em caso de danos, roubo ou perda de ativos de TI contendo informações proprietárias e credenciais de acesso a TIM. Em relação aos casos que envolvem dispositivos de autenticação fortes, o terceiro deve também prever a revogação do certificado contido no dispositivo.

4) O terceiro é obrigado a notificar a TIM sobre todos os eventos, sem discriminação, inclusive os acidentais, e sobre as informações detalhadas relativas, que podem ser consideradas como violações de dados pessoais. Esta comunicação deve ser feita estritamente dentro de até 24 horas a partir do conhecimento dos eventos acima mencionados e enviada por e-mail para a pessoa de contato da TIM a quem o terceiro geralmente se refere na prestação de serviços e ao e-mail da área de Cyber Security citado no item 2. Neste sentido, o terceiro deve preparar ações internas adequadas para garantir essas obrigações (por exemplo, definindo procedimentos apropriados / instruções de operação) e deve garantir assistência a TIM fornecendo prontamente todas as informações adicionais que possam ser solicitadas pela própria, para avaliação e gestão corretas dos casos de potencial violação de dados pessoais.

5) As atividades de gerenciamento e resolução de incidentes devem ser devidamente documentadas e arquivadas, provendo toda linha do tempo do processo de tratamento.

6) Caso seja previsto em cláusulas contratuais, a possibilidade de utilização de outras empresas para execução do contrato, o terceiro deve garantir que esta empresa siga os requisitos expressos neste anexo técnico.

C. Segurança Física para os Escritórios de Terceiro

1) O terceiro, em suas instalações utilizadas para os serviços prestados a TIM, deve adotar proteções preventivas de segurança física e, quando possível, separar fisicamente as

instalações utilizadas exclusivamente para prestação do serviço contratado e sendo obrigatório quando for um serviço de atendimento que utilizam dados pessoais, cliente e colaboradores da TIM.

2) O terceiro deve manter um controle de acesso físico às instalações da empresa para colaboradores e visitantes.

3) O terceiro deve possuir um sistema de CFTV com gravação e armazenamento das imagens por pelo menos 30 dias on-line.

D. Estações de Trabalho, Servidores e demais dispositivos de terceiros

Para as estações de trabalho, servidores e demais dispositivos utilizados pelo terceiro, incluindo qualquer mídia de armazenamento removível (como pen drives USB, discos rígidos externos etc.), usada para o desempenho das atividades de trabalho previstas no contrato/acordo firmado com a TIM, o terceiro deve assegurar que:

1) Não devem ser usadas de maneira que possam causar danos às informações da TIM;

2) O acesso deve ser realizado por meio de credenciais de acesso individual, composto por combinação de uma credencial de identificação (UserID) e uma credencial de autenticação (senha forte, sempre que viável, com a utilização de duplo fator de autenticação, como: PIN);

3) As atualizações de software do sistema e de aplicativos necessárias para corrigir defeitos e evitar vulnerabilidades devem ser instaladas, mensalmente, com o objetivo de manter esses equipamentos sempre atualizados e protegidos. Para os casos de atualização de software de alta criticidade, a mesma deve ser realizada imediatamente;

4) Devem estar equipados com software antivírus, atualizados constantemente e com a função "monitor" sempre ativo, inclusive com Light Scan diário e Full Scan semanal. Além disso, a menos que tenham alguma restrição técnica, a possibilidade de desativar o antivírus pelo usuário deve ser inibida. Caso ocorra algum incidente com vírus, o usuário do fornecedor ou parceiro comercial deve comunicar o incidente ao contato de segurança;

5) Os dados de propriedade da TIM não devem ser salvos, exceto nos casos em que isso é previsto por contrato para atender às finalidades do serviço/atividade. Caso haja necessidade, prevista em contrato, de armazenamento das informações em mídias removíveis, as mesmas deverão ser criptografadas e devem ser removidas de todos os equipamentos no final da atividade;

6) A função de proteção de tela protegida por senha deve ser sempre ativada nas estações de trabalho de terceiros;

7) As estações de trabalho de terceiro quando conectadas às redes que lidam com os recursos da TIM:

- Devem estar equipadas com Firewalls Pessoais ativos, sendo desejável também Host IPS ou EDR/XDR;
- Devem estar livres de software contendo ferramentas capazes de permitir que sistemas certificados na Internet interajam, acessem ou gerenciem sistemas corporativos, por meio de fluxos de comunicação encapsulados no tráfego transmitido por proxies corporativos (por exemplo, Log Me In, Go to my PC);
- Elas não devem ser usadas como dispositivos de ponte (chamadas pontes) para a interconexão de redes logicamente ou fisicamente segregadas, em particular em estações de trabalho de terceiros equipadas com mais de uma interface de conexão

(por exemplo, placa de rede e modem presente em uma estação de trabalho de terceiro móvel). Elas nunca devem ser usadas simultaneamente;

- Devem ter acesso a internet restrito e controlado por proxy com políticas de proteções a sites maliciosos, a fim de proteger qualquer tipo de acesso indevido que exponha a estação de trabalho ou ambiente em risco;
- Devem estar com patches atualizados semanalmente.

E. Sistemas de Informação de Terceiros

Sistemas de informação de terceiros são os sistemas, plataformas ou, mais geralmente, as ferramentas tecnológicas físicas e lógicas dos terceiros através das quais a informação/dados da TIM são processados. Para estes sistemas de informação, o terceiro deve assegurar que:

