CONTRATO DE PATROCÍNIO

Os abaixo identificados celebram entre si o presente Instrumento Particular de Contrato de Patrocínio (o "**Contrato**"):

TATA CONSULTANCY SERVICES DO BRASIL LTDA, pessoa jurídica de direito privado, com sede na Rua Alameda Madeira, nº 328 – 13º andar – Alphaville – Barueri SP – CEP 06454-010, inscrita no CNPJ/MF sob n° 04.266.331/0001-29, neste ato representada nos termos de seus instrumentos societários em vigor, doravante denominada simplesmente "**PATROCINADORA**" ou "**TCS**",

E, de outro lado,

INSTITUTO NÃO ME ESQUEÇAS, com sede na Rua Paes Leme, 569 – Jardim América – Londrina PR- CEP 86010-610, inscrita no CNPJ/MF sob o **n.º 27.943.469/0001-10**, representada neste ato nos termos de seus instrumentos societários em vigor, doravante denominado **"PATROCINADA**";

PATROCINADA e **PATROCINADORA** serão individualmente denominadas como "Parte" e coletivamente como "Partes".

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente **Contrato** tem por objeto o patrocínio, pela **PATROCINADORA** à **PATROCINADA**, para viabilizar a realização do **Projeto NeuroLúdico,** aprovado pelo **Conselho Municipal dos Direitos da Pessoa Idosa.**

1.2. A presente contratação não pressupõe qualquer direito de exclusividade entre as Partes, razão pela qual a **PATROCINADORA** poderá, a seu exclusivo critério, realizar patrocínios a outros projetos e eventos que tenha interesse, o que também se aplica à **PATROCINADA**, desde que não colida com os interesses da **PATROCINADORA**.

CLÁUSULA SEGUNDA – DAS CONTRAPARTIDAS À PATROCINADORA

2.1. Em razão do patrocínio objeto do presente **Contrato**, a **PATROCINADORA** terá direito às seguintes contrapartidas:

a) Divulgação da logomarca do patrocinador no site institucional;
b) 12 postagens nas redes sociais do Instituto;
c) Menção em 6 newsletters;
d) Menção em 2 releases;

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA PATROCINADA

3.2. Sem prejuízo das demais obrigações dispostas neste **Contrato**, a **PATROCINADA** se compromete a:

a) Executar o projeto conforme aprovação pelo órgão incentivador, responsabilizando-se junto às autoridades governamentais pelo cumprimento de todas as obrigações atribuídas em razão do patrocínio, principalmente no que se refere à prestação de contas dos recursos captados para o desenvolvimento do projeto;

b) Inserir a logomarca da **PATROCINADORA**, respeitando as diretrizes do seu Manual de Marca, submetendo todo material antes da sua efetiva confecção à prévia aprovação da **PATROCINADORA;**

c) Responsabilizar-se civil e/ou criminalmente por qualquer dano e/ou prejuízo decorrente da execução do projeto, causado à **PATROCINADORA** ou terceiro, por si ou terceiros contratados pela **PATROCINADA**;

d) Autorizar que a **PATROCINADORA** utilize imagens do projeto, fornecidas pela **PATROCINADA**, para divulgação de seus patrocínios em ações institucionais, bem como as imagens produzidas pela própria **PATROCINADORA** desde que no âmbito do projeto;

e) Treinar e supervisionar os profissionais envolvidos na execução do projeto, não expondo estes profissionais a condições de trabalho degradantes ou análogas de escravo, bem como não utilizar mão-de-obra infantil, exceto na condição de aprendiz, nos termos da lei;

f) Providenciar a imediata substituição de colaborador que tenha se comportado de forma imprópria e incompatível com as normas gerais de conduta previstas neste **Contrato**, de modo prejudicial ao regular andamento do projeto, sem quaisquer ônus para a **PATROCINADORA**;

g) Empregar na realização de suas atividades pessoal habilitado, assumindo inteira responsabilidade pelo pagamento de todos os direitos e encargos trabalhistas e previdenciários, sujeitando-se a exibir os documentos respectivos sempre que solicitados pela **PATROCINADORA**, devendo observar a legislação aplicável quanto aos seus aspectos trabalhistas, previdenciários, tributários e normas de segurança, dentre outros;

h) Fornecer e exigir de todos os Colaboradores e pessoas beneficiadas pelo projeto, sempre que aplicável, o uso do equipamento de segurança pessoal, incluindo todo material de proteção, de acordo com a legislação emanada dos órgãos competentes;

i) Prestar à **PATROCINADORA** todos os dados e informações relacionadas à presente contratação, garantindo total transparência em relação a todas as operações realizadas no projeto e com base neste **Contrato**;

j) Responsabilizar-se, exclusivamente, por providenciar as licenças que se fizerem necessárias para o desempenho pleno de suas atividades, inclusive obter todas as autorizações e licenças de uso de imagem junto aos beneficiados pelo projeto, de forma que a **PATROCINADORA** não será, em nenhuma hipótese, responsável por quaisquer reclamações ou reinvindicações de terceiros relacionadas ao tema;

k) Comunicar a **PATROCINADORA**, imediatamente e por escrito, acerca de quaisquer dificuldades que possam prejudicar o projeto, bem como comunicar de imediato a **PATROCINADORA** sobre o recebimento, ainda que por preposto ou qualquer terceiro, de toda e qualquer citação, intimação ou notificação, judicial ou extrajudicial direta ou indiretamente relacionada ao projeto, que tenha a potencialidade de afetar a imagem e/ou a reputação da **PATROCINADORA;**

l) Entregar à **PATROCINADORA** qualquer alteração havida em seus documentos societários constitutivos, informar, também, sobre situações e quaisquer alterações que tenham

significativo impacto em seu passivo, bem como apresentar, quando solicitado pela **PATROCINADORA**, os balanços, balancetes, outras demonstrações financeiras e quaisquer outros documentos cadastrais e econômico-financeiros da **PATROCINADA**;

m) Zelar pelo bom nome e pela boa reputação da **PATROCINADORA**, bem como abster-se, por si e por qualquer de seus colaboradores e prepostos, de praticar qualquer ato ou omissão que prejudique, efetiva ou potencialmente, a imagem e/ou a reputação da **PATROCINADORA** e de sua marca.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA PATROCINADORA

4.1. É obrigação da **PATROCINADORA** efetuar o pagamento do patrocínio na forma estabelecida na Cláusula Sexta do presente **Contrato**;

CLÁUSULA QUINTA – DO PRAZO

5.1. O presente **Contrato** entrará em vigor na data da sua assinatura e terminará com a conclusão do projeto.

CLÁUSULA SEXTA – DO VALOR DO PATROCÍNIO E CONDIÇÕES DE PAGAMENTO

6.1. Em virtude do presente **Contrato**, a **PATROCINADORA** se compromete a destinar ao projeto o valor de R$ 188.644,00 (Cento e oitenta e oito mil, seiscentos e quarenta e quatro reais) por meio de boleto bancário que será gerado na página oficial do Fundo Municipal do Idoso do Município de Londrina.

6.2. No valor antes mencionado, já estão inclusos todos os tributos que possam incidir, direta ou indiretamente, sobre o patrocínio objeto deste **Contrato**.

CLÁUSULA SÉTIMA – DA CONFIDENCIALIDADE

7.1. Todas as informações fornecidas pelas Partes sob este **Contrato** serão consideradas como de propriedade exclusiva e de natureza confidencial, e não deverão ser reveladas ou divulgadas a qualquer terceiro, sem o seu prévio e expresso consentimento.

7.2. As Partes compreendem e concordam que nenhuma informação, documento e/ou qualquer dado disponibilizado pela outra Parte está sendo vendido ou licenciado à Parte contrária, e que todas as informações, documentos e quaisquer dados a serem disponibilizados por uma Parte à outra, destinam se única e exclusivamente para que a Parte realize o projeto/evento, de acordo com as condições ajustadas neste **Contrato**.

7.3. No ato do término ou rescisão deste **Contrato**, por qualquer motivo, as Partes se comprometem a devolver ou inutilizar as informações confidenciais recebidas, sem reter quaisquer cópias, exceto se a sua manutenção se destine ao cumprimento de obrigações previstas na legislação em vigor.

7.4. As obrigações assumidas nos termos desta Cláusula permanecerão válidas e exigíveis durante a vigência do presente **Contrato**, bemcomo pelo prazo de 02 (dois) anos contados do término ou rescisão deste **Contrato**, por qualquer motivo.

7.5. A infração desta cláusula por qualquer das Partes dará ensejo à Parte lesada de resolver o presente **Contrato** de pleno direito, bem como de pleitear as perdas e danos devidamente comprovados.

