PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ACORDO DE COOPERAÇÃO TÉCNICA SLC/TRT 19ª REGIÃO N. 03/2026
(Proad n. 956/2024)

TERMO DE ACORDO DE COOPERAÇÃO TÉCNICA SEM TRANSFERÊNCIA DE RECURSOS QUE ENTRE SI CELEBRAM O TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO – TRT-19 E A EMPRESA TELEFÔNICA BRASIL S.A. (VIVO), a fim de disponibilizar via *web* a magistrados e servidores públicos da Justiça do Trabalho o sistema eletrônico PORTAL JUS (doravante denominado Sistema), para acesso a dados de clientes e registros de fluxos telefônicos e de dados, que sejam necessários para instruir processos judiciais em conformidade com a legislação vigente.

O **TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO**, pessoa jurídica de direito público**,** sediado na Avenida da Paz, n. 2.076, Centro, Maceió-AL, inscrito no CNPJ sob o n. 35.734.318/0001-80, doravante denominado **TRT19** ou neste ato representado por seu Presidente, Desembargador JASIEL IVO, residente e domiciliado nesta Capital, e a empresa **TELEFÔNICA BRASIL S.A.** com sede na Av. Engenheiro Luiz Carlos Berrini, 1376, Cidade Monções, São Paulo/SP no CNPJ sob o nº 02.558.157/0001-62,doravante denominada **VIVO**, neste ato representada por seus procuradores, **FERNANDA FORTUNATO MARTINS CHAGURI**, portadora do documento de identidade n° ***.957, expedido pela OAB/SP e inscrita no CPF/MF sob nº ***.795.***-** e **PATRÍCIA ANDREA TEDESCO GODOI**, portadora da Carteira de Identidade RG **.775.***-* SSP-SP e inscrita no CPF/MF sob nº ***.822.***-**,resolvem firmar o presente Termo regido pela Lei n° 14.133/2021,Decreto nº 11.531, de 16 de maio de 2023 e à Portaria SEGES/MGI nº 3.506/2025,e alterações posteriores, pelas cláusulas e condições que se seguem.

CLÁUSULA PRIMEIRA– DO OBJETO

1.1) O presente Acordo de Cooperação Técnica tem por objeto permitir o acesso, via

WEB, a magistrados e servidores públicos do **TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO** ao sistema eletrônico denominado “Portal Jud” da **VIVO**, possibilitando o fornecimento de informações de dados cadastrais de seus clientes, conforme condições e fluxo estabelecidos neste ajuste.

1.1.1) Fazem parte integrante do presente instrumento os Anexo I – Termo de Aceite do Portal Jud, Anexo II -Termo de Tratamento de Dados Pessoais, Anexo III - Segurança Digital, Anexo IV – Certificado Anticorrupção e Anexo V - Plano de Trabalho, valendo seus termos e suas condições para todos os fins de direito, salvo no que contrariem o disposto neste instrumento, caso em que prevalecerão os termos deste Acordo de Cooperação Técnica.

1.2) Os partícipes têm total e pleno conhecimento de que toda e cada consulta realizada sempre será embasada em uma determinação (ordem) judicial específica proferida nos autos de processo judicial por magistrado ou desembargador competente.

1.3) O acesso ao sistema “Portal Jud” será disponibilizado aos magistrados, desembargadores e servidores públicos, os quais serão autorizados mediante ofício encaminhado a **VIVO**, devidamente assinado pelo Desembargador Presidente do **TRT19**, ou por quem venha a ser designado pelo mesmo, contendo as seguintes informações individualizadas: nome completo, RG, CPF, e-mail funcional, e telefone de contato, nos termos do Anexo I.

1.3.1) Os magistrados e servidores públicos autorizados serão cadastrados no Portal Jud para concessão de respectivo “login” e “senha”, os quais são pessoais e intransferíveis, permanecendo o usuário responsável pela correta e exclusiva utilização e pelo total sigilo destas informações.

1.4) Os servidores cadastrados serão responsáveis pelo lançamento da determinação judicial proferida por magistrado competente no sistema Portal Jud, para posterior aceite sistêmico por parte do magistrado designado para respectiva aprovação da consulta.

1.5) A consulta de dados cadastrais dos usuários, via “Portal Jud”, ocorrerá mediante prévia autorização do magistrado competente, nos autos do processo judicial a que se refere, ficando expressamente vedada a consulta para fins diversos, sob pena de responsabilização cível e criminal.

1.6) Consideram-se dados cadastrais a identificação do nome completo, RG, CPF/CNPJ, endereço do titular e código de acesso de determinada linha telefônica.

1.7) Os objetivos do presente Acordo de Cooperação Técnica são:

(i) Informatizar as solicitações judiciais oriundas do PODER JUDICIÁRIO para fornecimento de informações de dados cadastrais dos clientes da Vivo;

(ii) Reduzir/eliminar a troca de ofícios/correspondências em papel; e

(iii) Padronizar as consultas e levantamento do dado cadastral;

1.8) Todas as solicitações e/ou acessos ao "Portal Jud" da **VIVO** devem respeitar as instruções e especificações constantes no Anexo I (Especificações de uso do Portal Jud) do presente Acordo de Cooperação Técnica.

1.9) Todos os usuários do "Portal Jud" deverão firmar, sem exceção, "Termo de Aceitação", nos moldes do Anexo I do presente ajuste. Tal aceite será realizado "online", quando do primeiro acesso de cada usuário, conforme descrito no 4º passo do Anexo I (Especificações de uso do Portal Jud) e ficará registrado no banco de dados da **VIVO**.

1.10) A **VIVO** é titular sobre os direitos, inclusive de propriedade intelectual do "Portal Jud", e o presente Acordo de Cooperação Técnica não concede ao **TRT19** nenhum direito, título ou interesse de qualquer natureza com este sistema eletrônico, sendo que neste ato o **TRT19** reconhece a titularidade acima mencionada.

CLÁUSULA SEGUNDA- DAS OBRIGAÇÕES

2.1) o **TRT19**, sem prejuízo das demais obrigações estabelecidas no presente ajuste e documentos anexos, possui as seguintes obrigações:

a) Dispor de meios próprios, seguros e necessários para acesso ao sistema eletrônico "Portal Jud", tais como computadores aptos a utilizar a rede mundial de computadores e provedor de acesso à Internet, para obter acesso, via WEB, ao "Portal Jud".

b) Enviar à **VIVO**, nos termos disposto na cláusula primeira, item 1.3., bem como manter atualizada a relação dos magistrados e servidores públicos do **TRT19**, autorizados a acessar o sistema "Portal Jud" da **VIVO** a fim de viabilizar o cadastro dos mesmos, sempre que necessário.

c) O cumprimento das requisições judiciais exclusivamente de dados cadastrais, objeto do presente ajuste, somente será possível quando emanadas de magistrado de Direito nominalmente identificado nas respectivas requisições, assim como a indicação do número do processo judicial que autoriza cada requisição de dado cadastral.

d) Comunicar imediatamente a **VIVO** a substituição ou exclusão de servidor(es) e/ou magistrado (s) credenciado(s)na forma prevista no item 1.1 da cláusula primeira, evitando a utilização indevida do sistema "Portal Jud".

e) Utilizar as facilidades do presente Acordo de Cooperação Técnica exclusivamente nas atividades que, em virtude de lei, lhe compete exercer, com rigorosa observância dos deveres de sigilo e confidencialidade que lhe são inerentes, sob pena de

responsabilidade cível e criminal pelos danos causados, sem prejuízo da rescisão automática deste ajuste, por parte da **VIVO**, independentemente de prévio aviso.

f) Responsabilizar-se inteiramente pelo conhecimento, utilização e sigilo dos dados cadastrais requeridos, utilizando-os exclusivamente nos fins para os quais foram requisitados.

g) Divulgar o presente ajuste entre as unidades jurisdicionais de sua competência e estimular sua utilização, adotando os procedimentos necessários para reduzir/eliminar o envio de ofícios/correspondências em papel a **VIVO**, bem como orientar a emissão de ofícios deforma padronizada, caso ainda se façam necessários.

h) Preferencialmente promover as solicitações de dados cadastrais via sistema “Portal Jud”, sendo que as respectivas respostas, serão obtidas automaticamente via sistema.

i) A não divulgar para terceiros estranhos aos procedimentos aqui previstos o número de telefone 0800-7708486, indicado no item 2.2 alínea e, conforme abaixo descrito.

2.2) Cabe à **VIVO**, sem prejuízo das demais obrigações estabelecidas no presente Acordo de Cooperação Técnica e documentos anexos:

a) Manter em funcionamento o sistema objeto do presente ajuste.

b) Disponibilizar acesso ao sistema aos magistrados e/ou servidores do **TRT19**, desde que previamente credenciados e autorizados na forma prevista neste Acordo de Cooperação Técnica.

c) Fornecer ao **TRT19** relatórios estatísticos de acesso ao sistema de consulta de dados cadastrais, mediante prévio requerimento expresso assinado por seu representante.

d) Ressalva-se que a veracidade da informação cadastral, dependerá da correta indicação dos dados por seus titulares, sem que caiba à **VIVO** qualquer responsabilidade sobre a fidedignidade e veracidade dos mesmos.

e) Comunicar ao **TRT19** qualquer problema sistêmico que possa impactar ou impossibilitar o atendimento às determinações judiciais, designando desde já o telefone nº 0800-770-8486, da Divisão de Serviços Especiais, para dirimir dúvidas quanto ao cumprimento desde Acordo de Cooperação Técnica;

f) Compromete-se a promover, sempre que necessário e na medida de sua disponibilidade, capacitação aos magistrados e servidores usuários do sistema objeto deste ajuste.

CLÁUSULA TERCEIRA – DA VIGÊNCIA E DA PUBLICAÇÃO

3.1) Este Acordo de Cooperação Técnica entra em vigor na data de sua assinatura,

sendo de 5 (cinco) anos o prazo de vigência, renovável, automaticamente, pelo mesmo período.

3.2) A eficácia do presente Acordo de Cooperação Técnica fica condicionada à publicação do respectivo extrato no Diário Oficial da União, a qual deverá ser providenciada pelo TRT19 no prazo de até 20 (vinte) dias a contar da respectiva assinatura.