1) Eles sejam mantidos em instalações protegidas e com acesso controlado;
2) Qualquer software instalado em sistemas de informação deve ser legalmente licenciado;
3) Exista um software antivírus atualizado sempre que houver versões disponíveis;
4) Os sistemas operacionais e aplicações, devem estar sempre atualizados, seguindo no mínimo as recomendações de Segurança do Padrão OWASP TOP10, sempre que aplicável. Sejam efetuadas reconfigurações apropriadas para a modificação/eliminação das configurações da aplicação e padrões do sistema, como senhas, comunidade SNMP, contas e serviços desnecessários;
5) Deve ocorrer a resolução de vulnerabilidades de segurança conhecidas de acordo com os padrões de proteção;
6) Todo ambiente deve ser protegido por Firewalls e IDS, assim como ter as devidas segregações de redes, a fim de proteger a infraestrutura, deixando exposto apenas o front-end e a camada de exposição. Além disso, para sistemas expostos na internet deve ter WAF (Web Application Firewall);
7) Sejam adotados procedimentos de backup adequados que contemplem dados da TIM, em concordância com o gestor do contrato. Estes procedimentos devem ser documentados e conter pelo menos a indicação da frequência, dos métodos de execução, do arquivamento e da retenção dos backups. Os dados devem ser mantidos apenas pela duração do período contratual, após isso, os mesmos devem ser entregues a TIM e eliminados;
8) No caso de danos ou incidentes nos seus sistemas de informação, devem ser adotados procedimentos operacionais específicos para a execução das atividades de restauração, que devem incluir tempos de implementação acordados com o gestor do contrato e que garanta a continuidade do serviço contratado pela TIM;
9) Para sistemas de informação que processam dados pessoais de propriedade da TIM, o armazenamento, e transmissão de dados devem ser realizados de forma criptografada, garantindo que não haja vazamento de informações;
10) Todos os usuários de acesso (incluindo os sistemas técnicos e M2M) devem ser identificados e gerenciados de acordo com procedimentos definidos e documentáveis seguindo melhores práticas de segurança de mercado, que permitam fornecer evidências das autorizações emitidas para usuários individuais;
11) Todos os usuários devem receber credenciais de acesso individuais, contendo um UserID e uma senha. Os UserIDs de um usuário não devem ser atribuídos novamente a outros usuários, mesmo em momentos diferentes, devem ser desativados para manter

todo o histórico dos usuários. Para usuários técnicos, o histórico documentado de liberação/uso deve ser fornecido;

12) A utilização de credenciais de acesso para usuários sistêmicos M2M deve ser utilizada apenas em caráter de Troubleshooting, de forma monitorada e após o uso, a senha deve ser alterada;

13) Caso o terceiro possua servidores em sua infraestrutura que vão se comunicar com os servidores da Tim, o mesmo deverá ter um cofre de senhas;

14) Os perfis de autorização definidos, para acesso aos dados do Ativo TIC, devem ser atribuídos com os privilégios proporcionais às necessidades mínimas para o desempenho das atividades/serviços contratados pela TIM (*Need to Know e* Segregation of Duties) esses perfis devem ser identificados e configurados antes do início do processamento para documentar os perfis que podem ser associados para cada usuário ou para um conjunto de usuários que executam a mesma função;

15) Uma verificação periódica de credenciais e perfis de acessos à sistemas devem ser realizada, pelo menos a cada três meses, e documentada em relação à necessidade de manter válidos os perfis definidos e às autorizações concedidas aos usuários;

16) Os acessos dos usuários que não estiverem mais atribuídos ao serviço da TIM ou que não precisem mais acessar os dados da TIM devem ser imediatamente removidos, a fim de impedir acessos indevidos as informações. Além disso, os acessos devem ser:

- Removidos, devido à inatividade, após 3 meses do último acesso realizado;
- Suspenso, após várias tentativas de logon incorretos;
- Suspenso como resultado de uso ilegal ou daqueles que colocam em risco a segurança. podendo ser solicitado também pelas empresas da TIM;
- Removido na data de expiração especificada na solicitação de autorização (a menos que seja estendida).

17) Em casos de sistemas, a senha de acesso aos seus sistemas de informação deve atender, no mínimo, às seguintes características:

- Composta por pelo menos 8 caracteres (pelo menos 1 caractere numérico, pelo menos 1 caractere alfabético, pelo menos 1 caractere especial, e não pode conter 3 ou mais caracteres idênticos consecutivos);
- Deve ser alterada no primeiro acesso;
- Deve ser substituída pelo menos a cada três meses (somente logins nominais atribuídos a um indivíduo) e a nova senha deve diferir das dez anteriores;
- Deve possuir um segundo fator de autenticação.

18) Medidas adequadas sejam implementadas para o rastreamento dos usuários e administradores do sistema de terceiros. Essas medidas devem incluir a geração, coleta e armazenamento de registros de acesso (login e logout) e todas as demais ações realizadas por esses acessos para os quais a integridade, a não repetibilidade e o não-repúdio devem ser garantidos. Além disso, estas informações devem ser armazenadas por um período mínimo de 2 anos;

19) Todo sistema e infraestrutura de atendimento para a TIM sejam avaliados semestralmente por meio de testes de Invasão e análise de vulnerabilidades, assim como todos os controles e ferramentas de proteção devem ser medidos e reportados para a TIM;

F. Infraestrutura de Rede de Terceiros

A infraestrutura de rede de terceiros refere-se ao conjunto de equipamentos/plataformas de Ativos TIC localizados nos escritórios do terceiro, dentro dos quais os Ativos TIC/estações de trabalho de terceiros que lidam com informações/dados de propriedade da TIM são atestados.

O terceiro, que realiza atividades em nome da TIM exclusivamente dentro de sua própria infraestrutura de rede, deve garantir que:

1) A parte da rede na qual os sistemas de informação e as estações de trabalho de terceiros são identificados e autorizados a acessar/processar os recursos da TIM, deve ser mantida isolada de outras redes, pelo menos em um nível lógico;

1) Os sistemas de informação e dados relacionados residam em redes (ou partes da rede) protegidas por um ou mais firewalls e IDS, nos quais a implementação de regras destinadas a combater tentativas de acesso não autorizado é garantida;

2) Exista um sistema para monitorar o acesso à sua parte da LAN na qual as estações de trabalho de terceiros de seus usuários que trabalham para a TIM são atestadas, a fim de detectar quaisquer anomalias ou ameaças que possam comprometer a segurança dos Recursos da TIM;

3) Caso seja necessário, apenas para fins do serviço/atividade contratada, interconectar a rede de acesso aos recursos da TIM com a rede pública (Internet), essa interconexão não pode ocorrer diretamente. Ela deve incluir mecanismos de proteção, como por exemplo, proxy ou gateway de acesso. Sob nenhuma circunstância, os recursos de rede de terceiros, responsáveis pelo acesso / processamento dos Recursos da TIM, podem ser exibidos diretamente na Internet.

G. Segurança Física para os Escritórios da TIM

1) O terceiro deve seguir os processos de segurança física da TIM.