CLÁUSULA OITAVA – DA PROTEÇÃO DE DADOS PESSOAIS

8.1. As Partes se comprometem a tratar os dados pessoais envolvidos na confecção e necessários à execução do presente **Contrato**, única e exclusivamente para cumprir com a finalidade a que se destinam e em respeito a toda a legislação aplicável sobre segurança da informação, privacidade e proteção de dados, inclusive, mas não se limitando à Lei Geral de Proteção de Dados (Lei Federal n. 13.709/2018 e suas eventuais alterações supervenientes) e desde já, declaram-se plenamente responsáveis por qualquer vazamento ou violação ilegal que derem causa, eximindo a Parte contrária de eventual responsabilidade solidária quanto aos riscos da coleta, tratamento, utilização, compartilhamento e descarte dos dados coletados e fornecidos pela outra Parte, seus clientes e partes relacionadas), sob pena de rescisão contratual, sem prejuízo de perdas e danos.

8.2. Cada Parte deverá cumprir as obrigações que lhe são aplicáveis nos termos da legislação que trata sobre a proteção de dados, especialmente no que diz respeito à coleta, tratamento, processamento, utilização, compartilhamento e descarte de dados pessoais.

8.3. Após o encerramento deste **Contrato**, os dados coletados serão descartados e cada Parte se responsabilizará por qualquer vazamento e mau uso dessas informações.

8.4. As obrigações assumidas nesta Cláusula deverão sobreviver ao término ou à resolução deste **Contrato**, independentemente do motivo, pelo prazo legal aplicável.

CLÁUSULA NONA – DA INEXISTÊNCIA DE VÍNCULO EMPREGATÍCIO

9.1. Fica expressamente estabelecido que este **Contrato** não implica na formação de qualquer relação ou vínculo empregatício entre as Partes ou seus colaboradores, permanecendo a Parte contrária livre de qualquer responsabilidade ou obrigação trabalhista ou previdenciária, direta ou indireta.

9.2. As Partes assumem integral e exclusiva responsabilidade quanto ao cumprimento das exigências legais para o desenvolvimento de suas próprias atividades, objeto deste **Contrato**, se obrigando a assumir as relações trabalhistas do pessoal que possa vir a empregar e/ou utilizar no desenvolvimento de suas obrigações, responsabilizando-se pelas relações jurídicas com esses profissionais nos termos da legislação civil ou trabalhista que lhes for aplicável, responsabilizando-se pelo pagamento de todas as despesas, tributos e demais encargos, sem nenhuma exceção, decorrentes do exercício de sua atividade.

9.2.1. A **PATROCINADA** deverá manter a **PATROCINADORA** indene de todas e quaisquer perdas e danos que decorram ou possam decorrer de qualquer ação ou omissão atribuível à **PATROCINADA**, incluindo, sem limitação, perdas e danos relacionados a obrigações de natureza tributária, civil, trabalhista, previdenciária, securitária ou outras relativas a toda e qualquer pessoa envolvida em atividades relacionadas à prestação dos serviços.

9.3. A **PATROCINADA** deverá responsabilizar-se integral e exclusivamente por todos os atos de seus empregados envolvidos no projeto, preservando a **PATROCINADORA** de toda e qualquer ação ou procedimento judicial ou extrajudicial que venham a ser promovidos por estes e/ou terceiros.

9.4. Caso qualquer processo seja ajuizado em face da **PATROCINADORA** por qualquer pessoa

envolvida pela **PATROCINADA** e/ou subcontratados desta última em atividades relacionadas à prestação dos serviços, a **PATROCINADA** deverá requerer a sua integração à lide. A **PATROCINADA** compromete-se, ainda, na hipótese de a **PATROCINADORA** não ser excluída da lide, a ressarcir à **PATROCINADORA** prontamente todos e quaisquer custos ou despesas que venham a ser comprovadamente incorridos pela **PATROCINADORA** com tal processo, incluindo, sem limitação, custas processuais, ônus de sucumbência, honorários de peritos e assistentes judiciais, e honorários advocatícios.

9.4.1. Em não sendo acatada a exclusão da **PATROCINADORA** da lide, deverá a **PATROCINADA** resguardar e indenizar a **PATROCINADORA** de qualquer condenação, perdas e danos, custas processuais e honorários advocatícios que a **PATROCINADORA** tenha que contratar para a defesa de seus interesses em até 05 (cinco) dias do recebimento da respectiva solicitação neste sentido, sob pena de multa não cominatória em 30% (trinta por cento) sobre o valor devido, adicionados a juros mensais de 01% (um por cento) e corrigidos monetariamente pelo IGP-M/FGV, todos a contar do desembolso até a data do efetivo pagamento.

CLÁUSULA DÉCIMA – DA OBSERVÂNCIA DAS LEIS ANTICORRUPÇÃO

10.1. As Partes reconhecem e concordam com as políticas das normas internacionais relativas às disposições da FCPA-EUA de 1977 e o Ato de Bribery de 2011 e da mesma forma reconhece que a **PATROCINADORA** é aderente às referidas políticas. As Partes estão comprometidas com a implementação e a divulgação de todos os princípios e regras que visam à luta contra a corrupção de funcionários internos e externos, lavagem de dinheiro e financiamento de terrorismo. As Partes concordam e se comprometem a não tomar qualquer ação que possa constituir uma violação as políticas e o envolvimento da outra Parte em violação de leis internacionais sobre o assunto, em qualquer jurisdição em virtude deste **Contrato**.

10.2. As Partes comprometem-se a não dar, emprestar, pagar, prometer, oferecer ou autorizar o pagamento, direito, indireto ou por meio de terceiros, de qualquer objeto de valor ou pagamentos a qualquer "funcionário público", nacional ou estrangeiro, com a finalidade de obter vantagens indevidas. As Partes declaram que qualquer comprovada ação deste tipo será de inteira responsabilidade da Parte infratora e motivo absoluto de rescisão imediata deste **Contrato**, sujeito a pagamento de perdas e danos à outra Parte.

10.3. As Partes declaram, ainda, que na assinatura deste **Contrato** nenhum funcionário público encontra-se associado ou possui qualquer interesse direto ou indireto com a empresa, bem como nenhuma relação jurídica ou benefício oriundo deste **Contrato**. Em vista do exposto, qualquer fato que venha a ser de conhecimento da outra Parte deve ser imediata e formalmente comunicado às Partes.

10.4. A **PATROCINADA** declara que os mecanismos, programas, procedimentos, sinais distintivos, assim como os serviços prestados, não infrigem nenhuma lei nem legislações aplicáveis ao serviço objeto do presente **Contrato**. Além disso, para o cumprimento dos serviços estabelecidos no presente **Contrato**, a **PATROCINADA** se obriga, durante a vigência do presente contrato, a conhecer, aplicar e cumprir rigorosamente e de boa-fé os preceitos do Modelo de Prevenção de Delito da Tata Consultancy Services do Brasil Ltda a que se refere o **Anexo II**, denominado "Prevenção de Delito", o qual faz parte integrante do presente **Contrato**.

CLÁUSULA DÉCIMA PRIMEIRA – DO CONFLITO DE INTERESSES

11.1. A **PATROCINADA** declara expressamente que não possui relações com executivose empregados da **TCS** ou de suas subsidiárias que implique ou possa implicar conflito de interesses na prestação de serviços ou nas relações éticas entre a **PATROCINADA** e a **PATROCINADORA**. Esta declaração abrange desde os empregados da **PATROCINADA** até os seus principais executivos, tanto nas relações comerciais

como nas relações familiares até o segundo grau de consanguinidade.

11.2. A relação e as atividades entre a **PATROCINADORA** e a **PATROCINADA** são reguladas também pelo Código de Conduta da **TCS** que está disponível no seguinte link: https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/about-us/Supplier-Code-OF-Conduct-Portuguese.pdf

11.3. Desse modo, a **PATROCINADA** declara ter conhecimento e seguir o Código de Conduta da **PATROCINADORA**, sendo que qualquer violação por parte da **PATROCINADA** deve ser imediatamente informada ao Comitê de Ética da **PATROCINADORA**.

CLÁUSULA DÉCIMA SEGUNDA - DAS DISPOSIÇÕES GERAIS

12.1. A **PATROCINADA** fica obrigada a manter durante toda a execução do **Contrato**, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas pela legislação aplicável.

12.2. Cada Parte é responsável por suas próprias obrigações. Nenhuma das Partes deverá fazer qualquer declaração ou incorrer em qualquer obrigação em nome ou benefício da outra Parte. A relação entre as Partes é exclusivamente de contratantes independentes.

12.3. As Partes não poderão ceder ou transferir, total ou parcialmente, qualquer das suas obrigações, direitos ou prerrogativas a terceiros ou sucessores legais, sem o prévio e expresso consentimento, por escrito, da outra Parte.

12.4. As Partes declaram, mutuamente, que o objeto do presente **Contrato** não infringe ou viola seus respectivos objetos sociais e atividades empresariais, nem quaisquer normas de natureza legal, regulamentar, administrativa, judiciária, convencional ou contratual.

12.5. As Partes declaram serem capazes para a celebração do presente instrumento, reconhecendo ainda que participaram conjunta e ativamente de sua negociação e redação, agindo de boa-fé, e na plena expressão e livre exercício de suas vontades.