CLÁUSULA QUARTA– DA DENÚNCIA

4.1) O presente ajuste poderá ser denunciado de pleno direito, por qualquer um dos acordantes e a qualquer tempo, mediante aviso, por escrito, com antecedência mínima de 60 (sessenta) dias, sem qualquer ônus para os partícipes.

4.2) Em caso de alteração de endereços, os partícipes comunicarão a alteração nos 30 (trinta) dias subsequentes, sob pena de reputarem-se eficazes as correspondências remetidas para os endereços aqui referidos.

CLÁUSULA QUINTA - DO ACOMPANHAMENTO

5.1) Os partícipes indicarão representantes para acompanhar o desenvolvimento dos objetivos e metas, e se comunicarão por escrito, no curso da execução dos serviços, diretamente ou por quem vierem a indicar, e fiscalizar a fiel observância das disposições deste Acordo de Cooperação Técnica.

CLAÚSULA SEXTA - CUMPRIMENTO DAS LEIS DE COMBATE A CORRUPÇÃO

a) **O TRT19** se compromete, reconhece e garante que: Tanto o **TRT19**, como qualquer das sociedades ou pessoas que a controlam, assim como suas controladas, seus sócios, representantes legais, administradores, empregados e agentes relacionados de alguma maneira com o Compromisso Relevante[1], cumprirão a todo momento durante o Compromisso Relevante (incluindo, se for ocaso, a aquisição dos produtos e/ou conteúdo que estiverem relacionados com o fornecimento de bens e/ou prestação de serviços objeto deste contrato) com todas as leis, estatutos, regulamentos e códigos aplicáveis em matéria de combate à corrupção, incluindo, em qualquer caso e sem limitação, a Lei Anticorrupção no Exterior, dos Estados Unidos (Foreign Corrupt Practices Act – FCPA) (coletivamente, “Leis de Combate à Corrupção”);

b) em relação ao Compromisso Relevante, o **TRT19**, as sociedades ou pessoas que a

[1]Compromisso Relevante” é o objeto deste contrato.

controlam, suas controladas, seus sócios, representantes legais, administradores, empregados e agentes, não oferecerão, prometerão ou entregarão, ou, antes da assinatura deste contrato, já ofereceram, prometeram ou entregaram, direta ou indiretamente, dinheiro ou objetos de valor a(i) "Funcionário Público"[2] afim de influenciar em suas ações ou junto a determinado órgão público ou, de alguma forma, para obter uma vantagem indevida; (ii) qualquer outra pessoa, caso tenha conhecimento que todo ou parte do dinheiro ou do objeto de valor será oferecido ou entregue a Funcionário Público a fim de influenciar em suas ações ou junto a determinado órgão público ou, de alguma forma, para obter uma vantagem indevida; ou (iii) qualquer outra pessoa a fim de induzi-la a agir de maneira desleal ou, de alguma forma, inapropriada;

c) o **TRT19** possui, e manterá em vigor durante a vigência deste contrato, políticas e/ou procedimentos próprios para assegurar o cumprimento das Leis de Combate à Corrupção, e suficientes para garantir de forma razoável que violações às Leis de Combate à Corrupção sejam prevenidas, detectadas e dissuadidas;

d) o **TRT19** comunicará de imediato à **VIVO** eventual descumprimento de qualquer das obrigações descritas nas letras (a), (b) e (c) desta Cláusula. Caso ocorra tal descumprimento, a **VIVO** se reserva o direito de exigir do **TRT19** a adoção imediata de medidas corretivas apropriadas;

e) as manifestações, garantias e compromissos do **TRT19** constantes nesta Cláusula serão aplicáveis na sua totalidade a qualquer terceiro sujeito ao controle e influência do **TRT19**, ou que atue em seu nome, com relação ao Compromisso Relevante; de forma que o **TRT19** manifesta que adotou todas as medidas razoáveis para assegurar o cumprimento das manifestações, garantias e compromissos por parte desses terceiros. Além disso, nenhum direito ou obrigação, assim como nenhum serviço a ser prestado pelo **TRT19** com relação ao Compromisso Relevante, será cedido, transferido ou subcontratado a qualquer terceiro sem o prévio consentimento por escrito da **VIVO**;

f) o **TRT19** certificará periodicamente que cumpre com esta Cláusula sempre que solicitado pela **VIVO.**

6.1) Descumprimento.

a) O descumprimento desta Cláusula de "Cumprimento das Leis de Combate à Corrupção" será considerado um descumprimento contratual grave.

[2]Funcionário Público" inclui qualquer pessoa que trabalhe para ou em nome de um órgão do governo federal, estadual, municipal ou distrital, da administração direta ou indireta (incluindo empresas de propriedade ou controladas pelo governo) ou qualquer organização pública internacional.
Esta expressão inclui também partidos políticos, empregados de partidos e candidatos a cargos públicos.

Na hipótese de ocorrer tal descumprimento, exceto se o mesmo for corrigido conforme disposto na letra (e) desta Cláusula, este contrato poderá ser imediatamente suspenso ou rescindido pela **VIVO**, e a **VIVO** não será obrigada a pagar qualquer valor devido ao **TRT19.**

b) Na medida do permitido pela legislação aplicável, o **TRT19** indenizará e isentará a **VIVO** de toda e qualquer reivindicação, danos, perdas, prejuízos, penalizações e custos (incluindo, mas não se limitando, honorários advocatícios) e de qualquer despesa decorrente ou relacionado ao descumprimento por parte do **TRT19** de suas obrigações contidas nesta Cláusula de "Cumprimento das Leis de Combate à Corrupção".

6.2) A **VIVO** terá o direito de auditar o cumprimento, por parte do TRT19, de suas obrigações e manifestações constantes na presente Cláusula de "Cumprimento das Leis de Combate à Corrupção". O **TRT19** cooperará totalmente com qualquer auditoria, revisão ou investigação realizada pela VIVO ou em nome desta.

CLÁUSULA SÉTIMA- DO ADITAMENTO

7.1) O presente Acordo de Cooperação Técnica poderá ser modificado de comum acordo entre as partes, mediante Termo Aditivo, desde que não haja mudanças no objeto do mesmo.

CLÁUSULA OITAVA- DO ÔNUS

8.1) Cada partícipe arcará com o ônus relativo às suas respectivas obrigações.

8.2) De imediato, a implementação do presente Acordo de Cooperação Técnica não gera quaisquer ônus financeiros entre os partícipes.

8.3) Os recursos humanos eventualmente utilizados por quaisquer dos partícipes, no âmbito da execução do ajuste, permanecerão vinculados à sua origem, sem gerar qualquer vínculo funcional ou encargo para o outro partícipe.

CLÁUSULA NONA – DAS DISPOSIÇÕES GERAIS

9.1) As informações contidas no "Portal Jud" estão abrangidas pelo sigilo de dados, nos termos do artigo 5º, inciso X da Constituição Federal, artigos 3º incisos V, VI, IX, XII, 39 e artigo 72 §1º e §2º da Lei n. 9.472/97, sendo-lhes dado o tratamento estabelecido na legislação correlata e demais regulamentações.

9.2) O acesso ao “Portal Jud” por usuários credenciados está baseado em procedimentos de validação e de autenticação, com a utilização de identificadores institucionais e pessoais e de senhas individuais exclusivas e intransferíveis.

9.3) O presente Acordo de Cooperação Técnica corresponde à totalidade do ajuste firmado entre seus partícipes, não prevalecendo, para qualquer efeito, outras manifestações de vontade eventualmente expressas, salvo se decorrente de lei ou norma regulamentar aplicável.

9.4) Os casos omissos ou quaisquer divergências decorrentes da execução deste Acordo de Cooperação Técnica serão resolvidos pelos partícipes por meio de consulta e mútuo entendimento, observadas as disposições de leis e regulamentos aplicáveis e os princípios gerais de Direito.

9.5) Caberá ao **TRT19** fiscalizar a fiel observância das disposições deste Acordo de Cooperação Técnica e das instruções constantes nos Anexos I, II, III, IV e V, sem prejuízo da fiscalização a ser exercida pela **VIVO**.

9.6) A **VIVO** não se responsabilizará por qualquer desconformidade das informações constantes em seu cadastro, por ser composto por informações prestadas por terceiros, a quem cabe responsabilidade sobre as mesmas.

CLÁUSULA DÉCIMA–DO FORO

10) Para as que questões divergentes que surjam do presente Acordo de Cooperação Técnica, não resolvidas na esfera administrativa, os integrantes elegem o Foro da Comarca da Capital de Maceió, renunciando a qualquer outro, por mais privilegiado que seja.

E, por estarem ajustadas e de acordo, as partes, por seus representantes legais, firmam o presente Acordo de Cooperação Técnica em 02(duas) vias, de igual forma e teor, para que surta seus jurídicos e legais efeitos, juntamente com 02 (duas) testemunhas.

Maceió, data da última assinatura eletrônica.

JASIEL IVO - Desembargador Presidente
TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO

Fernanda Fortunato Martins Chaguri
FERNANDA FORTUNATO MARTINS CHAGURI

PATRICIA ANDREA TEDESCO GODOI
PATRÍCIA ANDREA TEDESCO GODOI

TELEFONICA BRASIL S.A. (VIVO)

Testemunhas: Cleverson Cronemberger Martins

1 - ----------
Cleverson Cronemberger Martins CPF: 350.737.078-69

Rodolfo Comar

2 - ----------
Rodolfo Comar CPF: 299.301.138-35

ANEXO I - TERMOS E CONDIÇÕES DE USO DO "PORTALJUD"

Este Termo e Condições de Uso (doravante denominado "TERMO") aplicam-se aos serviços oferecidos pela TELEFONICA BRASIL S.A (doravante denominada "VIVO") por meio do sistema denominado PORTAL JUD, aos USUÁRIOS previamente cadastrados, permitindo-lhes realizar upload de ofícios expedidos pelas autoridades competentes e consultar a base de dados contidas nos sistemas da VIVO, limitadas à ação judicial ou ao procedimento investigatório objeto da consulta.