H. Estações de Trabalho da TIM

As Estações de Trabalho fornecidas pela TIM para executar as atividades de trabalho exigidas pelo contrato/acordo. As estações de trabalho de terceiros são tipicamente equipadas com uma configuração básica padrão que pode variar dependendo da tarefa específica coberta pelo terceiro. A responsabilidade pelo uso e custódia corretos das estações de trabalho de terceiros é do terceiro, que:

1) Não deve modificar de forma independente a configuração padrão de hardware/software presente na estação de trabalho da TIM. Além disso, não deve instalar outro software além daqueles fornecidos e/ou autorizados pela TIM para a realização de tarefas de trabalho;

2) Não deve usar a estação de trabalho de maneira diferente do estabelecido no contrato firmado entre as partes;

3) Não deve impedir ou atrasar a atualização centralizada do software. Se não houver atualizações automáticas para um software específico, ele deve ser atualizado manualmente, de acordo com as instruções fornecidas pela TIM;

4) Não deve instalar software/ferramentas além daquelas fornecidas e/ou autorizadas pela TIM, incluindo:

- Software de comunicação VoIP (Voice over IP);
- Ferramentas de controle remoto (por exemplo, Log Me In etc.);

- Software destinado a criar uma rede compartilhada (como as redes virtuais peer-to-peer).

5) Deve garantir que o protetor de tela seja protegido por senha e o Personal Firewall esteja sempre ativado nas estações de trabalho da TIM usadas por seus usuários.

I. Sistemas de informação da TIM – Acesso e Uso

Os *sistemas de informações* da TIM são sistemas gerenciados/próprios da TIM nos quais as informações são acessadas pelo terceiro.

1) A TIM comunica as credenciais para acessar os seus sistemas de informações, consistindo em um UserID e uma Senha (*autenticação padrão*) ou um código de autenticação de dois fatores (*autenticação forte*), quando necessário, para a pessoa de contato terceirizada que deve garantir a confidencialidade. Essas credenciais podem ser suspensas pela TIM e, posteriormente, encerradas:

- Devido à inatividade;
- Após várias tentativas de acesso incorretas;
- Como resultado de uso ilegal ou daqueles que colocam em risco a segurança dos Recursos da TIM, a critério exclusivo da TIM;
- Na data de expiração especificada na solicitação de autorização (a menos que seja estendida);
- Caso o usuário tenha saído do terceiro ou foi avisado pela TIM para remover.

2) Todo os envolvidos no processo de gerenciamento de acessos deve garantir que a entrega de cada credencial de acesso aos respectivos usuários, seja realizado através de um procedimento adequado que associe cada usuário a uma credencial, garantindo que não seja atribuído a outros usuários mesmo em momentos diferentes. O terceiro deve garantir a confidencialidade da entrega (exemplo: uso de envelope fechado ou e-mail interno do fornecedor).

Além disso, o terceiro, sem prejuízo da presença de controles automáticos nos sistemas da TIM, deve dar instruções apropriadas aos seus usuários sobre como compor senhas fortes e de difícil adivinhação para acessar os sistemas da TIM.

O terceiro é obrigado a fazer com que seus usuários mantenham as credenciais de acesso atribuídas a eles, para tratar/acessar os Ativos TIC da TIM, a fim de garantir a absoluta confidencialidade e impedir seu compartilhamento.

3) O terceiro deve solicitar ao gestor do contrato a remoção imediata dos acessos em caso de desligamento ou transferência de função do usuário.

4) O terceiro deve realizar uma auditoria periódica e documentada, pelo menos trimestral, sobre a necessidade de manter as credenciais válidas para os usuários conectados a ele, informando imediatamente a TIM sobre a necessidade de suspender/encerrar os usuários dispositivos correspondentes a pessoal não designado ao serviço da TI, ou que, em qualquer caso não precisa mais acessar os dados da TIM. Além disso, os dispositivos de autenticação devem ser devolvidos à TIM quando não forem mais necessários para executar a atividade de trabalho (por exemplo, para uma mudança de funções) ou no final do contrato de serviço.

5) Toda automação RPA (Robotic Process Automation) desenvolvida interna ou externamente deverá seguir o processo oficial da TIM, garantindo dentre outras coisas, a gestão de acesso e perfil, o inventário e avaliação de impacto da TI da aplicação.

J. Acesso Local à Infraestrutura de Rede da TIM

O acesso direto à infraestrutura de rede da TIM, a partir de um escritório da TIM, pode ser feito conectando o dispositivo à rede Wi-Fi dedicada ao pessoal externo ou conectando o dispositivo à infraestrutura de rede TIM através de um cabo de rede e seguindo os processos de validação da TIM. No acesso local, o terceiro:

1) Não deve instalar seus próprios pontos de acesso, criar redes paralelas e configurar sua própria rede Wi-Fi para estabelecer uma conexão com a rede TIM. A conexão a serviços Wi-Fi só é permitida por meio de sua placa wireless, usando a infraestrutura Wi-Fi fornecida pela TIM;

2) Não deve usar simultaneamente múltiplos pontos LAN fornecidos pela TIM através do uso de dispositivos de rede (por exemplo: HUB, switch, roteador). O possível uso desses dispositivos pode ser permitido somente em casos limitados de emergência real e com autorização formal prévia e documentada da pessoa de contato de segurança da TIM;

3) Não deve realizar qualquer tipo de atividade que possa danificar o serviço ou a infraestrutura da rede TIM. Abaixo estão listadas, a título de exemplo, algumas atividades consideradas ilegais:

- Varredura de portas: identificação dos sistemas conectados à rede TIM;
- Varredura de vulnerabilidades: identificação de vulnerabilidades presentes nos sistemas de informação;
- Identificação de senhas: atividades destinadas a violar as credenciais definidas no sistema de informações de destino (ataque de força bruta, adivinhação de senha, captura de senha hash);
- Sniffing: atividade que consiste em interceptar, através de ferramentas apropriadas, o tráfego de rede nos segmentos da rede interna, definindo no modo promíscuo a placa de rede;
- Spoofing: uma atividade que consiste em forjar a identidade de um sistema de informações na rede, adquirindo o endereço IP associado ou seu endereço MAC;
- Descoberta de rede: atividade que permite derivar, com ferramentas específicas, a topologia de uma rede e a presença nela dos diferentes sistemas (roteador, switch, firewall, host);
- Fingerprinting do sistema operacional: atividade que permite estabelecer o tipo de sistema operacional de um sistema de informação;
- Footprinting: visa descobrir nos ativos da rede, qualquer informação que possa ser válida para posteriormente realizar um teste de invasão;
- Testes de penetração: uma atividade que consiste em avaliar a robustez dos ataques de um sistema de informação;
- Redirecionamento e modificação de tráfego: redirecionamento ou modificação de fluxos de tráfego de rede para sistemas de informação ou sistemas que não sejam os definidos pelas funções competentes.