12.6. As Partes firmam o presente **Contrato** em caráter de irrevogabilidade e irretratabilidade, obrigando seus sucessores a qualquer título, e substituindo quaisquer outros entendimentos anteriores, orais ou por escrito, com relação a seu objeto, termos e condições.

12.7. As Partes expressamente declaram e concordam que:

a) A demora ou omissão no exercício de direitos que lhes sejam assegurados por lei ou pelo presente **Contrato** não constituirá novação ou renúncia a tais direitos, nem prejudicará seu eventual e oportuno exercício;
b) A renúncia a direitos que lhes assistam em razão de lei ou do presente **Contrato** somente será válida se formalizada por escrito; e
c) A nulidade ou invalidade de qualquer das cláusulas do presente **Contrato** não prejudicará a validade e eficácia das demais.

12.8. Todas as correspondências, notificações e comunicações entre as Partes deverão ser feitas via e-mail, carta protocolada, notificação cartorária ou qualquer outro meio idôneo que permita confirmação de recebimento, direcionadas aos endereços constantes do preâmbulo do presente **Contrato**, devendo a Parte que tiver alteração de endereço, e-mail, telefone ou fax comunicar a outra

imediatamente, por escrito.

12.9. Fazem parte do presente **Contrato**, de forma complementar e indissociável, os seguintes Anexos:
Anexo I: Descrição do projeto;
Anexo II: Prevenção de Delitos; e
Anexo III: Acordo de Proteção de Dados – APD.

12.9.1. Ocorrendo dúvidas ou conflitos na interpretação dos termos de um Anexo e os dispositivos deste **Contrato**, os termos deste **Contrato** deverão prevalecer.

CLÁUSULA DÉCIMA TERCEIRA – DA ASSINATURA ELETRÔNICA

13. 1. As Partes e as testemunhas reconhecem a autenticidade, a validade e a eficácia deste **Contrato**, nos termos do art. 219 do Código Civil, em formato eletrônico e/ou assinado pelas Partes e testemunhas por meio de certificados eletrônicos, ainda que sejam certificados eletrônicos não emitidos pela ICP-Brasil, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, além de expressamente anuírem, aceitarem e reconhecerem como válida qualquer forma de comprovação de autoria das Partes e testemunhas signatárias deste **Contrato** por meio de certificados eletrônicos, sendo certo que quaisquer de tais certificados será suficiente para confirmar a autenticidade, a validade e a eficácia deste **Contrato** e a vinculação das Partes e das testemunhas aos seus termos, em conformidade com o § 4º do Art. 784 do Código de Processo Civil, com redação dada pela Lei nº 14.620, de 13 de julho de 2023. Não obstante, considerando que as assinaturas eletrônicas dos representantes legais das Partes e das testemunhas poderão ser realizadas na plataforma de assinatura eletrônica em data(s) posterior(es) à data de assinatura constante deste **Contrato**, as Partes e as testemunhas consentem desde já que a data de assinatura indicada expressamente neste **Contrato** deverá sempre prevalecer para todos os efeitos legais.

CLÁUSULA DÉCIMA QUARTA– DO FORO

14.1 F i c a eleito o Foro de Londrina, Estado do Paraná, com expressa renúncia a qualquer outro, por mais privilegiado que seja, como único competente para dirimir quaisquer dúvidas ou litígios acerca dos termos deste **Contrato**.

E por estarem justas e contratadas, as partes assinam este **Contrato**.

São Paulo, 08 de dezembro de 2025.

Carlos Renato Sposito

TATA CONSULTANCY SERVICES DO BRASIL LTDA

Juliana

INSTITUTO NÃO ME ESQUEÇAS

Testemunhas:

1. Jessica Mesquita
Nome:

2. Elaine Fernandes Mateus
Nome: Elaine Fernandes Mateus

U

ANEXO I

ANEXO II
Prevenção de Delitos

O presente anexo faz parte deste Contrato e tem como objetivo dar ciência à PATROCINADA que Tata Consultancy Services do Brasil Ltda ("TCS") estabeleceu um "Modelo de Prevenção de Crimes", alinhado com leis internacionais, boas práticas globais, Código Penal e Processo Penal Brasileiro e demais leis criminais aplicáveis, que definem políticas, procedimentos e controles que são obrigatórios para todos os fornecedores da TCS, cujo conhecimento, adesão, aceitação e cumprimento é reforçado pela TCS e aceito pela PATROCINADA.

O Modelo de Prevenção de Delito (sucessivamente chamado de "MPD") é um conjunto de normas e procedimentos que a TCS implementou para prevenir a ocorrência de delitos e evitar atos que possam causar impacto negativo à imagem, integridade e patrimônio financeiro da TCS.

Nesse sentido, o MPD busca identificar riscos, definir e monitorar os controles que de forma efetiva mitiguem tais riscos, impondo obrigações e sanções, assim como a implementação de um canal de denúncia, investigação de tais denúncias e mecanismos de capacitação/divulgação da informação, destinado tanto aos empregados TCS quanto aos fornecedores da TCS.

O MPD tem por objetivo especificamente o cumprimento da legislação aplicável relacionada com a prevenção de delitos que geram ou possam gerar, responsabilidade penal contra a TCS, tais como: suborno a funcionário público ou privado; lavagem de dinheiro – lavagem de ativos; financiamento ao terrorismo; corrupção entre particulares; receptação; administração desleal; negociação incompatível; apropriação indevida; bem como qualquer outro delitos ou conduta que no futuro possa ser incorporada à legislação aplicável e que possa gerar responsabilidade penal para a TCS.

Conforme cláusula anterior, através do Contrato e do presente Anexo, a PATROCINADA se obriga a:

a) Dar cumprimento as medidas de prevenção de delitos contemplados na legislação aplicável;

b) Dar conhecimento do conteúdo do presente anexo a todos seus sócios, diretores, empregados e demais colaboradores;

c) Utilizar a máxima diligência para a identificação de qualquer situação que tenha relação com os delitos definidos na legislação aplicável, e caso identificada qualquer situação suspeita, comunicar imediatamente a TCS de acordo com os termos do presente Anexo;

d) Colaborar com as investigações que a TCS esteja conduzindo para identificar possíveis descumprimentos ao MPD ou a ocorrência de delitos de acordo com a legislação aplicável, incluindo a entrega da informação que seja requerida conforme a legislação aplicável;

e) Não se envolver, por conta própria ou em nome da TCS, em nenhum dos delitos indicados no presente Anexo nem realizar nenhuma conduta que possa gerar qualquer infração à legislação aplicável;

f) Adotar todas as medidas necessárias para garantir que seus empregados, colaboradores, contratados e subcontratados não incorram em nenhuma conduta proibida pela lei e em especial aquelas que possam gerar algum tipo de responsabilidade para a TCS, bem como executar mecanismos de controle e supervisão necessários para evitar tais condutas por seus empregados, colaboradores, contratados e subcontratados.

Em caso da PATROCINADA, seus empregados, colaboradores, diretores e/ou representantes tenham conhecimento de qualquer situação suspeita, deverá reportá-la à TCS, através do e-mail mpd.latam@tcs.com, ou através do representante legal da TCS (bruno.rocha@tcs.com).

A TCS manterá a identidade daquele que realizar a denúncia em estrita confidencialidade.

Além disso, a PATROCINADA declara que não está sendo investigada atualmente por delitos apontados anteriormente, que possam gerar responsabilidade penal para a TCS, seus empregados, diretores, representantes ou acionistas. A PATROCINADA declara ainda que todo recurso, espécie ou dinheiro empregados para a prestação dos serviços objeto do presente Contrato foram obtidos de forma lícita.

Em caso de a PATROCINADA, seus empregados, colaboradores, diretores, representantes, colaboradores externos ou fornecedores não cumprirem com suas obrigações de vigilância, controle, denúncia, capacitação ou qualquer outra estabelecida no MPD e no presente Anexo, assim como no Código de Conduta da TCS para fornecedores, estarão sujeitos às consequências previstas no Contrato celebrado com a TCS, sem prejuízo da responsabilidade e consequências civis e penais que estão estabelecidas na legislação aplicável.

Qualquer descumprimento aos deveres impostos neste anexo pela PATROCINADA será considerado falta grave, e neste caso, a TCS poderá rescindir imediatamente o contrato, sem penalidades e/ou multas e sem a necessidade da TCS necessitar de ir à juizo para a resolução judicial.

