1. Objeto

1.1. O objetivo desse apêndice técnico de segurança da informação (Anexo SI) é estabelecer diretrizes e obrigações referentes à Segurança da Informação para o monitoramento contínuo dos endereços IPs pertencentes e registrados em nome da American Tower do Brasil - Comunicação Multimídia Ltda. ("ATCM") e temporariamente cedidos à Contratante, visando proteger todos os dados, sistemas, comunicações e documentos trocados, armazenados ou processados entre as partes durante a vigência do contrato. Além disso tem o intuito de identificar vulnerabilidades à segurança cibernética que possam comprometer a integridade, confidencialidade, disponibilidade dos ativos de informação ou denegrir direta ou indiretamente o nome da ATCM.

1.2. Este Apêndice Técnico de Segurança da Informação ("Anexo SI") é celebrado em observância à legislação brasileira aplicável à segurança da informação, à proteção de dados pessoais e à governança da internet, em especial à Lei nº 12.965/2014 (Marco Civil da Internet), à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), ao Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética), bem como às normas e princípios gerais de direito civil previstos na Lei nº 10.406/2002 (Código Civil).

1.3. Considerando que a ATCM atua como operadora de infraestrutura de telecomunicações e detentora formal de recursos de endereçamento IP, sem ingerência sobre aplicações, conteúdos, dados, tráfego ou usuários finais, e que a responsabilidade jurídica deve observar a conduta, o controle e a camada de atuação do agente, nos termos do artigo 18 da Lei nº 12.965/2014, as disposições deste Anexo SI têm por finalidade estabelecer diretrizes técnicas e jurídicas claras quanto à segurança da informação, à prevenção de incidentes e à correta alocação de responsabilidades entre as Partes.

1.4. Este Anexo SI também reflete o dever legal de adoção de medidas técnicas e administrativas aptas a proteger dados, sistemas e infraestruturas críticas, nos termos do artigo 46 da Lei nº 13.709/2018 e das diretrizes nacionais de segurança cibernética, não constituindo tais medidas exercício de ingerência operacional, mas sim cumprimento de obrigação legal voltada à preservação da estabilidade, funcionalidade e segurança das redes, conforme o artigo 3º, inciso IV, da Lei nº 12.965/2014.

1.5. As Partes reconhecem, ainda, que a cooperação com autoridades administrativas ou judiciais, quando legalmente exigida, será realizada nos estritos limites da legislação aplicável, nos termos do artigo 10 da Lei nº 12.965/2014, sem que tal cooperação implique assunção de responsabilidade por atos, conteúdos ou condutas atribuíveis à outra Parte.

1.6. Dessa forma, o presente Anexo SI deve ser interpretado à luz dos princípios da boa-fé objetiva, da autonomia privada, da prevenção de danos e da responsabilização conforme a atuação efetiva do agente, nos termos dos artigos 421-A e 422 do Código Civil, constituindo instrumento de governança, compliance e mitigação de riscos legais, regulatórios, operacionais e reputacionais.

2. Definições

2.1. Contratante: Signatária do Contrato ao qual este Anexo SO está vinculado

2.2. Contratada: American Tower Comunicação Multimídia ("ATCM")

3. Princípios de Segurança

3.1. As Partes comprometem-se a adotar melhores práticas nacionais e internacionais que assegurem: confidencialidade, integridade, disponibilidade e legalidade, observando, exemplificadamente, as seguintes leis:

a) Lei Geral de Proteção de Dados (Lei no13.709/2018 – LGPD), especialmente os artigos 6º e 46;

b) Lei nº 12.965/2014 – Marco Civil da Internet;

c) Decreto nº 10.222/2020 – Estratégia Nacional de Segurança Cibernética;

4. Disposições gerais

4.1. As atividades proibidas listadas a seguir não constituem um rol exaustivo. A ATCM reserva-se o direito de adotar as medidas cabíveis para remediar qualquer conduta que considere violar este Anexo SI ou que possa ser prejudicial à rede da ATCM ou a outros usuários.

4.2. Os usuários não devem usar os serviços para transmitir, distribuir ou armazenar material de modo que:

a) viole qualquer lei, estatuto, regulamento ou norma aplicável;

b) possa afetar adversamente os Serviços ou outros usuários;

c) exponha a ATCM a responsabilidade civil ou criminal;

d) viole, infrinja ou se aproprie indevidamente de direitos de terceiros, tais como direitos autorais, patentes, marcas, segredos comerciais, ou direitos de publicidade e privacidade;

e) configure ato que a ATCM julgue inapropriado, obsceno, indecente, difamatório, libeloso, delituoso, ameaçador, abusivo, odioso ou excessivamente violento;

f) transmita, distribua ou armazene material que possa ser prejudicial ou interferir nos Serviços, na rede da ATCM ou nas redes, sistemas, serviços ou sites de terceiros.