K. Acesso Remoto à Infraestrutura de Rede da TIM

A infraestrutura de rede da TIM refere-se ao conjunto de equipamentos/plataformas de Ativos TIC que permitem conexões à parte da rede de terceiros, que devem acessar os sistemas da TIM.

1) A interconexão remota de um escritório de terceiros para a infraestrutura de rede TIM é permitida através dos seguintes tipos de conexões: Rede Privada Virtual cliente – para - Rede (VPN C2L) ou Rede Privada Virtual – para – Rede (VPN L2L).

2) O terceiro deve garantir que o canal de comunicação das conexões VPN (C2L e L2L) está equipado com proteção criptográfica dos dados em trânsito.

3) Nas conexões VPN C2L, o cliente de terceiros deve ser configurado de tal forma que:

- Encapsulamento dividido seja proibido, ou seja, não é permitida a capacidade de enviar tráfego para fora do gateway IPsec;
- Somente a interface de rede usada para a conexão VPN esteja habilitada. Se isso não for viável, um firewall pessoal deve ser configurado no cliente para bloquear tráfego de rede desnecessário e não autorizado em todas as interfaces.

4) Em conexões VPN L2L, é necessário que:

- O terceiro deve fornecer ao representante de segurança da TIM a documentação técnica específica relacionada à sua infraestrutura de rede, a fim de permitir a preparação, pelos departamentos de engenharia relevantes da TIM, de um documento técnico que especifique, em detalhes, as condições/modo da conexão (por exemplo, IP público do gateway de terminador de VPN, plano de IP/endereçamento de origem, número das estações de trabalho do terceiro conectadas em VPN, criptografia). Este documento deve ser aprovado e assinado pelo terceiro, como parte integrante e substancial do relacionamento (contrato de fornecimento, licitação, NDA, etc.) que foi assinado entre o terceiro e a TIM;
- O terceiro deve garantir que a parte da rede, na qual as estações de trabalho identificadas estão autorizadas a acessar a infraestrutura de rede da TIM, esteja isolada das outras redes, pelo menos em um nível lógico. Esta LAN também deve ser protegida por um Firewall de terceiros, o que garante a implementação das regras necessárias apenas para o fornecimento do objeto do serviço.

5) O terceiro deve formular (através de sua pessoa de contato da TI) uma solicitação para habilitar o acesso remoto à infraestrutura da Rede da TIM, de acordo com as instruções da TIM.

6) O terceiro não deve executar qualquer tipo de atividade que possa causar danos ao serviço ou infraestrutura de rede da TIM (por exemplo, varredura de portas, varredura de vulnerabilidades, identificação de senhas, sniffing, spoofing, descoberta de rede, impressão digital do sistema operacional, testes de penetração, redirecionamento e modificação de tráfego).

7) O terceiro deve realizar, internamente, atividades de verificação periódica, com o objetivo de averiguar a implementação de medidas de segurança para conexões entre sua própria rede e a rede da TIM.

L. Serviço de e-mail da TIM

Caso o terceiro receba conta(s) de acesso ao domínio de e-mail da TIM, o mesmo deve utilizá-las exclusivamente para o desempenho da atividade de trabalho decorrente das obrigações contratuais, observadas as obrigações legais vigentes e de acordo com as seguintes regras comportamentais:

1) Não deve compartilhar sua caixa de correio com outros usuários;

2) Não deve executar programas recebidos como anexos de mensagens de e-mail, baixando-os de sites ou usando mídia removível;

3) Não deve clicar em links de origens desconhecidas;

4) Não deve inserir seus dados de login clicando diretamente nos links oferecidos em um e-mail;

5) Enviar como anexo para DL_phishing e excluir imediatamente, sem abri-los, e-mails de origem desconhecida e/ou com conteúdo suspeito.

M. Serviço de Conexão à Internet da TIM

Caso o terceiro acesse a Internet por meio de conexões da TIM, ele deve utilizá-la exclusivamente para o cumprimento da atividade de trabalho decorrente das obrigações contratuais, excluindo-se a navegação de sites não relacionados a essas atividades, no cumprimento das obrigações da lei em vigor e de acordo com as seguintes regras comportamentais:

1) Usar software ou outras ferramentas para compartilhar arquivos apenas para os propósitos contratuais;

2) Não deve modificar/mascarar as configurações de rede (por exemplo: endereço IP ou endereço MAC) ou ignorar/desabilitar os dispositivos responsáveis pelo gerenciamento de segurança e comunicações de rede (por exemplo: Firewall, Proxy, Roteador);

3) Não é permitido baixar arquivos executáveis se a fonte for desconhecida;

4) Não deve usar a conexão para executar qualquer atividade que possa, mesmo que potencialmente, causar mau funcionamento, reduzir a eficiência do serviço ou causar danos de qualquer tipo (por exemplo: uso de software ponto-a-ponto);

5) A utilização da Internet é permitida apenas para fins lícitos, de acordo com as disposições legais vigentes e aplicáveis ao Código de Ética e Conduta do Grupo TIM no Brasil;

6) O acesso à Internet disponibilizado pela TIM para desenvolver sua atividade profissional, é de propriedade da Empresa e tem natureza exclusiva de ferramenta de trabalho. Assim, a utilização da Internet deve ser feita de forma correta, exclusivamente para fins profissionais, voltada somente para o acesso às informações relacionadas com as atividades de interesse da TIM;

7) Não é permitido utilizar a conexão à internet para:

- Trocar e/ou divulgar dados, áudio, vídeo, foto ou arquivos executáveis desnecessários ou incompatíveis com a atividade de trabalho;
- Contornar ou tentar desabilitar os sistemas automáticos implantados pela empresa para garantir a segurança da navegação e controle de conteúdo;
- Manifestar-se em nome e por conta da TIM, salvo autorização prévia.