ANEXO III
ACORDO DE PROTEÇÃO E TRATAMENTO DE DADOS PESSOAIS

As partes infra-assinadas, de um lado, **TATA CONSULTANCY SERVICES DO BRASIL LTDA**., inscrita no CNPJ sob o nº 04.266.331/0001-29, doravante **CONTROLADOR**; e, doutro lado **INSTITUTO NÃO ME ESQUEÇAS -** inscrita no CNPJ sob o **n.º 27.943.469/0001-10** doravante **OPERADOR**, conjuntamente denominados Partes, tem acordado celebrar o presente Acordo De Proteção E Tratamento De Dados Pessoais (doravante ACORDO), que será regido pelas cláusulas e condições a seguir:

CONSIDERAÇÕES

1. Levando em consideração a expertise do **OPERADOR** no tratamento de dados pessoais coletados pelo **CONTROLADOR** e a finalidade prevista neste ACORDO, as Partes acordam celebrar o presente e estipular as condições que regerão tal atividade, de acordo com o estabelecido na Lei Geral de Proteção de Dados Pessoais (LGPD), bem como outras leis, regulamentos, decretos e/ou outras normas de proteção de dados pessoais do Brasil (doravante "Legislação de Proteção de Dados"). Em razão disso, o **CONTROLADOR** entrega ao **OPERADOR** os dados pessoais que são necessários para a prestação do serviço para o qual foi contratado, e, desta forma, o **OPERADOR** realize o tratamento dos dados pessoais atendendo a todo momento as instruções do **CONTROLADOR.**

2. Os termos "Controlador", "Titular de Dados Pessoais", "Dados Pessoais", "Incidente/Violação de Segurança", "Operador", "Tratamento" e "Autoridade Nacional de Proteção de Dados", entre outros que sejam aplicáveis a este Contrato, terá o significado fornecido a esses termos ou termos semelhantes nos termos da Legislação de Proteção de Dados.

Desse modo, as Partes**:**

TEM JUSTO E ACORDADO

CLÁUSULA PRIMERA - OBJETO.

Através do presente ACORDO, o **OPERADOR** se obriga a realizar em nome do **CONTROLADOR** o tratamento de dados pessoais dos titulares que tenham concedido seu consentimento previamente ao **CONTROLADOR**, ou se houver outra base legal aplicável, para tratar os referidos dados de acordo com a finalidade indicada no Apêndice A (doravante "OBJETO").

O **OPERADOR** se obriga a realizar o tratamento dos dados pessoais se realizará única e exclusivamente dentro território do **Brasil**, sendo proibida a transferência para fora do território indicado.

CLÁUSULA SEGUNDA – DURAÇÃO DO TRATAMENTO.

As Partes acordam que o **OPERADOR** tratará os dados pessoais da **CONTROLADORA** TCS durante a vigência do CONTRATO PRINCIPAL, a menos que doutra forma indicado pela TCS.

CLÁUSULA TERCEIRA. – ESCOPO DO TRATAMENTO DE DADOS.

O **OPERADOR** sob orientação do **CONTROLADOR** realizará o tratamento dos dados pessoais indicados no Apêndice A (conjuntamente denominados "Dados Pessoais da TCS).

CLÁUSULA QUARTA. – OBRIGAÇÕES DO CONTROLADOR.

Em razão do presente ACORDO o **CONTROLADOR** se obriga a:

1. Dar conhecimento ao **OPERADOR** dos Dados Pessoais do **CONTROLADOR** objeto do presente ACORDO de acordo com o previsto entre as Partes.
2. Será responsável por assegurar que qualquer instrução transmitida ao **OPERADOR** com relação ao tratamento de dados pessoais estará de acordo con a Legislação de Proteção de Dados.

3. Retificar a informação quando estiver incorreta e comunicar o que for pertinente ao **OPERADOR.**

4. Exigir do **OPERADOR** o cumprimento das medidas de segurança requeridas segundos os Dados Pessoais da TCS entregues e o cumprimento das políticas em matéria de proteção de dados.

5. Processar os pedidos, consultas ou reclamações formuladas pelos titulares nos termos indicados na Lei de Proteção de Dados.

CLÁUSULA QUINTA – OBRIGAÇÕES DO OPERADOR

Em razão do presente ACORDO o **OPERADOR** se obriga com o **CONTROLADOR** do tratamento dos dados pessoais, a:

1. Dar tratamento aos Dados Pessoais da TCS por encargo do **CONTROLADOR** e de acordo com as instruções e as políticas de tratamento do **CONTROLADOR** disponíveis no link https://www.tcs.com/privacy-policy, e para o cumprimento do objeto do ACORDO, em relação aos propósitos definidos no CONTRATO PRINCIPAL.

2. Permitir o acesso à informação unicamente às pessoas que, em razão dos serviços contratados, precisem ter acesso a ela. Nesse sentido, deverá tratar os Dados Pessoais da TCS estritamente necessários para a execução do presente ACORDO, não podendo ser informados ou entregues a terceiros em nenhuma hipótese, ainda que para sua conservação, salvo com expressa autorização por escrito do **CONTROLADOR** para os casos permitidos pela lei. Em nenhuma hipótese o **OPERADOR** utilizará referidos dados pessoais para finalidades próprias e/ou finalidades distintas. Se o **OPERADOR**, por razões legais, tiver que compartilhar informação com alguma autoridade, o **OPERADOR** deverá notificar o **CONTROLADOR** imediatamente antes realizar o compartilhamento.

3. Os Dados Pessoais da TCS a serem tratados serão de titularidade exclusiva do **CONTROLADOR**, estendendo-se esta propriedade também a quaisquer elaborações, avaliações, segmentações ou processos similares que, em relação a eles, o **OPERADOR** realize de acordo com os serviços contratados, declarando as Partes que os Dados Pessoais da TCS serão confidenciais para todos os efeitos.

4. Auxiliar o **CONTROLADOR**, tendo em conta a natureza do tratamento, através de medidas técnicas e organizacionais adequadas, sempre que possível, para que possa cumprir a sua obrigação de responder às solicitações que visem o exercício dos direitos dos titulares de dados pessoais. estabelecido na Lei Geral de Proteção de Dados. Em qualquer caso, quando os interessados exercerem os direitos indicados perante o **OPERADOR**, este deverá notificar o **CONTROLADOR**. A comunicação deverá ser feita imediatamente e, em nenhum caso, depois do primeiro dia útil seguinte ao da recepção do pedido, juntamente, se for caso, com outras informações que possam ser relevantes para a resolução do pedido.

5. É responsabilidade do **CONTROLADOR** fornecer o direito à informação no momento da coleta de dados. Porém, caso, para a execução do serviço contratado, o **OPERADOR** colete dados em nome do **CONTROLADOR**, deverá o **OPERADOR** fornecer as informações relacionadas ao tratamento de dados que será realizado de acordo com a Lei Geral de Proteção de Dados. A redação e o formato

em que serão fornecidos deverão ser acordados com o **CONTROLADOR** antes do início da coleta dos dados.

6. Zelar pela segurança dos dados pessoais/bases de dados que contenham dados físicos e digitais, de acordo com o estabelecido neste CONTRATO e na Lei Geral de Proteção de Dados.

7. Auxiliar, colaborar, cooperar e ajudar ativamente o **CONTROLADOR** em relação a notificações e comunicações de violação de segurança dos Dados Pessoais da TCS às autoridades e aos titulares.

8. Implementar protocolos para a adequada condução de incidentes de segurança da informação.

9. Informar oportunamente ao **CONTROLADOR** sobre qualquer inconsistência evidenciada na informação recebida, para que possa tomar as medidas pertinentes.

10. Suprimir todos os Dados Pessoais da TCS quando for solicitado pelo **CONTROLADOR**, ou assim que seja encerrada a prestação dos serviços do CONTRATO PRINCIPAL, suprimindo as cópias existentes a menos que seja necessária a conservação por exigência legal (em qualquer caso, aplicando as medidas de segurança pertinentes), contribuindo, caso assim seja solicitado pelo **CONTROLADOR**, com certificado de cumprimento disso firmado pelos representantes legais do **OPERADOR** ou terceiro independente de renome. Da mesma forma, se exigido pelo **CONTROLADOR**, o **OPERADOR** deverá devolver em formato legível todos os Dados Pessoais da TCS.

11. Garantir a necessária formação e sensibilização relativamente à proteção dos dados pessoais das pessoas autorizadas a tratar Dados Pessoais da TCS. Em particular, deve garantir que sua equipe esteja ciente das medidas de segurança utilizadas pelo **OPERADOR** e como aplicá-las e como responder a incidentes relacionados a violações de segurança.