Ao aceitar este TERMO, o USUÁRIO adere e concorda integralmente com os termos e condições aqui estabelecidos, incluindo quaisquer alterações futuras, bem como aceitar as disposições abaixo descritas:

O USUÁRIO declara aceitar as condições de uso do PORTAL JUD da VIVO e assume integralmente a responsabilidade pelos seus atos, nos seguintes termos:

1. CONDIÇÕES GERAIS DE USO DO PORTAL JUD

O USUÁRIO concorda expressamente em:

(i) Ser exclusiva e integralmente responsável pela utilização das senhas e consultas realizadas no sistema;

(ii) Ter ciência de que as informações disponibilizadas no sistema PORTAL JUD são revestidas de caráter sigiloso e seu uso é restrito aos processos e/ou procedimentos objeto da consulta;

(iii) Acessar o PORTAL JUD exclusivamente através do sistema operacional Windows 32 bits (versão 2000 ou superior), sendo que a utilização de quaisquer outros sistemas operacionais será de total e exclusiva responsabilidade do USUÁRIO;

(iv) A VIVO não se responsabiliza por quaisquer problemas de interrupção dos serviços disponibilizados por meio do PORTAL JUD por motivos alheios à sua vontade e/ou de seus prestadores de serviço, incluindo, sem limitação, fornecimento de energia e queda de conexão discadas ou dedicadas, com os provedores de conexão;

(vi) O acesso é protegido por um segundo fator de segurança, que pode ser acionado por meio do envio de token para o e-mail ou telefone celular do USUÁRIO ou gerado via Google Authenticator, o qual deve ser configurado previamente pelo USUÁRIO;

(vii) Dúvidas sobre a utilização do sistema poderão ser sanadas via contato telefônico, através do plantão de atendimento 0800-770.8486.

(viii) Ter lido e estar ciente e de pleno acordo com todos os termos e condições deste TERMO, razão pela qual o aceita de livre e espontânea vontade.

2. NÃO DIVULGAÇÃO A TERCEIROS

O USUÁRIO deste sistema deverá considerar como confidenciais e sigilosas as informações obtidas por meio dele, ficando impedido de divulgá-las a terceiros, bem como de utilizá-las para fins diversos da respectiva ordem judicial autorizadora ou dos termos do Acordo de Cooperação Técnica firmado, ou ainda para fins diversos das investigações conduzidas, ficando obrigado a zelar pela informação como se fosse seu

titular.

3. CONDIÇÕES DA CONSULTA

O USUÁRIO deste sistema será responsável pelo acesso ou consulta não autorizada, sendo obrigatória a identificação em cada consulta da respectiva ordem judicial autorizadora ou do Acordo de Cooperação Técnica firmado, informações estas que estarão previamente cadastradas pela VIVO para credenciamento do USUÁRIO.

4. PENALIDADES

A não observância de quaisquer disposições contidas neste Termo sujeitará o USUÁRIO, e, se for o caso, solidariamente ao agente causador ou facilitador, por ação e/ou omissão, responsabilização civil, criminal e administrativa decorrentes da violação deste termo, bem como pela violação de direitos e garantias fundamentais dos clientes da VIVO, sem prejuízo do pagamento de indenização e/ou recomposição de todas as perdas e danos comprovados, nos termos da legislação em vigor.

Adicionalmente, a VIVO estará autorizada a advertir o USUÁRIO e/ou suspender, por tempo indeterminado, as senhas de acesso a este sistema e/ou o Acordo de Cooperação Técnica firmado, sem que lhe seja imputada qualquer responsabilidade por eventuais prejuízos causados ao USUÁRIO em decorrência do uso indevido do sistema.

5. PRIVACIDADE

A garantia à privacidade das informações dos USUÁRIOS no PORTALJUD é um compromisso da VIVO, que não fornecerá as informações do USUÁRIO, obtidas para fins de cadastramento no sistema PORTAL JUD, a terceiros sem prévia autorização do mesmo, salvo por obrigação legal, em cumprimento às determinações judiciais.

6. LEI APLICÁVEL E FORO

O presente instrumento é regido pelas leis da República Federativa do Brasil, bem como pelos tratados e acordos internacionais dos quais a República Federativa do Brasil seja signatária.

As Partes elegem o Foro estabelecido no termo de Acordo de Cooperação Técnica firmado entre as partes para dirimir quaisquer dúvidas ou questões oriundas deste TERMO. Na ausência de previsão expressa no Acordo de Cooperação Técnica, será observada a regra de competência de cada estado da Federação, com menção expressa a qualquer outro foro, por mais privilegiado que seja.

ANEXO II –TERMO DE TRATAMENTO DE DADOS PESSOAIS

1. OBJETIVO

Este Termo de Tratamento de Dados Pessoais (“Termo”) se aplica aos tratamentos de dados pessoais realizados em razão de Contrato de Prestação de Serviços e/ou Fornecimento (“Contrato”), celebrado por e entre CONTRATANTE e CONTRATADA, ambas definidas no Contrato, e o integra para todos os fins de direito.

2. DEFINIÇÕES

A CONTRATANTE e a CONTRATADA são doravante designadas, em conjunto, “Partes” e, individualmente, “Parte”.

Não obstante qualquer disposição em contrário no Contrato, no caso de qualquer ambiguidade ou conflito entre os demais documentos integrantes do Contrato e deste Termo, os termos e condições deste Termo prevalecerão.

Quaisquer termos iniciados em letras maiúsculas e não definidos de outra forma neste Termo terão o significado atribuído a eles no Contrato. Exceto conforme modificado abaixo, os termos do Contrato permanecerão em pleno vigor e efeito.

“Controlador”: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

“Dado Pessoal”: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa, bem como nome, prenome, estado civil, filiação e endereço, e-mail, telefone.

“Encarregado”: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

“**Leis Aplicáveis**”: toda a legislação brasileira, incluindo leis, regulamentos, regras, ordens, decretos ou outras diretrizes com força de lei, relacionadas à proteção de dados e que sejam aplicáveis às Partes.

“Operador”: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

“Subcontratação”: ato de contratar Subcontratados.

“Subcontratados”: os subcontratados, representantes e outros prestadores de serviços terceirizados, pessoa natural ou jurídica, que tenham acesso a Dados Pessoais relacionados à execução do Contrato.

“Titular”: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

“Tratamento”: toda operação realizada com dados pessoais, como as que se referem 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.

3. OBRIGAÇÕES SOBRE A PROTEÇÃO DE DADOS

3.1. As Partes, para os Tratamentos de Dados Pessoais definidos por este Contrato, assumirão, ambas, o papel de Controladores de Dados Pessoais, não respondendo uma a outra, sob nenhuma hipótese, como Operador.

3.2. As Partes se comprometem a:

3.2.1. Cumprir com as Leis Aplicáveis, em especial a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), realizando os tratamentos única e exclusivamente com o objetivo de assegurar o cumprimento do objeto do presente Contrato.

3.2.2. Observar as Leis Aplicáveis, em especial a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), respondendo as Partes, na medida de sua culpabilidade, por eventuais prejuízos, penalidades e condenações, inclusive para as hipóteses ocorridas por força de atuação de qualquer autoridade fiscalizadora ou agência governamental de proteção de dados.

3.2.3. Nomear um Encarregado, de acordo com os critérios estabelecidos pelas Leis Aplicáveis.

3.2.4. Estabelecer e cumprir medidas técnicas e organizacionais internas para o tratamento, visando o cumprimento dos requisitos legais para o tratamento.

3.2.5. Respeitar e atender aos direitos dos Titulares, sendo cada parte responsável pela comunicação e respostas referentes ao seu Tratamento de Dados Pessoais.

3.2.6. Colaborar entre si para responder a quaisquer solicitações e/ou demandas de titulares de dados e/ou da Autoridade Nacional de Proteção de Dados, bem como em caso de incidentes de segurança.

3.2.7. Se responsabilizar, integralmente, por Subcontratações que possam existir, respondendo à outra parte pelos atos de seus subcontratados, com se seus fossem.

ANEXO III-SEGURANÇA DIGITAL

1. **Das Políticas, Normas e Procedimentos de Cibersegurança e Garantia de Segurança de Dados e/ou Informações**

1.1. A CONTRATADA garante possuir e cumprir a segurança das informações em seu ambiente, em um modelo sustentável de gerenciamento de Segurança Digital com a aplicação de políticas e normas, assegurando a integridade, a confidencialidade, a disponibilidade e segurança, das informações e dos seus respectivos sistemas, tanto fisicamente quanto logicamente, implementando todas as medidas técnicas, processuais e/ou organizações para cumprimento desse Anexo de Segurança. A CONTRATADA também é responsável pelo cumprimento das regras de segurança da Vivo quando a CONTRATADA acessa as informações e os sistemas da Vivo (incluindo, quando aplicável, o software utilizado pela CONTRATANTE, onde a CONTRATADA foi o desenvolvedor).

1.2. Durante o acesso às informações ou sistemas em ambientes da CONTRATANTE, inclusive no exercício do papel de desenvolvedora, a CONTRATADA se responsabiliza também pelo cumprimento integral das regras de segurança da CONTRATANTE.

1.2.1. Eventuais custos relacionados a manutenção do sistema de gestão e controles de segurança da informação e proteção de dados, incluindo, quando aplicável, a recuperação de informações, sistemas ou infraestruturas, serão de total responsabilidade da CONTRATADA.

2. **Privacidade, Proteção de Dados e Segurança da Informação**

2.1 Todos os dados e/ou informações de propriedade e/ou controle da CONTRATANTE que a CONTRATADA tiver acesso no exercício das suas obrigações, independentemente do tipo do ativo de informação, senão públicos, para todos os efeitos são considerados confidenciais e, portanto, somente poderão ser utilizadas em observância à finalidade do cumprimento do presente contrato devidamente acompanhado do NDA (Non Disclosure Agreement/ Acordo de Não Divulgação) assinado.

a - Dada a propriedade, restrição e finalidade acima descritas, a CONTRATADA assegura, em nenhuma circunstância, utilizar dados e/ou informações da CONTRATANTE e/ou de seus clientes para benefício próprio e/ou de terceiros.

2.2 A CONTRATADA se compromete em cooperar com a CONTRATANTE para responderaseventuaissolicitaçõesquetenhamporobjetivooexercíciodosdireitosdos titulares de dados, especificados na legislação vigente de Proteção de Dados, dentre eles os que se referem, mas não se limitam à transparência, à informação, ao acesso, à retificação, à exclusão (direito ao esquecimento), à limitação e/ou à oposição ao tratamento, bem como a possibilidade de portabilidade de seus dados e/ou informações.