8) Transferir através da Internet informações corporativas sem a prévia autorização da empresa, exceto as informações classificadas como **públicas**, já divulgadas na imprensa.

N. Continuidade de Negócios

Em relação à Continuidade de Negócios, o terceiro deve apresentar:

1) Planos de recuperação para a continuidade dos serviços prestados à TIM, para casos de ocorrência de interrupção/incidente, devendo prever, no mínimo, os casos de indisponibilidade de Ativos TIC, indisponibilidade de escritórios e indisponibilidade de pessoal;

2) Evidências de que os respectivos planos foram testados ao menos semestralmente;

3) Identificação de canais e formas de comunicação imediata de incidentes que geram interrupção dos serviços, podendo ser de acordo com o item B - 1.

O. Desenvolvimento Seguro de Aplicativos de Software

A TIM considera que a mitigação de vulnerabilidades de segurança é fundamental para todos os tipos de aplicativos adquiridos por terceiros, tanto do tipo "Buy" - software para o qual a TIM não tem acesso direto ao código - quanto do tipo "Make" - software dos quais a TIM possui a propriedade intelectual do código- fonte.

Esse conjunto de requisitos deve ser considerado aplicável a todos os tipos de software, incluindo aplicativos móveis desenvolvidos para diferentes plataformas (por exemplo: Android, iOS e Windows Phone).

Os requisitos, listados abaixo, também são divididos de acordo com o diferente nível de exposição dos sistemas de TI ou dos aplicativos de software fornecidos.

Para todos os tipos de aplicativos de software fornecidos, o terceiro deve garantir:

1) A ausência de vulnerabilidade no código, para todos os módulos de software que compõem o objeto de aplicativo de software do suprimento (mesmo aqueles que não foram desenvolvidos diretamente) e, em qualquer caso, das seguintes categorias que se referem aos padrões internacionais "OWASP" e "SANS Institute":

- OWASP Top10 / OWASP MOBILE Top10: eles representam os 10 riscos mais críticos para a segurança de aplicativos da web:

  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- SANS Top25: representam os erros mais comuns e críticos que podem levar a sérias vulnerabilidades no software, geralmente fáceis de encontrar e de explorar. Esses erros frequentemente permitem que os invasores assumam os dados ou impedem o funcionamento do software:

  https://www.sans.org/top25-software-errors/

2) As atividades de análise do código fonte tenham sido realizadas e todas as vulnerabilidades detectadas tenham sido removidas. Isto deve ocorrer por meio de processos baseados nos padrões do setor, para todos os módulos de software do aplicativo que estão sendo fornecidos (mesmo aqueles que não foram desenvolvidos diretamente). Em particular, em cada versão do software, ele deve produzir documentação adequada indicando:

- Lista de módulos / bibliotecas que compõem o software lançado;
- As ferramentas utilizadas para a análise (código estático e dinâmico);
- Número de linhas de código digitalizadas;
- Número de vulnerabilidades identificadas divididas em classes de criticidade;
- Evidência das ações de reembolso realizadas.

4) O Fornecimento à TIM das licenças para uso de todos os módulos de software que compõem o objeto aplicativo do fornecimento;

5) Caso tenham dados de cartão de créditos, os aplicativos de software devem ser desenvolvidos de acordo com o padrão PCI-DSS.

Para sistemas internos de TI e sistemas expostos na Internet, o terceiro deve garantir:

1) Quando exigido, que:

- Sejam fornecidas à TIM todas as versões e pacotes dos principais lançamentos de software;

Adicionalmente, o terceiro deve garantir que estejam disponíveis as evidências que atestam:

- A ausência de vulnerabilidade após verificações de todos os componentes de software do tipo "Make" ou "Buy" que estão sendo fornecidos (por exemplo: componentes Web Application, APP Móvel, API gateway, interfaces de IoT, componentes de back-end), incluindo estruturas de código aberto;
- A realização das análises de vulnerabilidades e testes de invasão antes da entrada em produção e, periodicamente, realizar a apresentação do report. dos resultados para a TIM e as eventuais correções aplicáveis.

2) Que sejam realizadas atividades de análise de risco, por meio de processos baseados em padrões de mercado, incluindo sistemas expostos na internet e aplicativos móveis. Estes sistemas devem atender aos seguintes requisitos, em particular:

- O licenciamento de componentes de código aberto não deve ser do tipo "Strong Copyleft";
- Os componentes não devem ser usados sem o licenciamento declarado;
- As "obrigações" subjacentes a cada licença sempre devem ser cumpridas.

P. Avaliação de Vulnerabilidade

Caso sejam identificadas vulnerabilidades técnicas durante os testes de segurança realizados pela TIM ou mesmo incidentes tecnológicos de segurança e privacidade, identificados por qualquer outro meio (imprensa, fóruns de segurança, programas de Bug Bounty, etc) na plataforma de sistemas desenvolvida pelo terceiro, esta, após informada oficialmente (por e-mail) pela TIM, deve saná-las no período sinalizado, de acordo com o previsto nas Tabelas 1 e 2- Tempo previsto de correção, onde a classificação de criticidade é indicada através do modelo CVSS (Common Vulnerability Scoring System) ou comprovar tecnicamente a não aplicabilidade para a correção. O Terceiro será responsável pelos custos da implementação das vulnerabilidades identificadas.

A TIM se reserva no direito de realizar testes de vulnerabilidade e invasão a qualquer tempo, sem necessidade de aviso prévio ao terceiro.

Para fins de validação por parte da TIM, um novo teste é realizado para comprovação das correções. Os testes são repetidos até que todas as vulnerabilidades sejam totalmente sanadas pelo terceiro.

O terceiro também deve realizar testes independentes e sanar, preventivamente, vulnerabilidades identificadas ou informadas por fabricantes, com o objetivo de manter sua infraestrutura atualizada e segura, seguindo as melhores práticas de cibersegurança mundiais e em linha com o item **P. Desenvolvimento Seguro de Aplicativos de Software**, constante neste documento.

O não cumprimento destes itens podem ser considerados como um descumprimento contratual ou omissão na prestação de serviços.