CLÁUSULA SÉTIMA - MEDIDAS DE SEGURANÇA

Tendo em conta o estado da técnica, os custos de aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades dos titulares, ou do **OPERADOR,** aplicará medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, que, quando apropriado, deve incluir, entre outros:

i. medidas que permitam restaurar rapidamente a disponibilidade e o acesso aos Dados Pessoais da TCS, em caso de incidente físico ou técnico;
ii. medidas necessárias para garantir a confidencialidade, integridade, disponibilidade e resiliência permanente dos Dados Pessoais da TCS, bem como dos dois sistemas e serviços de tratamento utilizados;
iii. medidas que permitam verificar e avaliar, de forma regular, a eficácia das medidas técnicas e organizacionais implementadas para garantir a segurança do tratamento;
iv. medidas de pseudonimização e criptografia de dados pessoais;
v. implementar um conjunto de controles e medidas de segurança, tais como políticas de segurança, organização de segurança, gestão de ativos, classificação e processamento de informação, segurança física, segurança de infraestruturas, segurança de operações, segurança de redes e comunicações, gestão de incidentes;
vi. garantir que os Dados Pessoais da TCS só possam ser acessados por pessoal autorizado para os fins estabelecidos neste CONTRATO;
vii. tomar todas as medidas razoáveis para impedir o acesso não autorizado aos Dados TCS, utilizando controles de entrada físicos e lógicos apropriados (senhas), protegendo áreas para processamento de dados e implementando procedimentos para monitoramento de dados;
viii. uso de senhas fortes, tecnologia de detecção de intrusão de rede, tecnologia de criptografia e autenticação, procedimentos de login seguros e programas antivírus;

ix. responder por todos os riscos decorrentes do processamento, por exemplo, destruição acidental ou ilegal, perda ou alteração, armazenamento não autorizado ou ilegal, processamento, acesso ou divulgação de dados a pessoas; implementar medidas para identificar vulnerabilidades com relação ao tratamento de Dados Pessoais da TCS nos sistemas utilizados para prover os serviços contratados a o **CONTROLADOR**;
x. realizar treinamento sobre proteção de dados pessoais e segurança da informação, de forma regular, a seus empregados e contratados para garantir capacitação contínua para executar as medidas de segurança estabelecidas neste CONTRATO e em suas políticas de segurança.

Em caso de modificação da normativa vigente em matéria de proteção de dados ou de outra normativa relacionada e que resulte aplicável ao tratamento objeto do presente CONTRATO, o **OPERADOR** garante a implantação e manutenção de quaisquer outras medidas de segurança que sejam exigíveis, sem que isso se suponha como uma modificação dos termos e condições do presente contrato.

Em qualquer caso, o **OPERADOR** implantará as medidas de segurança indicadas no Apêndice B deste ACORDO.

CLÁUSULA SÉTIMA – VIOLAÇÃO DE SEGURANÇA DOS DADOS PESSOAIS.

O **OPERADOR** deverá notificar o **CONTROLADOR** imediatamente após tomar conhecimento sobre um Incidente o violação de segurança de dados pessoais ou um incidente de segurança que afete ou possivelmente comprometa a segurança dos Dados Pessoais da TCS (doravante "Incidente de Segurança"), proporcionando ao **CONTROLADOR** informação suficiente para permitir que o **CONTROLADOR** cumpra com qualquer obrigação de informar ou notificar aos titulares sobre o Incidente de Segurança conforme determine a Lei Geral de Proteção de Dados. O **OPERADOR** deverá incluir na notificação, ao menos, as seguintes informações:

i. Data e hora do incidente de segurança e da identificação do incidente.
ii. Descrever a natureza do Incidente de Segurança, dados pessoais afetados, as categorias e números de titulares envolvidos, e as categorias e números de registros de Dados Pessoais da TCS envolvidos;
iii. Comunicar o nome e dados de contato do Encarregado de Proteção de dados do **OPERADOR** ou outro contato relevante junto do qual possam ser obtidas mais informações;
iv. Descrever os possíveis riscos e consequências do Incidente de Segurança, em especial aos Titulares de Dados; e
v. Medidas técnicas e organizacionais que o **OPERADOR** aplicou (ou aplicará) aos titulares em questão para mitigar possíveis efeitos negativos.
vi. Qualquer outra informação que deva ser comunicada de acordo com o disposto na Legislação de Proteção de Dados. A existência de um Incidente de segurança que provoque, entre outros, a divulgação, destruição, perda ou alteração acidental ou ilícita de dados pessoais, ou a comunicação ou acesso aos referidos dados, obriga o **OPERADOR** a iniciar os procedimentos necessários para minimizar o impacto dos referidos incidentes nas primeiras 24 horas após a confirmação.

O **OPERADOR**, se exigido pelo **CONTROLADOR**, cooperará prontamente e com integridade na investigação e gestão que o **CONTROLADOR** realizar com relação ao Incidente de Segurança, incluindo: auxiliar em qualquer investigação, facilitar entrevistas com qualquer pessoal do **OPERADOR** e outras pessoas envolvidas no assunto, disponibilizar todos os registros, logs, arquivos, relatórios de dados e outros materiais relacionado s ao Incidente de Segurança.

CLÁUSULA OITAVA – AUDITORIAS

O **OPERADOR** colocará à disposição do **CONTROLADOR**, mediante prévia solicitação com 30 dias corridos de antecedência, toda a informação necessária para demonstrar o cumprimento do presente ACORDO, e

permitirá e contribuirá com as auditorias, incluídas as inspeções por parte da Autoridade Nacional de Proteção de Dados, por parte do **CONTROLADOR** ou um auditor autorizado por este com relação ao tratamento de Dados Pessoais da TCS por parte do **OPERADOR** para a prestação dos serviços contratados.

O **OPERADOR** pagará os custos de qualquer auditoria em que se verifique que o **OPERADOR** inadimpliu o presente ACORDO ou quando tenha ocorrido Incidente de Segurança, confirmado ou suspeito, que afete os Dados Pessoais da TCS.

CLÁUSULA NONA - SUBCONTRATAÇÃO

O **OPERADOR** não poderá subcontratar nenhum dos serviços integrantes do OBJETO deste ACORDO que envolvam o tratamento de Dados Pessoais da TCS, exceto os serviços auxiliares necessários ao normal funcionamento dos serviços do **OPERADOR**. Entretanto, mediante autorização prévia por escrito do **CONTROLADOR**, o **OPERADOR** poderá transmitir ou solicitar o tratamento dos Dados Pessoais da TCS a um subprocessador, exclusivamente se referido tratamento seja necessário e esteja diretamente relacionado ao OBJETO deste CONTRATO. Com relação a cada subprocessador, ou **OPERADOR** deve:

i. Cumprir com os requisitos estabelecidos pela Legislação de Proteção de Dados para efetuar referida solicitação ou transmissão ao subprocessador;
ii. Antes que o subprocessador trate pela primeira vez os Dados Pessoais da TCS, deverá realizar a devida diligência apropriada para garantir que o subprocessador seja capaz de fornecer o nível de proteção e segurança para os Dados Pessoais da TCS exigido por este CONTRATO;
iii. Garantir que o subprocessador, que também terá a condição de operador de dados e cumprirá com as obrigações estabelecidas neste ACORDO para o **OPERADOR** e com as instruções estabelecidas pelo **CONTROLADOR**;
iv. Garantir que o acordo que deve ser assinado com o subprocessador seja regido por um contrato escrito que inclua termos que ofereçam, pelo menos, o mesmo nível de proteção para os Dados Pessoais da TCS que aqueles aqui estabelecidos neste ACORDO.
v. A pedido do **CONTROLADOR**, fornece para revisão cópias de dois contratos de tratamento de dados pessoais FIRMADOS com os subprocessadores.
vi. Caso a ordem de processamento para o subprocessador envolva uma transferência internacional de Dados Pessoais da TCS, o **OPERADOR** deverá solicitar aprovação prévia por escrito do **CONTROLADOR**.

Em qualquer caso, o **OPERADOR** será exclusivamente responsável pelos atos, omissões ou inadimplementos do subprocessador com relação ao tratamento inadequado dos Dados Pessoais da TCS perante o **CONTROLADOR**.

CLÁUSULA DÉCIMA - INDENIZAÇÃO

O **OPERADOR** se obriga perante o CONTROLADOR a firmar e fazer com que seus funcionários, contratados e subcontratados assinem acordos de confidencialidade, declaração de conhecimento das políticas de segurança do **OPERADOR** bem como todos os documentos necessários para garantir a segurança e proteção dos Dados Pessoais da TCS.

Sem prejuízo das disposições do Contrato Principal, o **OPERADOR** deverá indenizar, defender e eximir de responsabilidade o **CONTROLADOR** e indenizar e reembolsar o **CONTROLADOR** por todos os custos razoáveis, sejam de remediação, judiciais e legais e quaisquer danos, perdas, decisões, acordos, responsabilidades, multas, custos relacionados e despesas incorridas pelo **CONTROLADOR** que surjam em relação a qualquer violação deste ACORDO ou da Legislação de Proteção de Dados pelo **OPERADOR** e/ou seu subprocessador. Esta obrigação de indenização não estará sujeita a qualquer limitação ou exclusão de responsabilidade sob o CONTRATO PRINCIPAL ou qualquer outro acordo entre as partes.

CLÁUSULA DÉCIMA PRIMEIRA – NOTIFICAÇÕES

Todas as comunicações necessárias para a execução deste CONTRATO serão feitas por e-mail.
Para efeito do acima estabelecido, a informação de contato das Partes é a seguinte:

Para **o CONTROLADOR**	Dpo.latam@tcs.com; dpo.brasil@tcs.com
Para **o OPERADOR**	contato@inme.org.br; elaine@inme.org.br

CLÁUSULA DÉCIMA SEGUNDA - ACORDO GERAL.