2.3 A CONTRATADA garante que não compartilhará, não realizará cópias e/ou integrações em seus ambientes (físicos e/ou digitais), nem de outra forma divulgará os dados e/ou informações da CONTRATANTE e/ou de seus clientes, e, tampouco, permitirá o tratamento destes por seus representantes, subcontratados e/ou terceiros, salvo se:

a- Houver a necessidade de se tomar conhecimento, para fins de fornecimento dos produtos e serviços contratados;

b- Até o limite necessário para fornecimento do que foi contratado;

c- Permitido segundo os contratos aplicáveis e formalizados;

d- For exigido de acordo com a legislação aplicável.

2.4 Caso exista a necessidade de a CONTRATADA transferir, compartilhar, divulgar e/ou permitir o tratamento de dados da CONTRATANTE por terceiros, deverá, prévia e formalmente, notificar a CONTRATANTE solicitando para que conceda sua anuência.

2.5 As informações e/ou dados de propriedade da CONTRATANTE e seus clientes devem estar classificados e rotulados, com medidas de proteção aplicadas em todo o ciclo de vida da informação, istoé, desde a criação/coleta até o descarte pela CONTRATADA, seguindo as seguintes premissas:

2.5.1 Criação ou Coleta dos dados e/ou informações:

2.5.1.1 A CONTRATADA se compromete, para fins de classificação e rotulação das informações, seguir as seguintes recomendações elencadas

abaixo:

a- RESERVADA: informações altamente sensíveis e críticas ao negócio que, devido à sua relevância, devem ser protegidas com mecanismos de segurança que garantam o acesso autenticado com autorização expressa e nominativa da fonte e sua distribuição é limitada a um pequeno grupo de funcionários. Por exemplo: projetos em desenvolvimento, decisões estratégicas, impacto financeiro, oportunidades de negócios, potencial de fraude, requisitos legais etc.

b- USO INTERNO RESTRITO: informações sensíveis e críticas ao negócio para as quais são estabelecidos mecanismos de segurança para garantir o acesso autenticado e que somente são acessadas e utilizadas por funcionários, bem como por contratados e terceiros envolvidos, mediante compromisso de confidencialidade (NDA). Deve ser protegido devido ao seu impacto sobre os interesses da empresa, de seus clientes ou parceiros e dos funcionários. Por exemplo: documentos técnicos de configurações de segurança, atas de comitês etc.

c- USO INTERNO: informação que, sem reserva ou restrição, deve ser mantida no âmbito interno do contrato e não deve ser divulgada ou disponibilizada externamente.

2.5.2 Armazenamento de dados e/ou informações:

a- As informações e/ou dados da CONTRATANTE devem ser armazenados em diretórios/bancos exclusivos e segregados, seguindo todas as regras determinadas nesse anexo. Em nenhuma hipótese a CONTRATADA deverá armazenar informações em seu ambiente, salvo se for objeto expresso deste contrato tal modelo.

b- O armazenamento em Nuvem está autorizado somente na modalidade Privada, para todas as infraestruturas do escopo do contrato, independente da Classificação da Informação e/ou tipo de informações;

c- Dados e/ou informações classificados como uso interno restrito ou reservados devem ser armazenados com criptografia;

d- A gestão dos acesos às informações armazenadas em nuvem deverá ser constituída seguindo todas as regras estabelecidas pela CONTRATANTE

por meio dos seus times de TI e Segurança.

2.5.3 Processamento de dados e/ou informações:

2.5.3.1 A CONTRATADA se compromete que em todo tipo processamento de dados e/ou informações decorrentes do objeto do presente contrato, deve conter medidas técnicas, processuais e organizacionais seguras, sendo desenvolvidas e configuradas de maneira a robustecer e garantir a segurança deles, observados todos os requisitos contidos neste anexo.

2.5.3.2 Independentemente do tipo de ativo de informação, o processamento dos dados deverá ser realizado de forma segura conforme descrito na clausula anterior. A validação do conceito “segura” deverá ser realizada junto ao time de Segurança da CONTRATANTE anteriormente a implementação de quaisquer soluções, a fim de que se identifique medidas técnicas e/ou processuais a serem implementadas desde a concepção para salvaguarda das informações. Fica firmado que a inobservância desta clausula, obrigará a CONTRATADA a realizar todos os ajustes necessário sem soluções utilizadas no processamento de dados e/ou informações que não atendam os requisitos de segurança e proteção dos dados, no tempo estipulado pela CONTRATANTE, independentemente do meio (parametrizações, configurações e/ou desenvolvimento) e tempo/momento da identificação, sem quaisquer custos à CONTRATANTE.

2.5.3.3 A inobservância do presente capítulo, poderá ainda acarretar à CONTRATADAS penalidades por descumprimento aos requisitos de segurança e proteção dos dados, inclusive acerca de quaisquer danos que tenha causado à CONTRATANTE, seja por dolo ou culpa e independentemente de notificação prévia.

2.5.3.4 Transferência de dados e/ou informações:

2.5.3.5 A CONTRATADA assume que em qualquer modalidade de comunicação, integração e/ou transferência de dados e/ou informações, haverá a aplicação da Triple A (Authentication (Autenticação), Authorization (Autorização) and Accounting (Responsabilização), além da utilização de técnicas de criptografia, anonimização/mascaramento dos dados e/ou quaisquer outras medidas de segurança que se fizerem necessárias para garantirem a segurança e proteção dos dados e informações durante

eventual transferência, sem prejuízo ainda, de prévia anuência, conforme já disposto nos itens 2.3 e 2.4 deste anexo.

2.5.3.6 A CONTRATADA se compromete em envolver a CONTRATANTE prévia, formalmente e em tempo hábil, sempre que houver a necessidade de transferência internacional de dados pessoais e/ou pessoais sensíveis, decorrente do objeto de sua prestação de serviço, a fim de garantir o atendimento à LGPD e/ou GDPR.

2.5.4 Descarte dos dados e/ou informações:

2.5.4.1 A CONTRATADA se compromete que, quando do término do presente contrato, ou ainda, em cumprimento de solicitação feita pela CONTRATANTE, todos e quaisquer dados e/ou informações de propriedade da CONTRATANTE ou de seus clientes, obtidos, processados, armazenados e/ou transmitidos em cumprimento à execução do objeto deste contrato, serão completamente destruídos com uso de medidas técnicas, processuais e organizacionais a garantir o descarte seguro e a impossibilidade de restauração.

2.5.4.2 As mídias óticas e/ou eletrônicas, tanto as fixas como as removíveis, que contenham dados e/ou informações da CONTRATANTE ou de seus clientes, quando não forem mais utilizadas, requerem os seguintes cuidados no descarte, os quais a CONTRATADA assume observar e cumprir:

a- Identificar e registrar as mídias que requerem descarte seguro, tais como fitas de backup, discos rígidos, DVDs, impressos e outros;

b- Triturar, incinerar ou inutilizar as mídias para que os dados não possam ser recuperados;

c- Os serviços terceirizados de coleta e descarte de papel, de equipamentos e de mídias magnéticas, devem ser efetuados por fornecedor com experiência comprovada e controles de segurança adequados;

d- Em último caso, quando não possível a observância dos itens acima, as informações deverão ser todas devolvidas pela CONTRATANTE à CONTRATADA, íntegras e integralmente, para que sejam devidamente descartadas.

e – Independentemente do meio, a CONTRATADA se compromete a não realizar quaisquer cópias para que seja mantida em sua posse, transferida a terceiros ou ainda, utilizada em benefício próprio e assume que arcará com as penalidades cabíveis se esse cenário se concretizar.

2.6 Rescisão do Contrato: proteção dos dados e/ou informações

2.6.1 Quando da rescisão do presente contrato ou mediante solicitação por escrito da CONTRATANTE, o que ocorrer primeiro, a CONTRATADA cessará imediatamente e garantirá que seus subcontratados, quando houver, cessem imediatamente, todo e qualquer uso de dados e/ou informações da CONTRATANTE, devolvendo-os, descartando-os, destruindo-os ou tornando-os anônimos de forma permanente, a depender do pedido da CONTRATANTE, utilizando para tanto, em cada caso, as medidas de segurança aplicáveis e necessárias, sejam elas técnicas, processuais e/ou organizacionais.

a- Se a legislação vigente e aplicável não permitir que a CONTRATADA destrua ou descarte os dados e/ou informações da CONTRATANTE, a CONTRATADA declara que não usará essas informações para nenhuma outra finalidade que não seja a que se encontra na obrigação legal ou regulatória e nos contratos aplicáveis, bem como que manifestará por escrito à CONTRATANTE tal impossibilidade assim que tomar ciência.

2.6.2 As empresas terceiras, parceiras ou subcontratadas da CONTRATADA, que foram expressamente autorizadas a utilizar os dados e/ou informações da CONTRATANTE em cumprimento ao objeto deste contrato, devem respeitar as cláusulas definidas neste Anexo de Segurança, assumindo, por meio deste, a CONTRATADA tal responsabilidade de se fazer cumprir.

3. Requisitos de Segurança Digital

3.1. A CONTRATADA deve seguir padrões de segurança e arquiteturas de referência adequadas de acordo com os requisitos de Segurança Digital disponibilizados pela CONTRATANTE para todos os sistemas e/ou aplicações próprias que serão desenvolvidas para cumprimento do objeto deste contrato, que manipulem dados ou informações da CONTRATANTE.

Com o objetivo de garantir os seguintes princípios: confidencialidade, integridade e disponibilidade. O objetivo é apresentar os padrões e premissas arquitetônicas para o desenvolvimento e manutenção segura de sistemas que manipulem, transmitam ou armazenem informações da CONTRATANTE.

3.2. Caso seja necessário o desenvolvimento, aquisição de novas ou utilizar soluções da CONTRATADA, esta mesma deverá solicitar a CONTRATANTE, via seu gestor de contrato a análise de riscos por Segurança Digital para aprovação prévia. A solução somente deverá ser utilizada em produção após a aprovação da CONTRATANTE.

3.3. A CONTRATADA deverá ter ciência e cumprir os requisitos estabelecidos nos documentos anexos no item 3.5 deste documento.