Sendo a tabela abaixo, aplicada exclusivamente para vulnerabilidades encontradas através de testes de invasão **em aplicações expostas na Internet:**

Nível	Tempo de correção/mitigação	Exceção
Crítica	Responder ao e-mail imediatamente, assim que informada. Sendo que a mitigação não pode ultrapassar o período de 4 horas.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Alta	Responder ao e-mail imediatamente, assim que informada. Sendo que a mitigação não pode ultrapassar o período de 48 horas.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Média	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar 15 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.
Baixa	Responder ao e-mail imediatamente, assim que informada. Não podendo ultrapassar os 30 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.

Tabela 1 - Tempo previsto de correção (aplicações expostas)

Sendo a tabela abaixo aplicada para as **demais aplicações**:

Nível	Tempo de correção/mitigação	Exceção

Crítica	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar o período de 15 dias.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Alta	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar o período de 30 dias.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Média	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar 45 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.
Baixa	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar os 60 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.

Tabela 2 - Tempo previsto de correção demais aplicações

Q. Serviços em Cloud (Cloud Service Provider)

Caso o terceiro seja um CSP (Cloud Service Provider) ou o serviço prestado utilize um CSP para o armazenamento das informações, a TIM solicita que:

1) O CSP (Cloud Service Provider) forneça todas as respostas ao CCM do CSA.

O Cloud Security Alliance (CSA) mantém o Registro de Segurança, Confiança e Garantia (STAR). Trata-se de um registro gratuito e acessível ao público, no qual os provedores de serviços de nuvem podem publicar suas avaliações relacionadas ao CSA. A Certificação STAR consiste em três níveis de garantia alinhados aos objetivos de controle no Cloud Controls Matrix (CCM) do CSA. O CCM abrange princípios fundamentais de segurança em 16 domínios para auxiliar os clientes na nuvem a avaliarem o risco geral de segurança de um serviço em nuvem.

2) Além do item acima, o CSP deve atender aos requisitos abaixo, de acordo com o tipo de infraestrutura utilizada IaaS, PaaS ou SaaS:

- Toda plataforma contratada deve possuir serviços de proteção anti-DDoS;
- Um termo de Non Disclosure Agreement deve ser assinado entre a TIM e o CSP sempre

que houver processamento de dados confidenciais;

- O CSP deve possuir ferramenta de Cloud Security Posture Management. (CSPM). Para monitoramento da postura de Cyber Security e compliance com regulamentações. Caso o CSP não possua solução nativa o mesmo deve prover a TIM uma lista de parceiros que tenham soluções integradas nativamente e homologada para monitorar a sua Cloud;
- Deve haver segregação de funções nas atividades administrativas das consoles e ferramentas providas pelo CSP, por exemplo: Administração de coleta de log, de IPS, de FW etc;
- Os processos de hardening e patching;

  (*) Exceto para SaaS.

- Toda atividade de autenticação de usuários de toda plataforma provida pelo CSP deve ser registrada em arquivos de log. Esses logs devem ser disponibilizados em tempo real para monitoramento da TIM através da ferramenta SIEM;
- Todos os acessos na console de gerenciamento providas pelo CSP devem ser realizados através de métodos de autenticação forte, envolvendo pelo menos dois fatores de autenticação;
- A máquina virtual/Storage dos ambientes com dados classificados como confidencialidade alta devem ser criptografados;
- Todas as máquinas virtuais devem ser catalogadas (rotulagem/marcação), usando ferramentas automatizadas, indicando função, funcionalidade e criticidade;
- Toda comunicação entre o CSP e a TIM deve ocorrer através de um canal encriptado ou exclusivo. Canais homologados pela TIM: VPN ou conexão privada;
- Todos os dados em repouso classificados como confidenciais devem ser criptografados. (máquina virtual/ armazenamento);
- Todos os backups (máquina virtual/armazenamento) devem ser criptografados no conteúdo e no canal de comunicação entre o cliente e o servidor de mídia;
- Nos processos de migração de dados de sistemas On-Premises para Cloud os dados classificados como confidenciais devem ser criptografados para transferência / cópia para o CSP. O CSP deve prover mecanismos tecnológicos para atendimento deste requisito;
- As chaves criptográficas de backup devem estar em posse e gerenciadas pela TIM;
- Contas privilegiadas de servidores Windows e Linux devem ser gerenciadas por cofre de senhas para garantir a rastreabilidade das ações;

  (*) Exceto para PaaS e SaaS.

- O CSP deve possuir ferramentas de gerenciamento de logs (*) capazes de centralizar os logs dos colaboradores, terceiros, a fim de garantir sua integridade e não repúdio e facilitar qualquer possível análise posterior. Esses logs devem ser disponibilizados para a TIM processá-los em suas ferramentas de gerenciamento de eventos de segurança para serem monitorados pela TIM em tempo real;

  Todos os logs de administração da Cloud devem ser disponibilizados tais como:

  - Identity and Access Management;
  - Compute;

- Storage;
- Networking;
- Business Applications;
- Security Functions (FW, IPS, WAF etc.).

(*) A administração deve ser de responsabilidade da função de segurança da TIM.

- Cada Ativo TIC, dispositivo ou componente de software deve sincronizar o relógio com o Network Time Protocol Server seguro;
- Toda plataforma provida pelo CSP deve ser desenvolvida seguindo as recomendações de desenvolvimento recomendada pelo OWASP. O processo de validação de código seguro deve ser garantido;
- Procedimentos de controle e rastreabilidade dos dados críticos devem ser implementados, esses logs devem, se solicitado pela TIM, ser disponibilizados em tempo real para a TIM e preservados por um período mínimo a ser definido pela TIM;
- O CSP deve garantir o envio por e-mail de notificações/alertas na presença de acesso anômalo ou suspeito feito por colaborador, fornecedor ou parceiro comercial TIM (por exemplo, acesso ao Ativo TIC e/ou console de gerenciamento feito de dispositivos ou locais não usados anteriormente). Além disso, o sistema deve permitir a configuração de alertas na presença de uso anormal de funções particularmente críticas para os negócios. Esses alarmes devem ser preferencialmente integrados e correlacionados no SIEM da TIM;
- Deve ser garantido o gerenciamento comum dos aspectos de segurança, bem como o gerenciamento de eventos de segurança decorrentes de emergências e/ou incidentes de segurança e privacidade. O CSP deve nomear um responsável pela segurança do serviço prestado e notificar a TIM;
- O CSP deve garantir que a senha para acessar seus Ativos TIC, Consoles de gerenciamento e Interface de aplicativo atenda pelo menos às seguintes características (ou critérios de robustez equivalentes):

- Parametrização de senha: Comprimento mínimo: 8 caracteres;
- A senha deve conter pelo menos um caractere alfabético maiúsculo;
- A senha deve conter pelo menos um caractere alfabético minúsculo;
- A senha deve conter pelo menos um caractere numérico;
- A senha deve conter pelo menos um caractere especial.