4.3 Os usuários estão proibidos de facilitar qualquer violação deste Anexo SI.

4.4 A Contratante reconhece que eventuais sanções, penalidades, autuações, multas ou demais medidas impostas por autoridades administrativas, regulatórias ou judiciais, inclusive pela Agência Nacional de Telecomunicações – ANATEL, decorrentes do uso dos endereços IP objeto deste contrato, observarão o princípio da responsabilização conforme a conduta e o controle do agente, nos termos dos artigos 186 e 927 do Código Civil e do artigo 18 da Lei nº 12.965/2014 (Marco Civil da Internet), não sendo imputáveis à ATCM quando inexistente participação ou ingerência nos atos praticados.

5 Atividades ilegais

5.1 Os usuários não devem usar os serviços de forma a constituir atividades ilegais, incluindo, mas não se limitando a: ameaças ilegais, esquemas de marketing multinível, invasão de privacidade, fraude com cartão de crédito, extorsão (racketeering), difamação, calúnia, pornografia infantil e violações da Child Protection Act de 1984, ou qualquer outra lei aplicável.

6 Propriedade intelectual

6.1 O material acessível pelos serviços pode estar protegido por direitos de privacidade, publicidade ou outros direitos pessoais, bem como por direitos de propriedade intelectual, incluindo direitos autorais, patentes, marcas e segredos comerciais. Os usuários não devem usar os serviços de modo a infringir, diluir, apropriar-se indevidamente ou violar quaisquer desses direitos.

7 Conteúdo fraudulento ou enganoso

7.1 Os usuários não devem usar os serviços para transmitir ou distribuir material que contenha ofertas fraudulentas de bens ou serviços, ou qualquer material publicitário/promocional com declarações,

alegações ou representações falsas, enganosas ou imprecisas. Além disso, é proibido o envio de dados falsos ou imprecisos em qualquer formulário de pedido ou contrato.

8 Ações inadequadas

8.1 Os usuários não devem usar os serviços para realizar atividades que sejam prejudiciais ou interfiram nos serviços, na rede da ATCM ou nas redes, sistemas, serviços ou sites de terceiros. É vedado praticar ações que assediem ou impeçam o uso dos serviços por outros usuários (por exemplo, ataques de sequência numérica sincronizada). Adicionalmente, os usuários não devem usar os serviços para:

a) evitar pagamento por qualquer meio ou dispositivo;

b) acessar conta ou serviços da ATCM após encerramento de sua própria conta;

c) praticar phishing.

8.2 Também é proibido realizar atividades que prejudiquem a capacidade de terceiros de acessar ou usar os serviços ou a internet.

9 Violação de segurança e obrigações

9.1 Os usuários estão proibidos de violar ou tentar violar a segurança dos serviços ou dos computadores, contas ou redes de terceiros, incluindo, mas não se limitando a burlar autenticação ou segurança de qualquer host, rede ou conta. Os usuários não devem usar os serviços para causar brechas de segurança ou interrupções na comunicação ou conectividade à Internet.

9.2 Brechas de segurança incluem, entre outras, acesso não autorizado a dados, contas ou sistemas, login em servidores ou contas sem permissão expressa e ataques de negação de serviço. Interrupções incluem varredura de portas, flood pings, e-mail bombing, spoofing de pacotes, IP spoofing e informações de roteamento forjadas.

9.3 O usuário deve manter seu software nos servidores da ATCM atualizado e com os patches de segurança mais recentes.

9.4 O eventual atendimento, pela ATCM, a ordens judiciais, requisições administrativas ou solicitações de autoridades competentes, nos limites do artigo 10 da Lei nº 12.965/2014 (Marco Civil da Internet), não implicará assunção de responsabilidade pelos atos investigados, restringindo-se à cooperação legalmente exigida, permanecendo a Contratante como única responsável pelos registros, dados e informações sob sua gestão, nos termos dos artigos 13 e 15 da referida lei.

10 Obrigações da Contratada

10.1 Alocação do IP: Os endereços IP pertencem e são registrados em nome da ATCM, que poderá eventualmente solicitar a subdesignação nos órgãos competentes para a Contratante.