3.4. Todos os entregáveis, incluindo o desenvolvimento, produzido para e/ou fornecido para a CONTRATANTE como parte dos serviços efetuados pela CONTRATADA ou qualquer subcontratado da CONTRATADA que estão cobertos sobre a lei de direitos sobre propriedade intelectual (direito de propriedade industrial, literário e artístico) devem, em respeito ao código de propriedade intelectual Brasileiro, serem atribuídos exclusivamente à CONTRATANTE.

3.5. A CONTRATADA deverá garantir que os seguintes requisitos mínimos sejam contemplados e implementados, conforme requisitos disponíveis no item 17.1 Ciência e Aceite:

Requisitos de segurança para RPAs;

Requisitos de Segurança para Arquitetura de Sistemas; Requisitos de Segurança para Cloud;

Requisitos de Segurança para Desenvolvimento Seguro.

4. Gestão de Incidentes de Segurança

4.1. A CONTRATADA notificará, através do canal de denúncias: CSIRT Vivo Brasil (csirt.br@telefonica.com), prontamente a CONTRATANTE sobre qualquer fato que comprometa a segurança da informação, tanto fisicamente quanto logicamente (por exemplo, tentativas de invasão, roubo

e vazamento de informações, novas vulnerabilidades e incidentes de segurança da informação) e 1tomará todas as medidas necessárias para corrigir a situação e manter a segurança de todas as informações da CONTRATANTE, durante e após a vigência do Contrato.

4.1.1. O reporte a CONTRATANTE comunicando a ocorrência do incidente deverá ser imediato, ou seja, logo após tomada de conhecimento.

4.2. A CONTRATADA deve garantir que os logs para análise ou perícia estejam disponíveis quando solicitados pela CONTRATANTE.

5. Controles de auditoria e revisão de atividades de sistemas de informação

5.1. A CONTRATANTE poderá anualmente, por si próprio ou usando uma auditoria terceira, realizar auditoria e/ou assessment de segurança a fim de garantir que o prestador de serviços está cumprindo com suas obrigações, mantendo o sistema de gestão de segurança e/ou garantindo a segurança da infraestrutura, mas também para responder a qualquer pedido feito por uma autoridade judicial ou administrativa.

5.2. As avaliações podem ser realizadas presencialmente, caso apropriado, e as visitas serão agendadas previamente.

5.3. No caso em que o relatório revele uma quebra significativa das obrigações da CONTRATADA na prestação dos serviços do presente Contrato, a CONTRATADA será informada via emissão do relatório e deverá implementar todas as medidas corretivas necessárias, sem qualquer custo à CONTRATANTE, no prazo de trinta (30) dias da data em que o descumprimento foi informado pela CONTRATANTE.

5.4. Durante o período de avaliação ou auditoria os níveis acordados de serviço não podem ser alterados.

5.5. Será necessário também que a CONTRATADA realize um teste de invasão no ambiente e serviço em escopo do fornecimento da CONTRATANTE e os resultados e planos de correção devem ser compartilhados com a

CONTRATANTE.

5.6. A CONTRATANTE quando for necessário deverá ter acesso a registros e logs que identifiquem todas as ações realizadas pelos colaboradores da CONTRATADA de forma que seja possível identificar qual foi o operador e suas respectivas ações visando (data/hora) e qual equipamento foi utilizado.

5.6.1. Os arquivos, registros e logs devem ser armazenados de forma segura e possuir restrição de acesso, principalmente nos casos de permissão de alteração ou exclusão. O acesso à leitura dos arquivos, registros e logs devem ser restritos aos usuários autorizados seguindo as orientações previstas em “Controle de acesso e gerenciamento de identidade”.

5.7. A CONTRATANTE também poderá realizar avaliações técnicas, mediante agendamento com a CONTRATADA. Os testes serão realizados apenas no escopo do serviço prestado. Caso sejam identificados pontos de correção, a CONTRATADA deve seguir o prazo abaixo para correção:

Tipo vulnerabilidade	**SLA esperado de Correção**
Crítica	5 dias
Alta	8 dias
Moderado	30 dias
Médio	60 dias
Leve	90 dias

(*) Vulnerabilidades V0 é a categoria criada pela CONTRATANTE para identificar vulnerabilidades iminentes de risco reputacional, riscos financeiros e/ou perda ou vazamento de informações, que por sua vez se tornam mais relevantes que vulnerabilidades classificadas como críticas. Para cada vulnerabilidade V0 e vulnerabilidades críticas identificadas no ambiente do escopo dos serviços prestados e não corrigidas nos prazos determinados acima poderá ser aplicada multa contratual conforme clausula 14 “Penalidades” deste anexo.

6. Controle de acesso e gerenciamento de identidade

6.1. Para sistemas em que a CONTRATANTE fornecerá acesso a CONTRATADA, as regras serão as mesmas utilizadas nas políticas vigentes para a CONTRATANTE. Para sistemas que a própria CONTRATADA faz a gestão de acessos deverão ser implantados os controles de acessos que garantam não repúdio dos acessos e logs para investigação posterior, caso solicitado pela CONTRATANTE.

6.2. As regras de controle de acesso devem respeitar revisões periódicas de acessos e perfis, senhas complexas, revogação de acesso e logs conforme estabelecidos nas políticas atualmente praticadas pela CONTRATANTE. Não deve existir nenhum processo ou função que altere ou apague qualquer registro da trilha de auditoria, salvo o script de retenção. Os registros de auditoria devem ser armazenados por no mínimo 90 dias (online) e devem suportar o prazo de retenção padrão definidos pela legislação atual.

6.3. Caso a CONTRATADA tenha acesso a dados críticos sensíveis, como, por exemplo, dados de sigilo telefônico ou dados sensíveis de pessoas físicas, a CONTRATANTE se reserva o direito de exigir medidas adicionais de segurança para colaboradores e computadores e a CONTRATADA não deverá realizar consultas de forma massiva. As medidas incluem, mas não se limitam a:

6.3.1. Treinamentos de Segurança Digital para os colaboradores;

6.3.2. Bloqueio do acesso à internet e restrições nas máquinas, liberando somente as ferramentas corporativas essenciais para execução das atividades;

6.3.3. Ferramentas de monitoramento.

6.3.4. Garantias de execução de controles que do ciclo de vida dos usuários.

6.4. A CONTRATADA deve seguir todos os controles referente à gestão de acessos lógicos, conforme determinado pela CONTRATANTE, tais como:

6.5. Gestão do Ciclo de Vida dos Acessos Lógicos

6.5.1. Acessos lógicos são os acessos a sistemas, softwares e ambientes da CONTRATANTE. Acessos lógicos envolvem as credenciais de acesso

(usuário, senha, e duplo fator de autenticação, caso aplicável), que permitem acesso pelos contratados aos sistemas da CONTRATANTE.

6.5.2. A CONTRATADA deverá ter ciência e cumprir os requisitos descritos nos procedimentos estabelecidos pela Gestão de Aliados, quanto ao processo de geração, manutenção e inativação de cadastro para aliados no sistema de Gestão de Aliados.

6.5.3. A CONTRATADA é responsável pelo ciclo de vida dos usuários (cadastro, atualização, revisão, férias, afastamento e desligamentos) pela acuracidade dos dados cadastrais imputados no sistema de Gestão de Aliados, grupo responsável por orientações (SAP GT). O Gestor da área CONTRATANTE é responsável por validação e acompanhamento contínuo dos cadastros gerados pela CONTRATADA, assim como, pela manutenção e inativação dos registros, conforme normativa interna. Será também responsável por prover as informações de cadastro de forma verídica dos campos solicitados no Sistema SAP GT.

6.5.4. A CONTRATADA deve realizar o desligamento imediato de aliados que estejam ausentes nas operações da Telefônica Brasil devido licença, afastamento ou férias em como, realizar as transferências de área, cargo e de qualquer atualização que se fizer necessária de todo e qualquer cadastro de usuário que possua acesso em sistemas da CONTRATANTE, com suas devidas revisões e revogações de acesso quando aplicáveis decorrentes dessa movimentação, através do Sistema de Gestão de Aliados, grupo responsável por orientação (SAP GT) tempestivamente. Tal procedimento se faz necessário por razões de segurança de dados.

6.5.5. A CONTRATADA deve responder as revisões das certificações sempre que solicitado pela CONTRATANTE dentro do prazo estabelecido pela CONTRATANTE. Apenas os acessos necessários para a função atual do colaborador devem permanecer liberadas. Não é permitido delegar esta atividade para outro colaborador que não tiver a função de gestão dos usuários.

6.5.6. Cumprir o SLA de até 1 (um) dia útil para comunicar todas as ações do ciclo de vida dos usuários, conforme citado acima.

6.6. Uso Das Senhas e Credenciais De Acessos

6.7. No que tange ao uso das senhas, a CONTRATADA deve cumprir os requisitos abaixo:

6.7.1. As senhas são pessoais e intransferíveis, portanto, não devem ser compartilhadas;

6.7.2. Nenhum colaborador, seja da CONTRATANTE ou da CONTRATADA tem autorização para alterar a senha das credenciais de acesso antes do envio para os seus responsáveis;

6.7.3. Apenas o responsável pela credencial de acesso pode determinar e fazer uso do usuário e senha das credenciais de acesso, ou seja, a senha deve ser cadastrada pelo próprio colaborador, NÃO podendo ter nenhuma atuação de outros colaboradores ou compartilhamento.

6.7.4. O Solicitante de Acessos Lógicos NÃO tem autorização para trocar as senhas antes do envio para os seus responsáveis;

6.7.5. Os gestores NÃO têm autorização para trocar as senhas antes do envio para os seus responsáveis;

6.7.6. Os colaboradores devem receber as senhas expiradas para que realizem a troca. Não devem ser aceitas senhas não expiradas ou previamente definidas que não sejam passíveis de troca;

6.8. Na definição das senhas não devem ser usadas senhas fracas, senhas padrões ou com combinações óbvias, conforme requisitos mínimos estabelecidos, em requisitos disponíveis no documento de Requisitos de Segurança para Desenvolvimento Seguro conforme disposto no item 3.5 deste anexo.

6.8.1. Utilizar senhas complexas que contenham: Números, letras maiúsculas e minúsculas e caracteres especiais.

6.8.2. Cada colaborador é responsável pelas ações realizadas em seu usuário e senha, o que a torna pessoal e intransferível.