Este ACORDO e os documentos subsequentes dele derivados, constituem a totalidade do acordo entre as partes, portanto qualquer acordo prévio, oral ou escrito entre as partes relacionado ao objeto deste instrumento, fica extinto e sem validade jurídica a partir da assinatura do presente instrumento. Todas as modificações, alterações ou alterações a qualquer condição deste instrumento serão acordadas por escrito entre as partes, anexando a referida alteração, modificação ou alteração como ANEXO a este ACORDO.

FIM DO ANEXO II

APÊNDICE A: Detalhes do tratamento de dados pessoais

Finalidade(s)	*indicar propósito(s) para o(os) qual(is) o operador tratará os dados pessoais entregados por TCS.*	
Tipos de tratamento *(ações que realizará o operador com relação aos Dados Pessoais da TCS)*	☐ *Coleta/Recepção* ☐*Armazenamento* ☐ *Classificação* ☐ *X Consulta* ☐X *Divulgação* ☐ *Avaliação/Controle* ☐ *Supressão/Eliminação* ☐ *Conservação* ☐ *Outros: .....*	☐ *Registro* ☐ *Modificação* ☐ *Extração* ☐ *X comunicação* ☐ *Transferência* ☐ *Limitação* ☐ *Destruição* ☐ *Uso*
Categorias de dados pessoais	*indicar tipos de dados pessoais que serão tratados pelo operador para a execução do serviço contratado.* ☐**Gerais:** ☐ Identificação (nome e sobrenome) ☐ endereço pessoal e/ou do local de trabalho ☐ país de residência ☐ nº passaporte ☐ Visto ☐ data de Nascimento ☐ *Curriculum Vitae* ☐ Salário ☐ correio eletrônico ☐ número de telefone ☐ informação acadêmica (escola, instituição, universidade, curso) ☐ experiencia de trabalho	

	☐ dados de navegação de internet (web) ☐ dados da conta bancária ☐ gênero ☐ estado civil ☐ registros criminais ☐ X Outros: N/A ☐**Sensíveis** *(Ex. dados pessoais origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico):*_____ ☐**Crianças e Adolescentes:** Qualquer informação de crianças e adolescentes ☐**Crédito:** ☐ Dados identificativos financeiros ☐ Dados de crédito (cartão de crédito e/ou conta bancária) ☐ Dados econômicos e de solvência patrimonial
Categoria de interessados	*Indicar quem serão os titulares dos dados pessoais tratados pelo operador.* ☐ empregados TCS ☐ de clientes da TCS ☐ fornecedores da TCS ☐ X Outros: N/A

FIM DO APÊNDICE A

Apêndice B ao Anexo II: Medidas de Segurança para tratamento de dados pessoais

Descrição das medidas de segurança técnicas e organizacionais a serem implementadas pelo **OPERADOR**, de acordo com a Legislação de Proteção de Dados.

Para efeitos do presente Anexo, o cliente corresponde ao **CONTROLADOR**.

Controle de acesso	É necessário documentar e implementar um processo de ciclo de vida de gerenciamento de acesso de usuários. O processo abrangerá: a) novos usuários, mudanças, saídas; b) acesso com privilégios e sem privilégios c) revisão periódica/recertificação d) rotinas de aprovação e) monitoramento do processo f) garantia de que apenas contas individuais e exclusivas sejam permitidas.
Mecanismos de controle de acesso	O acesso aos sistemas de informação requer autenticação forte/de dois fatores. O produto/serviço deve suportar mecanismos padronizados de integração de controle de acesso, como Kerberos e SAML.
Proteção de aplicações	O produto/serviço deve ser protegido contra acesso não autorizado a informação através de: a) fortalecimento, garantindo que todos os softwares, serviços de rede e aplicativos desnecessários tenham sido desativados/removidos b) fornecer "defesa em profundidade" (ou seja, usando múltiplas camadas de diferentes tipos de proteção) para evitar a dependência de um único tipo ou método de controle de segurança

	e) permitir o acesso aos serviços do Prestador apenas a partir da rede corporativa de dois clientes (em oposição, por exemplo, a partir dos computadores pessoais de dois funcionários). O produto/serviço deve ser protegido contra divulgação não autorizada de informações confidenciais, garantindo que: a) Executar com "privilégios mínimos" (ou seja, apenas os privilégios de acesso mais baixos possíveis são concedidos a um usuário ou processo ao acessar o sistema, e não privilégios de acesso especiais, como "root" em sistemas UNIX ou "Administrador" em sistemas Windows) b) impor a separação de privilégios (por exemplo, dividir funções de aplicativos e dividir chaves criptográficas) c) impedir o início de conexões de rede com a Internet (por exemplo, por meio de configuração de servidor ou por regras em um firewall) d) impedir que informações sobre o funcionamento interno dos aplicativos sejam divulgadas (por exemplo, em respostas de aplicativos, mensagens de erro ou comentários de desenvolvedores (particularmente em aplicativos baseados em HTML e Javascript)). e) separar os dados e serviços de dois clientes de outros clientes de forma a garantir a segurança (confidencialidade, integridade e disponibilidade) dos dados do cliente, mesmo que a lógica da aplicação ou os controles de acesso que separam os diferentes clientes falhem. Descrever como os dados e os serviços do cliente são separados uns dos outros nas diferentes camadas (aplicativo, sistema operacional, VM, hiper visor, físico, rede). f) não afetar a segurança (confidencialidade, integridade, disponibilidade) do cliente devido a decisões judiciais, intimações legais, etc. endereçado aos seus outros hóspedes.
Registro de ativos	Todo hardware/software deve ser registrado em um registro de ativos preciso e atualizado.
Cópias de segurança.	Deve ter padrões/procedimentos documentados para fazer cópias de backup, que abrangem: a) os tipos de informações e software dos quais será feito backup b) ciclos de backup d) proteção de cópias de segurança.
Proteção de aplicações baseadas em navegador	O produto/serviço será desenvolvido de acordo com as diretrizes do Open Web Application Security Project (www.owasp.org) e será continuamente protegido contra os 10 principais riscos/vulnerabilidades do WASP mais recentes.
Gestão de mudanças	Deve ser estabelecido um processo de gestão de mudanças que cubra todos os tipos de mudanças (por exemplo, atualizações e modificações em aplicativos e software, modificações em informações comerciais, "correções" emergenciais e mudanças em sistemas e redes de informação) que abranjam: - aprovação do gerente autorizado - análise de impacto - prova - plano de retirada As atualizações do produto devem ser testadas, revisadas e aplicadas por meio de um processo de gerenciamento de mudanças.
Dispositivos de consumo e BYOD (*Bring Your Own Device* - traga seu próprio aparelho)	Quando uma organização permite o uso de dispositivos de consumo para fins comerciais, isso deve ser apoiado por padrões/procedimentos documentados para garantir que informações comerciais críticas e confidenciais tratadas em dispositivos de consumo recebam o mesmo nível de proteção normalmente fornecido para dispositivos móveis (por exemplo, laptops).
Gerenciamento de Crise	O processo de gerenciamento de crises deve: a) incluir medidas claramente definidas que devem ser tomadas em situações de crise

	ou emergência b) fornecer detalhes de contato de todas as pessoas chave (incluindo a equipe de gestão de crises e aquelas associadas a partes externas, como órgãos de aplicação da lei, reguladores do setor e organizações da cadeia de suprimentos) c) ser testados e aprovados regularmente, utilizando simulações reais.
Gestão de chaves criptográficas	Deve haver padrões/procedimentos documentados para gerenciamento de chaves criptográficas, abrangendo: a) o ciclo de vida das chaves criptográficas b) responsabilidades de dois proprietários de chaves criptográficas c) proteção de chaves criptográficas As chaves criptográficas devem ser gerenciadas de forma segura e protegidas contra acesso não autorizado ou destruição.
Soluções criptográficas	A criptografia deve ser usada para dados em trânsito e em repouso em toda a organização para: a) proteger a confidencialidade de informações confidenciais/sensíveis ou informações sujeitas a requisitos legais e regulatórios de criptografia (por exemplo, o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) e a Diretiva 95/46/EC da Comissão Europeia). As soluções criptográficas devem estar sujeitas a aprovação, documentadas e aplicadas.
Arranjos de acesso do cliente	Deve haver padrões/procedimentos documentados para o fornecimento de acesso aos aplicativos de negócios da organização pelos clientes.
Ataques de crimes cibernéticos	Deve haver procedimentos documentados para lidar com ataques cibernéticos.
Correio Eletrônico	Os sistemas de e-mail e de mensagens instantâneas devem ser protegidos para garantir que estejam disponíveis quando necessário, que a confidencialidade e a integridade das mensagens sejam protegidas em trânsito e que o risco de uso indevido seja minimizado.
Reparos de emergência	Devem existir normas/procedimentos documentados para a aplicação de soluções de emergência a informações empresariais, aplicações empresariais e infraestruturas técnicas (incluindo software de sistemas e equipamento informático). Os reparos de emergência devem ser aprovados por um representante de vendas apropriado, registrados e realizados de acordo com padrões/procedimentos.
Conexões de rede externas	Todas as ligações de rede externa a sistemas e redes de informação devem ser identificadas, verificadas, registadas e aprovadas individualmente pelos sistemas de informação ou pelo proprietário da rede.
Processo de gestão de fornecedores externos	Deve haver um processo documentado para gerenciar os riscos de informação associados a fornecedores terceirizados (incluindo hardware, software, terceirização e serviços em nuvem). O processo deve ser incorporado ao processo de aquisição da organização e envolver a função de segurança da informação durante todo o processo de aquisição do ciclo de vida de gestão de fornecedores.
Firewall	Os firewalls protegerão as redes fazendo com que o tráfego de rede seja roteado através do firewall antes de acessar ou sair das redes.
Proteção contra perigos	As instalações críticas (incluindo locais que armazenam sistemas informáticos, como bases de dados, redes, equipamentos de telecomunicações, materiais físicos sensíveis e outros ativos importantes) devem ser protegidas contra incêndios, inundações, perigos ambientais e outros perigos naturais.
Classificação da informação	Deve ser estabelecido um esquema de classificação da informação que seja aplicado em toda a organização, com base na confidencialidade, integridade e disponibilidade da informação. Ao lidar com dados de clientes, a classificação das informações dos clientes deve ter prioridade sobre a política de classificação da organização.
Proteção	Mecanismos de proteção contra vazamento de informações devem ser empregados