Expiração periódica: 90 (noventa) dias.

Troca inicial obrigatória: Ao primeiro acesso a senha temporária é desabilitada e deve ser substituída.

Controle de Sessão: A sessão do usuário deve encerrar (Logoff), após um período de 10 (dez) minutos de inatividade.

Histórico da senha: A nova senha não pode ser igual às 10 senhas anteriores.

- O CSP deve fornecer mecanismos de autenticação forte para o acesso de colaborador, fornecedor ou parceiro comercial que processam dados classificados como críticos (confidencial e/ou exclusiva), para os negócios com um alto grau de Confidencialidade e/ou Integridade;
- O CSP deve fornecer acesso utilizando autenticação mútua, com credenciais baseadas em criptografia assimétrica para todos os acessos M2M (Machine to Machine) que

processam dados classificados como críticos (confidencial e/ou exclusiva), para os negócios com um alto grau de Confidencialidade e/ou Integridade;

- Serviços em nuvem diretamente acessíveis pela internet devem possuir um método de autenticação que impeça ações maliciosas de "quebra" de senha (por exemplo: implementar tempo de suspensão do acesso ao portal após um número limitado de tentativas de autenticação com falha ou a solicitação para verificar um código Captcha);
- Qualquer usuário, seja colaborador, fornecedor ou parceiro comercial quando gerenciado pelo CSP deve:
  - Verificar constantemente os usuários inativos para suspensão imediata (exceto usuários previamente autorizados para fins de gerenciamento técnico para os quais uma autorização foi concedida);
  - Conservar as requisições de cancelamento até o final do contrato com a TIM.
- O CSP deve garantir a adoção de procedimentos adequados (por exemplo, backup, replicação etc.) que garantam um ponto de recuperação (RPO) de até 01 (um) dia de informações/dados da TIM, em caso de perda de dados em Ativos TIC. As informações/dados devem ser mantidas apenas durante o período contratual, quando não, devem ser excluídos;

  Obs.: O RPO é definido de acordo com a solução.
- O CSP deve garantir que, em caso de mau funcionamento ou incidente em seus sistemas de TI, sejam adotados procedimentos operacionais específicos para a execução das atividades de restauração, que devem fornecer tempos de implementação alinhados com os SLAs contratados;
- As chaves criptográficas nunca devem ser armazenadas/transmitidas de forma clara. A propriedade e a gerência das chaves criptográficas são de responsabilidade da TIM;
- O CSP deve garantir que as atualizações do sistema operacional, middleware e software de aplicativo necessárias para corrigir defeitos e prevenir vulnerabilidades sejam instaladas em tempo hábil, de acordo com os padrões internacionais (por exemplo, OWASP, CERT). O CSP deve garantir testes adequados a fim de que a atualização não cause impacto na solução;

  (*) Exceto para IaaS.
- Os logs gerados e coletados pela TIM devem possuir mecanismos que garantam autenticidade, imutabilidade e a correta configuração de data e hora (sincronizado com uma fonte de tempo oficial do Brasil);
- O CSP deve garantir que qualquer software instalado seja licenciado legalmente;
- O acesso aos registros de atividades de colaborador, terceiro, inclusive usuário M2M que trocam dados da TIM deve ser garantido, com a possibilidade de serem enviados às infraestruturas da TIM. Acesso aos registros dos usuários do CSP também deve ser garantido, nos casos em que são realizadas atividades de gerenciamento dos Ativos TIC da TIM;
- Todos os acessos e operações de leitura, gravação, modificação e exclusão de dados críticos devem ser rastreados nos sistemas de informações do CSP (por exemplo, dados classificados como críticos para os negócios com um alto grau de Confidencialidade e/ou Integridade, configurações de administração, informações privilegiadas) realizado colaborador, fornecedor ou parceiro comercial da TIM, inclusive usuários M2M e funcionários do CSP, nos casos em que são realizadas atividades de gerenciamento Ativo TIM. Os logs devem permitir identificar:

- O sistema de destino e qualquer aplicativo acessado;
- A referência do usuário que executou as atividades;
- Qualquer detalhe dos recursos ou parâmetros de acesso (por exemplo, endereço IP do cliente);
- As referências de tempo para a execução das atividades individuais;
- Uma indicação dos tipos e características das atividades realizadas.

- Além do requisito **CSA IAM-08**, o CSP deve adotar uma solução técnica ou processual que permita o rastreamento inequívoca do colaborador, fornecedor ou parceiro comercial que utiliza logins sistêmicos/usuários técnicos (por exemplo, usuários root).

  O uso desses utilitários deve ser limitado em casos de necessidade operacional real e somente pelo tempo estritamente necessário, sempre com autorização da TIM;

- O CSP deve cumprir a cláusula contratual do Direito de Auditoria que permite à TIM realizar atividades de controle processual e técnico (por exemplo, Avaliação de Segurança), para verificar a presença e a eficácia das contramedidas de segurança que foram declaradas;

- Em caso de incidentes de segurança e privacidade ou potencial tentativa de ataque cibernético, o CSP deve realizar análise forense e reportar a TIM em um tempo máximo de até 01 (uma) semana sobre as vulnerabilidades exploradas e os dados comprometidos;

- A política, o controle da infraestrutura para os componentes de infraestrutura e os pré-requisitos de arquitetura adotados no datacenter on-premises devem ser garantidos como valores mínimos na nuvem;

- Todo ambiente exposto na Internet deve ser protegido por ferramentas de NGX Firewall, IPS e para aplicações Web deve ser protegido por WAF;

- As plataformas de segurança de NGX Firewall, microssegmentação, IPS e WAF deve ser administrado pela TIM.