6.8.3. Contas privilegiadas de serviço, genéricas e RPA, devem impreterivelmente estar dentro do Cofre de Senha, com o processo de

controle desenha e monitoração das contas.

6.9. A CONTRATADA deverá adequar seu ambiente para poder ter acesso aos sistemas de propriedade da Telefonica, sendo obrigatório implementar uma das tecnologias de MFA (Multi Factor Authenticator) abaixo:

6.9.1. Mobile Authenticator: trata-se de uma aplicação que atua como um autenticador e é instalado em um disposto móvel de posse do usuário e é sincronizado com o Access Manager;

6.9.2. OTP (One Time Password) por SMS ou por E-mail;

6.9.3. Autenticação por Certificado Digital: os usuários que acessarão os sistemas da Telefonica devem utilizar um certificado digital que contém o CNPJ da empresa em um campo específico (campo este que deve ser definido pela equipe responsável pelo Access Manager) e este certificado deve ser instalado em cada computador que pertencer à empresa e for ser utilizado pelos usuários da referida empresa. No momento da autenticação o Access Manager irá validar se o computador assinado e os usuários pertencem à mesma empresa (todos os usuários possuem o CNPJ informado no SAP GT ou HCM carregados no AD) e, caso positivo, libera o acesso.

6.9.4. O detalhando técnico da implementação consta no documento “Requisitos de Segurança para Arquitetura de Sistemas”.

7. Gerenciamento de ativos e configuração de sistemas

7.1. A utilização ou integração de robô (RPA – Robotic Process Automation) e/ou Inteligência Artificial (IA) com sistemas da CONTRATANTE ou outras formas de integrações entre sistemas e banco de dados de forma automatizada (APIs, Integradores, consultas à banco de dados, etc) deverão ser submetidas para avaliação e aprovação da CONTRATANTE, que devem ser, Tecnologia da Informação, Segurança Digital e Engenharia de redes, especialmente em relação a qualquer necessidade de integração a interfaces, sistemas, aplicativos, base de dados e serviços

etc. Somente após a aprovação prévia dessas áreas que a integração deve ocorrer. Para avaliação será necessário a criação de um desenho da arquitetura de solução (DAS).

7.1.1 Para os casos de Inteligência Artificial, essas prerrogativas devem ser cumpridas, incluindo as que seguem:

7.1.1. É necessária a utilização de uma sandbox (ambiente para consumo do LLM - Large Language Model) onde os dados são isolados, evitando assim possíveis vazamentos/trocas de informação para alimentar outras Inteligências artificiais;

7.1.1.2 Toda IA utilizada deve se basear em uma versão enterprise, que respeite os direitos dos usuários e que possua proteções contra-ataques cibernéticos diversos;

7.1.1.3 A solução deve ser treinada a fim de evitar/monitorar vieses que porventura possam gerar algum tipo de discriminação, seja por cor, sexo, religião, condição social outros, sendo aplicável a qualquer tipo de IA, generativa, de aprendizado supervisionado ou não;

7.1.1.4 Os modelos utilizados devem conter formas de validar entradas de dados, sanitizar saídas e monitorar constantemente os retornos dados aos usuários diminuindo assim o risco de "alucinações" e devem ser aplicadas avaliações constantes;

7.1.1.5 Os dados utilizados para treinar o modelo de IA devem ser devidamente avaliados e sanitizados;

7.1.1.6 Havendo necessidade de compartilhamento de dados com parceiros, por meio de arquivos, esses deverão ser realizados por meio de ferramentas homologadas pelo time de Segurança Digital da CONTRATANTE e só poderão ser realizados quando existir um contrato previamente firmado com o parceiro que contenha este Anexo de Segurança.

7.2. Todos os processos e projetos de automações aprovados pelas áreas destacadas acima deverão seguir as diretrizes pré-estabelecidas

conforme especificado nos Requisitos de Segurança Digital da CONTRATANTE.

7.3. A CONTRATADA deverá se responsabilizar pelo uso seguro de todos os ativos que trafeguem dados da CONTRATANTE, sejam esses ativos fornecidos pela CONTRATANTE ou não. Ativos lógicos também devem ser incluídos no mesmo padrão de segurança incluindo e-mails, domínios, marcas e demais ativos lógicos utilizados no exercício deste contrato.

7.4. Os recursos da CONTRATADA que irão realizar atividades, objeto deste contrato, em sites/prédios administrativos da CONTRATANTE somente poderão se conectar ao nosso ambiente corporativo após seus equipamentos (dispositivos móveis, computadores etc.) forem autorizados pelas áreas técnicas responsáveis na Vivo e deverão estar com aplicação de hardening para controle de violação de dados. A depender do escopo da contratação, a CONTRATADA deverá se adequar a controles específicos por parte da CONTRATANTE, como VDI ou outras soluções.

7.5. Gestão de Log’s

7.5.1. A CONTRATADA deve manter uma gestão de logs que devem estar disponíveis mediante solicitação da CONTRATADA.

7.5.2. Os ativos da CONTRATADA que suportam o objeto deste Contrato devem prover logs que informem no mínimo, mas não se limitando a:

- Login do usuário;
- Data;
- Hora;
- Tipo do evento;
- Endereço do IP e Host name do equipamento.

7.6. Os arquivos de log devem ser armazenados de forma segura e possuir restrição de acesso, principalmente nos casos de permissão de alteração e exclusão. O acesso e a leitura dos arquivos de logs devem ser restritos aos usuários autorizados.

7.7. Não deve existir nenhum processo ou função que altere ou apague qualquer registro da trilha de auditoria, salvo o script de retenção.

7.8. Os ativos envolvidos na prestação do serviço para a CONTRATANTE devem ser contemplados por um processo de Hardening:

7.9. Deve haver um método de Backup das informações da CONTRATANTE, e o mesmo deve ser testado periodicamente.

7.10. A CONTRATADA deve restringir o acesso físico aos pontos de rede acessíveis publicamente, pontos sem fio, gateways e dispositivos portáteis.

7.11. Os computadores devem ser bloqueados sempre que houver ausência do seu usuário ou por inatividade e devem ser desbloqueados através da senha de acesso do usuário.

7.12. Os equipamentos envolvidos na operação devem possuir apenas conexões, interfaces, aplicações e dispositivos necessários à sua finalidade. A CONTRATADA deve bloquear a utilização de dispositivos que permitam a gravação de informações em mídia ou periféricos.

8. Segurança de rede

8.1. A CONTRATADA deverá controlar os tratamentos realizados com dados pessoais e sensíveis quando utilizados ativos de propriedade da CONTRATANTE, exemplos: equipamentos informáticos (ex: notebooks); aplicações; sistemas; ferramentas; servidores; banco de dados etc., isto implica:

8.1.1. Monitorar desvios de acesso a dados pessoais e sensíveis, ou seja, identificar as pessoas não-autorizadas (quando, quem e o que foi feito).

8.1.2. Poder controlar o que se pode fazer com a informação (leitura, cópia, impressão e modificação) de forma individualizada.

8.1.3. Os requisitos do Item 2, Privacidade, Proteção de Dados e Segurança da Informação precisam ser seguidos durante todo o ciclo de vida dos dados (acesso a dados, manipulação, exclusão e etc).

8.2. A CONTRATADA deve manter um procedimento de segurança lógica que englobe e documente os processos para:

8.2.1. Prover um segmento de rede exclusivo e segregado para os serviços contratados pela CONTRATANTE.

8.2.2. Controlar e restringir os acessos de outras redes para a rede exclusiva utilizada na prestação do serviço, através de regras restritivas de firewall.

8.2.3. Prover, quando solicitado pela CONTRATANTE, diagramas físicos e lógicos atualizados das redes que suportam as operações que são objeto deste CONTRATO, contendo os equipamentos utilizados e suas interconexões.

8.2.4. Implementar regras de controle de comunicação com a internet de acordo com a necessidade da operação.

8.2.5. Proteger as conexões de rede da empresa de outras redes externas, de acordo com as melhores práticas de Segurança da Informação.

8.2.6. Os ativos da CONTRATADA devem prover proteção contra códigos maliciosos, tais como antivírus e personal firewall (manter atualizados diariamente);

8.2.7. A instalação e utilização de pontos de acessos em fio deve ser controlada e configurada conforme as melhores práticas do mercado nos padrões segurança.

9. Gestão de ameaças e vulnerabilidades

9.1. A CONTRATADA deverá manter um processo de gestão de vulnerabilidade que abranja totalmente o escopo de serviços prestados para a CONTRATANTE, considerando identificação, classificação da vulnerabilidade, classificação do risco, plano de correção e registro de correção. O inventário de ativos como base para monitoração de vulnerabilidades deverá estar completo e integro.

9.2. Patches deverão ser aplicado sem janelas programadas a to dos os ativos no inventário, cumprindo o SLA descrito no item 5.7 deste documento.

9.3. A CONTRATADA deve definir um procedimento para calcular o risco de cada vulnerabilidade identificado, considerando critérios de classificação

da informação, probabilidade de exploração da vulnerabilidade e o impacto relacionado.

9.4. Os resultados também devem ficar disponíveis para consulta da CONTRATANTE.

10. Conscientização e treinamento de Cibersegurança

10.1. A CONTRATADA deve manter um programa de conscientização periódico garantindo que seus colaboradores estejam treinados nos temas de Segurança Digital.

10.1.1. A CONTRATANTE poderá solicitar a qualquer momento evidências do programa de conscientização da CONTRATADA. A CONTRATADA deverá apresentara documentação em resposta a solicitação da CONTRATANTE no prazo de 30 dias corridos.

10.1.2. Caso a CONTRATANTE identifique uma necessidade de melhoria no programa de conscientização da CONTRATADA, a CONTRATADA avaliará a sugestão e apresentará um plano de ação para atender a demanda ou uma formalização da impossibilidade de aplicação no prazo de 30 dias corridos.