contrafugas de informação	para sistemas e redes de informação que processam, armazenam e transmitem informações confidenciais (por exemplo, informações altamente confidenciais, informações relacionadas à privacidade ou informações sujeitas a requisitos regulatórios, como o Padrão de Segurança da Informação). dados do setor (PCI DSS, Lei Sarbanes-Oxley ou HIPAA).
Programa de garantia de segurança da informação	Devem ser estabelecidas atividades de segurança da informação que garantam que: a) os requisitos de segurança são identificados com base na classificação da informação, na avaliação do risco da informação e nos requisitos de conformidade (legal/regulatório/contratual) b) os riscos identificados são tratados de acordo com os requisitos do negócio, e os riscos aceitos estão sujeitos à aprovação da empresa c) controles de segurança relevantes são implementados d) o risco da informação é gerenciado como parte da metodologia de gerenciamento de projetos da organização e) a eficácia e eficiência das medidas de segurança são monitoradas e comunicadas ao órgão responsável.
Gestão de incidentes de segurança da informação	Os incidentes de segurança da informação devem ser identificados, respondidos, recuperados e acompanhados (incluindo investigações forenses) através de um processo de gestão de incidentes de segurança da informação. Incidentes de segurança relacionados às informações do cliente devem ser relatados ao cliente imediatamente.
Política de segurança da informação	Existe uma política de segurança da informação documentada que se aplica a toda a organização? A organização possui uma equipe dedicada ao gerenciamento da segurança da informação? A quem este grupo se reporta? (Explique a estrutura até o CEO) A política de segurança da informação deve definir a segurança da informação, as responsabilidades associadas e os princípios de segurança da informação que todo o pessoal deve seguir.
Detecção de invasões	Os mecanismos de detecção de invasões devem ser aplicados a sistemas e redes de informação de alto risco.
Cumprimento legal e regulatório	Deve existir um processo para garantir o cumprimento do produto/serviço, que abrange: a) descobrir leis e regulamentos que afetam a segurança da informação b) interpretar as implicações de segurança da informação das leis e regulamentos descobertos c) identificar possíveis violações legais/regulatórias (por exemplo, realizar uma avaliação de risco de conformidade com leis e regulamentos) d) abordar áreas de possível não conformidade legal/regulatória.
Coordenação de segurança local	A responsabilidade pela segurança da informação deve ser atribuída ao responsável por cada unidade de negócios ou departamento local.
Software de proteção contra malware	Um software eficaz de proteção contra malware deve ser instalado, configurado e mantido em toda a organização.
Gestão da avaliação de riscos da informação	Deve haver padrões/procedimentos documentados para a realização de avaliações de risco de informações, que se aplicam a toda a organização. As normas/procedimentos devem abranger: a) necessidade de realizar avaliações de risco de informação b) tipos de ambiente-alvo que devem ser avaliados quanto a riscos de informação (incluindo processos de negócios internos e processos na cadeia de abastecimento) c) circunstâncias em que devem ser realizadas avaliações de risco da informação (pelo menos uma vez por ano, bem como em caso de alterações que possam afetar a segurança da informação) d) as pessoas que devem participar em suas responsabilidades específicas

	e) métodos de gestão e resposta aos resultados das avaliações de risco da informação.
Configuração do dispositivo móvel	Os dispositivos móveis (incluindo laptops e dispositivos de consumo) devem ser suportados por padrões/procedimentos documentados, abrangendo: a) configuração do sistema (por exemplo, firmware seguro e uso de versões padrão) b) fornecimento de software para protegê-los (por exemplo, ferramentas de administração de sistema, mecanismos de controle de acesso, software de proteção contra malware e recursos de criptografia) c) proteção de memória de dispositivos de computador contra uso indevido e ataque d) uso de criptografia para proteger informações confidenciais e) configuração do log de eventos.
Monitoramento de conformidade de segurança da informação	As normas/procedimentos devem abranger: a) identificar obrigações de conformidade de segurança (por exemplo, decorrentes de legislação, regulamentos, obrigações contratuais e padrões do setor) b) traduzir obrigações em requisitos e controles de segurança da informação relacionados à conformidade c) implementar controles de segurança para cumprir as obrigações d) monitorar os controles de segurança da informação relacionados à conformidade e) reportar os resultados das atividades de monitoramento e recomendar ações para mitigar os riscos de compliance. Deve haver padrões/procedimentos documentados para monitorar a conformidade da segurança da informação em toda a organização.
Configuração de dispositivos de rede	Deve haver padrões/procedimentos documentados para configuração de dispositivos de rede (por exemplo, roteadores, hubs, pontes, hubs, switches e firewalls), abrangendo: a) configuração do dispositivo b) restringir o acesso a dispositivos de rede c) vulnerabilidade e gerenciamento de patches d) revisão periódica da configuração e instalação de dois dispositivos de rede.
Equipe de Escritório	O equipamento de escritório deve ser apoiado por normas/procedimentos documentados, abrangendo: a) implantação e proteção física de equipamentos de escritório b) restringir o acesso a equipamentos sensíveis c) monitorar o uso de equipamentos de escritório d) criptografar as informações transmitidas e processadas pelo equipamento de escritório e) desmontar equipamentos de escritório com segurança.
Gestão de rede física	Os cabos de rede e os pontos de acesso à rede devem ser protegidos para evitar que usuários não autorizados acessem sistemas e redes de informação.
Proteção física	Os padrões/procedimentos devem ser preenchidos: a) proteger as instalações críticas contra o acesso não autorizado b) localizar as instalações críticas abaixo do acesso ou acesso público c) restringir o acesso a instalações críticas que permitem ou habilitam a infraestrutura crítica da organização; d) gerenciar a autorização para acesso físico a instalações críticas e) restringir o acesso de visitantes a instalações críticas. Os edifícios que abrigam instalações críticas devem ser protegidos contra acesso não autorizado mediante: a) instalar fechaduras, parafusos (ou equivalentes) em portas e janelas vulneráveis, e empregar guardas de segurança b) instalação de circuito fechado de televisão (CCTV) ou equivalente c) localizar sistemas de detecção de intrusos em portas e janelas externas acessíveis e realizar verificações com regularidade.