10.2 O usuário não detém qualquer direito de propriedade ou transferência sobre eles.

10.3 Para fins de correta alocação de responsabilidades, as Partes reconhecem que a ATCM atua exclusivamente na camada de infraestrutura e endereçamento de rede, não exercendo controle sobre aplicações, conteúdos, dados, tráfego, usuários finais ou finalidades atribuídas ao uso dos endereços IP, nos termos do artigo 18 da Lei nº 12.965/2014 (Marco Civil da Internet). Qualquer obrigação legal ou regulatória relacionada à camada lógica ou de aplicação será de responsabilidade exclusiva da Contratante.

11 Relatório técnico de Vulnerabilidades

11.1 A ATCM enviará os relatórios técnicos com as vulnerabilidades identificadas que precisam ser corrigidas, não sendo responsabilidade da ATCM a ação técnica para resolução dessas vulnerabilidades.

11.2 Em casos em que a vulnerabilidade identificada comprometa direta ou

indiretamente a segurança dos ativos da ATCM, sua imagem ou de outros clientes, a ATCM tomará ações que bloqueiam o ativo vulnerável após o 2º relatório técnico enviado com a reincidência da vulnerabilidade informado que a ação de bloqueio será feita pelos especialistas da ATCM.

11.3 A CONTRATADA compromete-se a manter confidencialidade sobre as informações coletadas e se exime da responsabilidade de armazenamento de log e/ou informação do usuário final responsável pela má utilização dos blocos de acesso públicos, de qualquer penalidade ou violação do uso desses IPs no âmbito da internet mundial, sendo essa de total responsabilidade do Contratante.

11.4 Sem prejuízo das disposições anteriores, as Partes reconhecem que a adoção de medidas preventivas e corretivas destinadas à proteção da segurança da informação, da estabilidade da rede e da continuidade dos serviços constitui dever legal do agente que opera a infraestrutura crítica, nos termos do artigo 3º, inciso IV, da Lei nº 12.965/2014 (Marco Civil da Internet), do artigo 46 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e do Decreto nº 10.222/2020. Assim, a implementação de ações técnicas de mitigação pela ATCM, quando motivadas por risco relevante ou iminente, não será caracterizada como falha na prestação do serviço ou descumprimento contratual.

12 Obrigações da Contratante

12.1 Autorização e Consentimento

A Contratante expressamente autoriza a ATCM a realizar, de forma periódica ou sob demanda, escaneamentos técnicos nos IPs públicos informados, utilizando ferramentas automatizadas e metodologias reconhecidas pelo mercado, com base em boas práticas como OWASP, NIST e ISO/IEC 27001.

12.1.1 Para os casos em que a subdesignação não seja tecnicamente possível de ser feita nos órgãos competentes a contratante assinará um termo se responsabilizando pelo Bloco de IP contratado durante o período do contrato.

12.1.2 A autorização concedida pela Contratante para a realização de escaneamentos e testes técnicos de segurança será interpretada conforme os princípios da boa-fé objetiva e da prevenção de danos, previstos no artigo 422 do Código Civil, e visa exclusivamente ao cumprimento de deveres legais de segurança da informação, nos termos do artigo 46 da Lei nº 13.709/2018 (LGPD), não gerando qualquer direito de ingerência da ATCM sobre os sistemas internos da Contratante.

13 Tratamento de Vulnerabilidades

13.1 A Contratante é responsável por corrigir as vulnerabilidades identificadas e reportadas pela ATCM nos prazos definidos na tabela abaixo, sob pena de responsabilização por incidentes decorrentes da negligência:

Nível de severidade	Prazo de correção	Descrição do risco
Muito Crítico -6	Até [7 dias]	Condição totalmente inaceitável quando medidas
Crítico -5	Até [30 dias]	Pessoas mal-intencionadas podem facilmente obter o
Alto -4	Até [40 dias]	Pessoas mal-intencionadas podem obter o controle do
Médio -3	Até [50 dias]	Documentos expostos na internet que contenham

13.2 As Partes reconhecem que a legislação e regulamentação aplicáveis à segurança da informação, proteção de dados e telecomunicações poderão ser alteradas ao longo da vigência contratual, obrigando-se a Contratante a promover, às suas expensas, as adequações técnicas e operacionais necessárias ao cumprimento de novas exigências legais ou regulatórias que impactem o uso dos serviços, nos termos do artigo 421-A do Código Civil.