11. Gestão de Continuidade de Negócios e Gestão de Crise

11.1. A CONTRATADA deverá implementar e manter um Sistema de Gestão de Continuidade de Negócios, atendendo os requisitos da ISO 22301, para garantir a disponibilidade e manutenção dos serviços/ produtos prestados a CONTRATANTE, dentro dos prazos acordados (SLA´s), considerando:

- A CONTRATADA deverá fornecer a qualquer momento, evidências da manutenção do SGCN (atualização dos documentos, planos e teste do período vigente do ciclo de GCN).
- A CONTRATADA deverá fornecer a qualquer momento, quando solicitado pela CONTRATANTE, as informações referentes à infraestrutura que suporta as atividades CONTRATADA, bem como o mapeamento das localidades e o número de estações de atendimento disponíveis em cada

uma das localidades onde estas são prestadas.

- A CONTRATADA deverá informar a CONTRATANTE toda e qualquer alteração em seu ambiente de trabalho e nos ambientes de contingência que estejam relacionados ao objeto ora contratado para o perfeito cumprimento desta cláusula.

11.2. Política de Gestão de Continuidade de Negócios

A CONTRATADA deve publicar e divulgar a política de GCN a todos os seus funcionários, e é de sua responsabilidade o cumprimento das diretrizes.

Os custos relacionados à manutenção do sistema de gestão de continuidade de negócios, planos de contingência e de recuperação, serão de total responsabilidade da CONTRATADA.

11.3. Gestão de Riscos para Continuidade de Negócios

Deverá ser realizado um processo de gestão de riscos que possam afetar produtos e serviços contratados, com a identificação, classificação e Planos de ação associados.

11.4. Planos de continuidade de negócios (PCN)

Os Planos de continuidade de negócios deverão contemplar:

- Plano de Continuidade Operacional para os processos que estejam envolvidos nos produtos e/ ou serviços fornecidos a CONTRATANTE.
- Plano de Resposta de Emergência para os incidentes com risco eminente à vida.
- Plano de Gestão de Incidentes com os canais e fluxo de reporte a CONTRATANTE.
- Plano de Gestão de Crise com os canais e fluxo de report e a CONTRATANTE.
- Plano de Recuperação de Desastres das infraestruturas críticas.

11.5. Plano de teste e Validação

Todos os planos de continuidade de negócio deverão ser testados de 6 em 6meses com coleta de evidência.

As evidências devem estar disponíveis para consulta da CONTRATANTE.

11.6. Estratégia de Continuidade de Negócio

Redundância e contingências para os recursos críticos para o fornecimento de serviços e/ou produtos nos sla´s acordados:

- Água;
- Energia elétrica comercial;
- Comunicação (links, rede de comunicação, telefonia, e-mail e etc.);
- Local de trabalho (ou alternativa, por exemplo: teletrabalho);
- Infraestrutura tecnológica ou de produção;
- Sistemas e Backup;
- Cadeia de suprimento;
- Demais recursos críticos.

11.7. Processo de Gestão de Crise

Ter um processo formal de gestão de crise, com a definição de papeis e responsabilidade, matriz de crise, fluxo e plano de comunicação.

Qualquer evento que gere impacto a CONTRATANTE (exemplo: interrupção, exposição da marca, pandemia) deverá ser comunicado nos canais definidos nos planos.

11.8. Plano de Conscientização e Treinamento para Continuidade de Negócios

As equipes deverão ser treinadas e conscientizadas sobre o tema de GCN e os planos em que atuam, a cada seis meses.

11.9. Volta à normalidade

Deve ser desenvolvido e implantado procedimentos de volta à normalidade após um incidente, utilizando-se dos planos de respostas específicos para cada tipo de cenário avaliado após a realização da análise de risco.

11.10. Melhoria contínua do Sistema de Continuidade de Negócios

Em todas as etapas do SGCN deve-se observar melhorias e lições aprendidas para implementação.

12. Segurança física e ambiental

12.1. Para as operações instaladas em sites de propriedade da CONTRATADA, esta deve:

12.1.1. Disponibilizar um ambiente logicamente reservado com controles de segurança físicos e/ou eletrônicos que garantam acesso individual e controlado. As informações de controle de acesso devem ser disponibilizadas no prazo de até 24 horas da solicitação, com um armazenamento disponível por no mínimo 60 meses ou tempo de contrato prevalecendo o maior quando solicitado pela CONTRATANTE. O objetivo é esclarecer incidentes relacionados ao ambiente físico e respaldo para fins de auditorias que se fizerem necessárias.

12.1.2. As portas e janelas devem ser mantidas fechadas quando não utilizada se dotadas de proteções externas, principalmente quando estiverem localizadas no andar térreo.

12.1.3. Instalar sensor de presença, para inibir o acesso por qualquer porta e janela acessível. As áreas desocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

12.1.4. Monitorar rigorosamente o ambiente interno por CFTV, de forma que seja possível visualizar todas as PAs (independente do mobiliário existente) e acessos.

12.1.5. Monitorar rigorosamente por CFTV e alarmes, os acessos de emergência e outros possíveis acessos (ex.: janelas).

12.1.6. Prover armazenamento das imagens gravadas pelo sistema de CFTV por, no mínimo, 120 (cento e vinte) dias e disponibilizá-las em até 24 (vinte e quatro) horas, quando solicitado pela CONTRATANTE e se certificando que as imagens possuam qualidade suficiente para identificar ações suspeitas. O objetivo é esclarecer incidentes relacionados ao ambiente físico.

12.1.7. Assegurar que as fitas das gravações de voz e das imagens sejam armazenadas em locais seguros.

12.1.8. As informações de clientes da CONTRATANTE não devem ser armazenadas pela CONTRATADA, com exceção das gravações de atendimento e de processos previamente acordados entre as partes.

12.1.9. Prover acesso às imagens de CFTV, em tempo real, para

monitoramento pela CONTRATANTE.

12.1.10. Atender às normas e leis reguladoras de Segurança, Detecção e Combate a Incêndio (Sistema de Segurança, Brigada de Incêndio, Bombeiro Civil residente, etc.).

12.1.11. Apresentar Auto de Vistoria do Corpo de Bombeiros (AVCB), ou seu congênere para o site, com a devida aprovação para as operações do site.

12.1.12. Deve apresentar procedimento formal de solicitação de acesso físico e controle da retirada ou instalação de equipamentos.

A CONTRATADA deverá apresentar formalmente, sua aderência e cumprimento das normas internacionais de acesso e controle, bem como também na questão ambiental, apresentar o AVCB do local em dia e com as devidas certificações dos órgãos reguladores para a operação do site.

13. Testes de Segurança

13.1. A CONTRATADA deve permitir que a CONTRATANTE realize os testes de segurança necessários quando solicitado em sistemas, sites, aplicações etc. para cumprimento dos objetos deste Contrato.

14. Encerramento do Contrato

14.1. A substituição ou mesmo o término dos serviços prestados pode ocorrera qualquer momento, para isso alguns itens de segurança da informação devem ser seguidos:

14.1.1. Garantia da revogação dos acessos;

14.1.2. Destruição dos dados armazenados (ao menos, que seja exigido a manutenção por legislação vigente, porém tão longo se atinja o prazo de conservação, os dados devem ser excluídos);

14.1.3. Entrega de todas as gravações telefônicas, gravações de tela, logs e quaisquer outros registros armazenados a CONTRATANTE.

15. Penalidades

15.1. Independente de eventuais reparações de danos (perdas e danos) a CONTRATANTE poderá efetuar a aplicação de multa não compensatória no valor mínimo de R$ 10.000,00 (dez mil reais) pelo descumprimento de qualquer regra de segurança prevista neste anexo. Na hipótese de reincidência no descumprimento dos requisitos de segurança o valor da penalidade poderá ser aplicado em dobro, bem como ser aplicada a penalidade prevista no Contrato, sem prejuízo da obrigatoriedade de deixar as soluções e/ou serviços em compliance com a segurança, independentemente do meio (parametrização, correção, configuração, desenvolvimento) e em tempo estipulado pela CONTRATANTE.

16. Vigência e Derrogações

16.1. A CONTRATANTE se reserva ao direito de alterar os termos e condições durante a vigência do contrato devido a mudanças nas análises de riscos de segurança. A CONTRATANTE se comunicará com a CONTRATADA via processo de gestão de terceiros descritos na clausula 5.

16.2. A CONTRATANTE poderá resolver o contrato devido a incumprimentos em matéria de segurança dos requisitos definidos neste anexo.

17. Ciência e aceite

Declaro que li e estou disposto a cumprir os requisitos de Segurança Digital, disposto em https://www.telefonica.com.br/a-telefonica/fornecedores/seguranca-da-informacao aplicáveis ao escopo e tecnologias que envolvam esse contrato.

ANEXO IV - CERTIFICADO ANTICORRUPÇÃO

O TRT-19 possui uma política de combate à corrupção, código de ética, código de conduta cuja finalidade seja a de assegurar o cumprimento de todas as leis de combate à corrupção aplicáveis e todas as normas internacionais de combate à corrupção.

DECLARAÇÃO

Declaro que, tanto quanto é do meu conhecimento, as informações prestadas acima, bem como as seguintes afirmações, são corretas, verdadeiras e completas. Forneço essa declaração como prova do compromisso do TRT-19 em cumprir com todas as leis de combate à corrupção aplicáveis.

O TRT-19 certifica que os seus proprietários, diretores, administradores, gerentes e empregados estão familiarizados com e concordam em cumprir todas as leis, estatutos, regulamentos e códigos aplicáveis nas jurisdições em que os negócios são conduzidos, no que diz respeito ao fornecimento de serviços, direitos e/ou bens a Telefônica, relativamente ao combate à corrupção, incluindo mas não se limitando, com a Lei Anti-Corrupção no Exterior, dos Estados Unidos (Foreign Corrupt Practices Act – FCPA) (coletivamente, "Leis de Combate à Corrupção"), conforme estabelecido na cláusula de combate à corrupção existente em qualquer contrato que venha a regular a relação entre o TRT-19 e a Telefônica (“Cláusula de Combate à Corrupção”).

Concordo que o TRT-19 irá cooperar de boa-fé em qualquer investigação a ser realizada por parte da Telefônica e de seus auditores, advogados e representantes em caso de alegada violação das

Leis de Combate à Corrupção e/ou da Cláusula de Combate à Corrupção.

Entendo que, caso seja provado que alguma das informações acima fornecidas seja materialmente incorreta e/ou que se o TRT-19 materialmente violar qualquer das declarações constantes neste documento, a Telefônica terá direito de rescindir imediatamente quaisquer contratos que tenha firmado com a EMPRESA.