Dispositivos de armazenamento portáteis	A utilização de dispositivos de armazenamento portáteis (por exemplo, unidades flash USB, discos rígidos externos, leitores multimédia e leitores de e-books) deve estar sujeita à aprovação, o acesso aos mesmos deve ser restrito e as informações armazenadas devem apenas ser protegidas.
Fontes de alimentação elétrica	Instalações críticas (incluindo locais que abrigam sistemas de computadores, como data centers, redes, equipamentos de telecomunicações, materiais físicos sensíveis e outros ativos importantes) devem ser protegidas contra cortes de energia.
Garantia de qualidade	A garantia de qualidade da metodologia de desenvolvimento de produtos/serviços deve incluir: b) verificar se os requisitos de segurança foram claramente definidos c) confirmar que os controles de segurança foram desenvolvidos e funcionam corretamente d) confirmar se os responsáveis pelo desenvolvimento, teste e implementação dos sistemas em desenvolvimento estão seguindo a metodologia de desenvolvimento de sistemas.
Ambientes remotos	A equipe que trabalha em ambientes remotos (por exemplo, em locais diferentes das instalações da organização) deve estar sujeita a autorização, proteger os dispositivos de computação contra perda e roubo, ser apoiada por materiais de conscientização sobre segurança e empregar controles adicionais ao viajar para países de alto risco ou regiões.
Mantenimento Remoto	A manutenção remota de sistemas e redes deve ser restrita a pessoas autorizadas e fortemente autenticadas, confinada a um período de tempo limitado, sujeita ao registo de todas as atividades realizadas e revistas periodicamente.
Funções e responsabilidades	A propriedade de informações críticas e sensíveis, aplicações empresariais, sistemas de informação e redes deve ser atribuída a indivíduos (por exemplo, gestores empresariais) e as responsabilidades dos proprietários devem ser documentadas. As responsabilidades pela proteção de informações críticas e sensíveis, aplicações empresariais, sistemas de informação e redes devem ser comunicadas e aceitas pelos proprietários.
Gestão de auditorias de segurança	Auditorias de segurança independentes devem ser realizadas regularmente para ambientes-alvo que sejam críticos para a entrega ao cliente. Descobertas significativas devem ser comunicadas imediatamente ao cliente.
Processo de auditoria de segurança: planejamento	Os auditores internos ou externos do cliente terão o direito de iniciar um exame da adoção administrativa (regulamentos, planos, políticas) bem como técnica (testes de penetração, exames de servidores) dos regulamentos de segurança nas instalações do Fornecedor.
Mensagens de concientização sobre segurança	As pessoas que tenham acceso a la información e los sistemas de la organización deben tener mensajes de segurança personalizados e apropiados que se les comuniquen periódicamente.
Programa de concientização sobre segurança	Um programa de conscientização sobre segurança deve ser estabelecido para promover a conscientização sobre segurança em toda a organização e estabelecer uma cultura de segurança positiva.
Registro de incidentes de segurança	As normas/procedimentos para registrar incidentes de segurança devem abranger: b) identificação de aplicações empresariais e sistemas de infraestrutura técnica em que o registro de incidentes deve ser habilitado para ajudar a identificar incidentes relacionados à segurança c) configurar sistemas de informação para gerar incidentes relacionados à segurança (incluindo tipos de incidentes como tentativas de login mal-sucedidas, bloqueio de sistema, exclusão de conta de usuário e atributos de evento como data, hora, ID de usuário, nome de arquivo, endereço IP) d) armazenamento de incidentes relacionados à segurança em dois logs de eventos (por exemplo, usando sistemas locais, servidores centrais ou usando armazenamento

	fornecido por um provedor de serviços externo) e) análise de logs de eventos relacionados à segurança (incluindo normalização, agregação e correlação) f) proteção de registros de incidentes relacionados à segurança (por exemplo, por meio de criptografia, controle de acesso e cópia de segurança) g) retenção de registos de incidentes relacionados com a segurança (por exemplo, para cumprir requisitos legais, regulamentares e comerciais para potenciais investigações forenses). Incidentes relacionados à segurança (incluindo tipos de incidentes como tentativas de login mal-sucedidas, bloqueio do sistema, exclusão de conta de usuário e atributos de incidente como data, hora, ID do usuário, nome do arquivo, endereço IP) devem ser registrados nos registros do produto/serviço e protegido contra alterações não autorizadas.
Testes de segurança	Os produtos/serviços devem estar sujeitos a testes de segurança nos sistemas em desenvolvimento, incluindo: a) realizar verificações de segurança independentes do código do aplicativo b) aprovação dos resultados da revisão do código c) determinar a eficácia de dois controles de segurança d) realizar testes de ataque específicos para identificar pontos fracos em aplicativos baseados em navegador e) usar dados de teste para testes de segurança f) resolução de bugs e falhas de segurança identificadas durante a revisão e teste do código. g) assinatura de falhas e mitigações de falhas de segurança.
Configuração do servidor	Os servidores devem ser configurados de acordo com padrões/procedimentos documentados, que abrangem: a) fornecer configurações de firmware padrão b) usar imagens de servidor padrão e padronizadas para construir/configurar servidores c) alterar os valores padrão do provedor e outros parâmetros de segurança d) desativar ou restringir funções e serviços desnecessários e) restringir o acesso a utilitários de sistema poderosos e configuração de parâmetros de host (por exemplo, o "Editor de Registro" do Windows) f) proteção contra acesso não autorizado Os servidores de hospedagem devem ser configuráveis de acordo com padrões/procedimentos documentados, que abrangem: a) fornecer configurações de firmware padrão b) usar imagens de servidor padrão e padronizadas para construir/configurar servidores c) alterar os valores padrão do provedor e outros parâmetros de segurança d) desativar ou restringir funções e serviços desnecessários e) restringir o acesso a utilitários de sistema poderosos e configuração de parâmetros de host (por exemplo, o "Editor de Registro" do Windows) f) proteção contra acesso não autorizado.
Especificações de requisitos	A metodologia de desenvolvimento de produtos/serviços deve incluir a especificação de requisitos para proteger a confidencialidade, integridade e disponibilidade da informação ao longo do seu ciclo de vida não-produto/serviço, incluindo: a) criação (por exemplo, validação de entrada) b) processamento (por exemplo, verificação de integridade e desempenho) c) armazenamento (por exemplo, localização e controle de acesso) d) transmissão (por exemplo, verificação de origem e destino) e) destruição (por exemplo, exclusão segura).
Acordos pessoais	Os termos e condições de emprego devem:

	a) declarar que as responsabilidades de segurança da informação se estendem além do horário e das instalações normais de trabalho e continuam após o término do emprego b) explicar as responsabilidades e os direitos legais do funcionário (por exemplo, no que diz respeito às leis de direitos autorais, proteção de dados ou legislação de privacidade) c) exigir que o funcionário cumpra a política de segurança da informação e as políticas de apoio da organização (por exemplo, políticas de uso aceitável) d) incluir cláusula de confidencialidade/não divulgação. Os candidatos a empregos (incluindo funcionários internos e externos, como consultores, prestadores, engenheiros e funcionários terceirizados) devem ser selecionados antes de iniciar o trabalho (por exemplo, obtendo referências, verificando antecedentes/qualificações profissionais e confirmando a identidade, por exemplo, inspecionando um Documento de Identidade).
Gestão de vulnerabilidades de software e sistemas	Deve haver padrões/procedimentos documentados para gerenciamento de vulnerabilidades de software e sistema que especifiquem: a) requisito para gerenciar vulnerabilidades de sistemas e software associadas a aplicativos de negócios, sistemas de informação e dispositivos de rede b) método para identificar a publicação ou descoberta de vulnerabilidades técnicas (por exemplo, de domínio não público), em tempo hábil c) necessidade de verificar aplicativos de negócios, sistemas de informação e dispositivos de rede em busca de vulnerabilidades de sistemas e software d) a abordagem da organização para aplicação de patches (ou seja, o processo de gerenciamento de patches) e) métodos de distribuição de patches (por exemplo, implantação automatizada). Deve existir um processo para identificação e correção de vulnerabilidades no produto/serviço, e deve ser distribuído/implementado em tempo hábil. Deve haver um processo para receber e remediar vulnerabilidades não relacionadas a produtos/serviços identificadas pelo cliente e distribuídas/implementadas em tempo hábil.
Ambientes de desenvolvimento de sistemas	O código-fonte da aplicação (ou equivalente) utilizado em ambientes de desenvolvimento deve ser protegido por: b) impedir que a equipe de desenvolvimento faça alterações não autorizadas em ambientes ativos (por exemplo, usando software de controle de acesso) c) aplicar controle de versão rigoroso sobre software de desenvolvimento de sistemas (por exemplo, usando gerenciamento de configuração, registrando o acesso em um log e arquivando regularmente versões antigas do software) O produto/serviço deve ser desenvolvido em ambientes de desenvolvimento especializados, isolados entre ambientes de produção e de teste, e protegidos contra acesso não autorizado. Deve haver uma metodologia de desenvolvimento de sistemas documentada (muitas vezes chamada de ciclo de vida de desenvolvimento de sistemas (SDLC)), que se baseia em práticas sólidas de desenvolvimento de sistemas e gerenciamento de projetos. Deve haver padrões/procedimentos documentados para o desenvolvimento do produto/serviço (incluindo aqueles em desenvolvimento), abrangendo: a) especificar requisitos b) projetar, construir e testar aplicativos c) promoção de aplicações em ambiente não ativo A metodologia de desenvolvimento do sistema deve garantir que o produto/serviço seja desenvolvido para atender: a) suas próprias políticas, padrões, procedimentos e diretrizes internas de segurança da informação

	b) requisitos legais e regulamentares, incluindo regulamentos de privacidade c) requisitos contratuais d) requisitos específicos de segurança de produtos/serviços baseados em riscos.
Autorização de usuário	Os processos de autorização de usuários devem: a) ser definido por escrito, aprovado pelo proprietário aplicável e aplicado a todos os usuários b) associar privilégios de acesso a usuários definidos (por exemplo, usando identificadores exclusivos como IDs de usuário) c) atribuir aos usuários acesso padrão com base no princípio do menor privilégio (por exemplo, "nenhum" em vez de "leitura") d) garantir que identificadores redundantes (por exemplo, ID de usuário) não sejam reemitidos para uso.
Acceso a redes sem fio	O acesso às redes sem fio deve ser autorizado, os usuários e os dispositivos de computação devem ser autenticados e o tráfego sem fio deve ser criptografado.

FIM DO APÊNDICE II