  Quando aplicável tecnicamente a TIM se reserva o direito de utilizar a sua ferramenta de microssegmentação para garantir o controle de tráfego dos seus ativos e a proteção de ataques.

  A TIM se reserva o direito de utilizar os appliances de segurança de sua escolha caso o CSP não possua as soluções ou as soluções providas pelo CSP não atendam aos requisitos mínimos de segurança e governança requeridos;

  (*) Exceto para as aplicações em SaaS.

- Todos os pontos de Interconexão de tráfego mesmo que interno devem ser protegidos por Firewall e IPS para filtragem de pacotes e tráfegos anômalos entre essas redes;

- Deve-se monitorar em tempo real os eventos e a correlação de informações por meio do SIEM (*), eventos relacionados a:

- Anomalias de tráfego;
- Eventos de segurança gerados por elementos de proteção (FW, IPS, Antivírus, autenticações etc.);
- Eventos de acesso de usuários e clientes;
- Eventos e atividades administrativas nas consoles.

  (*) A administração deve ser de responsabilidade da função de segurança da TIM.

- As políticas de configuração de equipamentos de segurança devem ser implementadas e documentadas seguindo os devidos fluxos de aprovações e logs de alterações de configurações;

  (*) A administração deve ser responsável pela função de segurança da TIM.

- As políticas e controles de segurança para os componentes de sistema/Ativos TIC adotados no datacenter local devem ser garantidos como medida mínima também na nuvem;

- Os sistemas devem estar segregados dos ambientes de produção, FQA e Desenvolvimento;

- Os acessos ao sistema operacional são realizados através de Gateway de sessão. As comunicações entre os componentes de sistema devem ser criptografadas;

  (*) Quando aplicável, a TIM se reserva o direito de utilizar o seu próprio Gateway de sessão.

- É necessário realizar o monitoramento em tempo real dos eventos para detectar ataques cibernéticos e um processo de resposta a incidentes, no caso de um incidente de segurança e privacidade;

- Em ambientes em nuvem, os ambientes devem obedecer às regras de segregação de ambiente definidas para o datacenter (micro segmentação), usando os recursos fornecidos pelo Cloud Service Provider (CSP). Adicionalmente a TIM se reserva o direito de utilizar a sua ferramenta de microssegmentação para garantir o controle de tráfego dos seus ativos e a visibilidade de ataques.

  A segregação dos aplicativos deve ser garantida usando o pool de recursos (VM, armazenamento de dados etc.) separados uns dos outros, respeitando o conceito de segregação horizontal e vertical de aplicativos;

- O movimento de dados horizontal (Leste-Oeste) deve ser regulado através do uso de infraestruturas que garantam a microssegmentação.

  Quando aplicável tecnicamente a TIM se reserva o direito de utilizar a sua ferramenta de microssegmentação para garantir o controle de tráfego dos seus ativos e a visibilidade de ataques;

- Todos os acessos na console de gerenciamento providas pelo CSP devem ser realizados através de métodos de autenticação forte, envolvendo pelo menos dois fatores de autenticação;

- O armazenamento/bancos de dados de ambientes com dados classificados com confidencialidade alta devem ser criptografados;

- As verificações de vulnerabilidade de Ativos TIC devem ser realizadas regularmente através de análise e/ou exploração de vulnerabilidade;

- Toda aplicação WEB e APIs devem ser disponibilizadas através de canais de comunicação criptografados através do uso de protocolos seguros e protegidas por solução de Web Application Firewall (WAF), por exemplo: SSL/TLS;

- Os servidores web que hospedam aplicações com acesso direto da Internet deve ser segregada dos servidores web que disponibilizam somente serviços as redes privadas da TIM.

  Os serviços web acessados via internet não devem ser acessados de forma direta, mas através de solução de Web Application Firewall e balanceadores de carga;

- Todo processo de autenticação deve ser criptografado;
- No caso de serviços em nuvem diretamente acessíveis na Internet (por exemplo, com navegador da Web sem VPN), o rastreamento de acesso e atividade deve incluir:
  - IP público do navegador e porta de origem;
  - indicações de tempo para o início e o fim da sessão de acesso;
  - Identificação da conta que efetuou login;
  - Identificação das atividades realizadas, em termos de URL das páginas navegadas, dos atributos sendo carregados, das funções relativas ativadas, das indicações de tempo correspondentes.

  Esses rastreamentos devem ser mantidos pelo CSP por um período mínimo de 6 meses com o objetivo de detectar incidentes ou comportamento anômalo, fraude ou abuso do serviço;
- Todas as consoles de administração ou gerencia do CSP devem ser criptografados;
- Deve ser prevista alta disponibilidade do ambiente, de forma a garantir menor impacto aos serviços/Ativos TIC TIM;
- Deve ser prevista a definição do DRP (Disater Recovery Plan), em caso de ocorrer um incidente nível desastre que impacte o ambiente da nuvem previsto na contratação. Os Ativos TIC previstos para DRP devem ser definidos pela TIM;
- A comunicação entre redes virtuais de diferentes ambientes/contextos deve ser autorizada, segundo o processo vigente na TIM. Exemplo: VPN;
- Todos os acessos realizados nas consoles providas pelo CSP devem ter sua rastreabilidade garantida por meio de logs, obedecendo os requisitos mínimos de rastreabilidade. Tais logs devem ser disponibilizados a TIM para a TIM processá-los em suas ferramentas de gerenciamento de eventos de segurança para serem monitorados pela TIM em tempo real;
- É desejável que o CSP possua certificações de mercado, como por exemplo: Atestado CSA-STAR, Certificação CSA-STAR, Autoavaliação da CSA-STAR, ISO 20000-1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, SOC, WCAG, PCI DSS, SOX (ISAE 3402 - Tipo 01 e 02), NIST 800-171, NIST CSF, União Europeia-US Privacy Shield, Regulamentação da SEC SCI, GDPR, LGPD, HIPAA/ALTA TECNOLOGIA). Essas certificações devem ser apresentadas à TIM;

ANEXO V

PRÁTICAS DE ANTIFRAUDE

Este anexo será elaborado antes da assinatura do Contrato de comum acordo pelas Partes.

ANEXO VI

INTERCEPTAÇÃO LEGAL

Este anexo será elaborado antes da assinatura do Contrato de comum acordo pelas Partes.