Concordo que o TRT-19 deve notificar imediatamente a Telefônica no caso de qualquer uma das declarações e informações contidas neste documento sofrer mudanças ou se tornar inválida de qualquer forma.

Declaro e garanto que tenho o poder de representação e autoridade suficientes para fornecer as informações contidas neste Certificado e para vincular o TRT-19 aos termos e condições aqui contidos. Entendo que a Telefônica pode exigir no futuro que o TRT-19 certifique novamente as declarações contidas neste certificado (e/ou outras declarações adicionais/distintas).

ANEXO V - PLANO DE TRABALHO

1) DADOS CADASTRAIS

PARTICIPE 1:

Tribunal Regional do Trabalho da 19ª
Região CNPJ: 35.734.318/0001-80
Endereço: Avenida da Paz, nº 2076, Centro, Maceió/AL, CEP: 57020-440 DDD/Fone: (82) 2121-8299
Nome do responsável: Jasiel Ivo
Cargo/função: Desembargador
Presidente

PARTICIPE 2:

Telefônica Brasil S.A (VIVO)
CNPJ: 02.558.157/0001-62
Endereço: Av. Engenheiro Luiz Carlos Berrini, n° 1.376, Cidade Monções, São Paulo/SP, CEP: 04571-936
DDD/Fone:
Nome do responsável: Fernanda Fortunato Martins Chaguri Cargo/função: Procurador
Nome do responsável: Patrícia Andrea Tedesco Godoi Cargo/função: Procurador

2) IDENTIFICAÇÃO DO OBJETO

O presente Acordo de Cooperação Técnica tem por objeto permitir o acesso, via WEB, a magistrados e servidores do Tribunal Regional do Trabalho da 19ª Região ao sistema eletrônico “Portal Jud”, da VIVO, possibilitando a obtenção de informações de dados cadastrais de seus clientes, nos termos e condições estabelecidos no ajuste.

3) DIAGNÓSTICO

Atualmente, grande parte das solicitações judiciais de dados cadastrais às operadoras de telefonia é realizada por meio de ofícios físicos ou expedientes eletrônicos não padronizados, o que ocasiona:

a) demora na tramitação processual;
b) excesso de correspondências em papel;
c) risco de extravio ou inconsistência de informações;
d) ausência de fluxo padronizado para consulta.

A implantação do acesso direto ao Portal Jud permitirá informatizar, centralizar e padronizar tais solicitações, reduzindo o tempo de resposta e assegurando maior eficiência e segurança.

4) ABRANGÊNCIA

O Acordo de Cooperação Técnica abrangerá:

a) Todas as Varas do Trabalho vinculadas ao TRT da 19ª Região;
b) Gabinetes de Desembargadores e Secretarias do 2º grau;
c) Servidores e magistrados previamente cadastrados no sistema.

5) JUSTIFICATIVA

Trabalhando junto ao Projeto Garimpo nos processos antigos e já arquivados, foi constatada a necessidade de obtenção de dados atualizados das partes, já que, muitas vezes, as petições iniciais e documentos existentes nos autos encontravam-se com informações incompletas ou antigas.

Sem as informações necessárias, não era possível a localização das contas bancárias das pessoas físicas, de modo que havia a necessidade do conhecimento do endereço ou telefone atualizado das partes para que a intimação fosse realizada e os alvarás pudessem ser expedidos.

Destaca-se que as ferramentas de pesquisa atualmente à disposição deste TRT, nem sempre fornecem os dados necessários, razão pela qual foi cogitada a possibilidade de um convênio técnico com a empresa Telefônica Brasil S/A. (VIVO) para facilitar e aprimorar a prestação jurisdicional, tornando-a mais célere e efetiva.

6) OBJETIVOS

Geral:

Modernizar e informatizar o fluxo de requisições judiciais de dados cadastrais junto à VIVO, por meio da integração do TRT19 ao sistema Portal Jud.

Específicos:

a) Garantir maior agilidade na obtenção de informações cadastrais;
b) Reduzir/eliminar o uso de ofícios físicos;
c) Padronizar a emissão e resposta de solicitações;
d) Aumentar a confiabilidade e segurança no tratamento de dados sigilosos;
e) Monitorar estatisticamente o uso do sistema para aprimoramento contínuo.

7) METODOLOGIA (CRONOGRAMA DE ATIVIDADES)

Etapa	Atividade	Responsável	Prazo
1	Cadastro inicial dos magistrados e servidores autorizados	TRT19	até 30 dias da assinatura
2	Liberação de acessos ao "Portal Jud"	VIVO	até 45 dias da assinatura
3	Treinamento e capacitação dos usuários	VIVO, com apoio do TRT19	até 60 dias da assinatura
4	Divulgação interna do sistema	TRT19	até 90 dias da assinatura
5	Início da utilização regular	TRT19	até 90 dias da assinatura
6	Emissão de relatórios de utilização	VIVO, sob demanda	contínuo
7	Avaliação anual dos resultados e ajustes	TRT19 e VIVO	anual

8) OBRIGAÇÕES DOS PARTÍCIPES

TRT19:
a) Disponibilizar os meios técnicos de acesso ao sistema;
b) Manter a relação atualizada de usuários autorizados;
c) Comunicar alterações de credenciamento;
d) Garantir o uso do sistema apenas em requisições judiciais válidas;

e) Assegurar sigilo e confidencialidade dos dados obtidos;
f) Estimular a utilização do sistema e reduzir ofícios físicos.

VIVO:
a) Manter o funcionamento do sistema Portal Jud;
b) Disponibilizar acesso aos usuários autorizados;
c) Fornecer relatórios de acesso quando solicitado;
d) Comunicar falhas sistêmicas e disponibilizar suporte técnico;
e) Promover capacitação dos usuários, sempre que necessário.

9) PRAZO DE VIGÊNCIA

O Acordo terá vigência de 5 (cinco) anos, a contar da data de sua assinatura, sendo automaticamente renovado por igual período, salvo manifestação em contrário de qualquer das partes.

10) UNIDADE RESPONSÁVEL E GESTOR DO ACORDO DE COOPERAÇÃO TÉCNICA

TRT da 19ª Região:
Unidade Responsável: Secretaria Judiciária de 1º Grau
Gestor: Catarina Sampaio de Souza Carneiro

VIVO:
Unidade Responsável: Gerência SR Serviços Especiais
Gestor: Rodolfo Comar

11) RESULTADOS ESPERADOS

a) Redução significativa do tempo de resposta às requisições judiciais;
b) Eliminação do uso de ofícios em papel para solicitações cadastrais;
c) Padronização e segurança no fluxo de informações;
d) Maior controle estatístico do uso do sistema;
e) Conformidade com os princípios da celeridade, eficiência e economia processual;
f) Fortalecimento da parceria entre o Judiciário e a iniciativa privada na modernização de serviços.

De acordo com os Termos do Plano de Trabalho

JASIEL IVO
Desembargador Presidente
TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO

FERNANDA FORTUNATO MARTINS CHAGURI PATRÍCIA ANDREA TEDESCO GODÓI
TELEFONICA BRASIL S.A. (VIVO)

Certificado de Assinatura

Informações de timestamp obtidas no NTP.br e Observatório Nacional (ON)

Baseadas no fuso horário (GMT -3:00) de Brasília, Brasil

Este Certificado de Assinatura, contendo o histórico de ações, foi gerado em 08/05/2026 às 16:30:35 (GMT -3:00)

Acorco de Cooperação Técnica - TRT-19.pdf

ID do documento #3e0a1ab1-b68b-4e32-bbe0-af24359fe469

Assinaturas

Jasiel Ivo

Assinou

CLEVERSON CRONEMBERGER MARTINS

Assinou

RODOLFO COMAR

Assinou

PATRICIA ANDREA TEDESCO GODOI

Assinou

FERNANDA FORTUNATO MARTINS CHAGURI

Assinou

Log

27/04/2026 17:51:10	ROSEANE DA FONSECA VILASBOA ALVES criou este documento de ID 3e0a1ab1-b68b-4e32-bbe0-af24359fe469.
04/05/2026 17:36:33	Jasiel Ivo (CPF 284.226.194-15; E-mail jasiel.ivo@trt19.jus.br; IP 104.23.190.141;), Assinou usando Assinatura Eletrônica. 04/05/2026 às 17:36:33 (GMT -3:00);
04/05/2026 17:42:51	CLEVERSON CRONEMBERGER MARTINS (CPF 350.737.078-69; E-mail cleverson.martins@telefonica.com; IP 104.23.253.131; Geolocalização -23.62038816666666, -46.698866499999994), Assinou usando Assinatura Eletrônica. 04/05/2026 às 17:42:51 (GMT -3:00);
06/05/2026 15:07:37	RODOLFO COMAR (CPF 299.301.138-35; E-mail rodolfo.comar@telefonica.com; IP 162.158.63.65;), Assinou usando Assinatura Eletrônica. 06/05/2026 às 15:07:37 (GMT -3:00);

08/05/2026 11:26:47	PATRICIA ANDREA TEDESCO GODOI (CPF 154.822.268-24; E-mail ptedesco@telefonica.com; IP 172.70.231.89;), Assinou usando Assinatura Eletrônica. 08/05/2026 às 11:26:47 (GMT -3:00);
08/05/2026 16:30:28	FERNANDA FORTUNATO MARTINS CHAGURI (CPF 130.795.038-80; E-mail f.martins@telefonica.com; IP 172.70.111.85; Geolocalização -23.612425, -46.690725), Assinou usando Assinatura Eletrônica. 08/05/2026 às 16:30:28 (GMT -3:00);

Hash do documento original (SHA512):
b7c03f60e5d11a7fa5abf65a67ee4cc4012bcdaa30f7be1ef0966fdb5578fc943a05f2260fa48eaed49b676308e88bcccfd4a22b913ecf079a4543a4dd400503
Hash do documento assinado (SHA512):
1674e4a27c1d77052339777e42c48a756666c6b31e9c4636e6ff8ae28af29ae6dfe45efaa7acc811e4562ea2e832572632e0ee4d5551f90b96455481de6bbdb2

Este histórico de ações deve ser considerado parte exclusiva do documento de ID 3e0a1ab1-b68b-4e32-bbe0-af24359fe469, com função descrita nos Termos e Condições do Portal de Assinaturas Vivo.