



CONVÊNIO N.I. 01.010.10.2025

CONVÊNIO QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO TRIBUNAL REGIONAL FEDERAL DA 3.^a REGIÃO E A TELEFÔNICA BRASIL S.A., COM A INTERVENIÊNCIA DA JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM SÃO PAULO E DA JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM MATO GROSSO DO SUL, PARA O ACESSO, VIA WEB, AO SISTEMA ELETRÔNICO DENOMINADO “PORTAL JUD”, CONFORME AUTORIZAÇÃO CONSTANTE NO PROCESSO SEI N.º 0004893-35.2018.4.03.8002. AUSÊNCIA DE TRANSFERÊNCIA DE RECURSOS FINANCEIROS.

A **UNIÃO FEDERAL**, por intermédio do **TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO**, com sede na Avenida Paulista, 1842, Bela Vista, CEP 01310-936, São Paulo - SP, inscrito no CNPJ/MF sob o nº 59.949.362/0001-76, doravante denominado **TRF3**, neste ato representado por sua Diretora-Geral, Sra. **MARTA FERNANDES MARINHO CURIA**, RF: 816, designada pelo Ato n.º 5.537, de 28 de fevereiro de 2024, no uso das atribuições contidas na Portaria n.º 537, de 17/6/1993, e a **TELEFÔNICA BRASIL S.A.**, com sede na Av. Engenheiro Luiz Carlos Berrini, 1376, Cidade Monções, São Paulo/SP, inscrita no CNPJ/MF sob o nº 02.558.157/0001-62, doravante denominada **VIVO**, neste ato representada por seus procuradores, **DANIEL WILLIAN GRANADO**, portador da Carteira de Identidade RG 30.272.129 SSP/SP e inscrito no CPF sob o nº 309.445.648-01 e **PATRÍCIA ANDREA TEDESCO GODOI**, portadora da Carteira de Identidade RG 20.775.706-9 SSP-SP e inscrita no CPF sob o nº 154.822.268-24, com a interveniência da **JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM SÃO PAULO**, com sede na Rua Peixoto Gomide n. 768, Jardim Paulista, São Paulo/SP, CNPJ n. 05.445.105/0001-78, representada pelo Diretor do Foro da Seção Judiciária de São Paulo, Juiz Federal **PAULO CESAR CONRADO**, designado mediante o Ato n.º 13.359, de 04 de março de 2024, da Presidência do Egrégio Conselho da



Justiça Federal da 3.^a Região, doravante denominada **JFSP**, e da **JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM MATO GROSSO DO SUL**, com sede na Rua Delegado Carlos Roberto Bastos de Oliveira n. 128, Parque dos Poderes, Campo Grande/MS, CNPJ n. 05.422.922/0001-00, representada pela Diretora do Foro da Seção Judiciária de Mato Grosso do Sul, Juíza Federal **MONIQUE MARCHIOLI LEITE**, designada mediante o Ato n.º 10.611 da Presidência do Egrégio Conselho da Justiça Federal da 3.^a Região, doravante denominada **JFMS**, firmam o presente **CONVÊNIO**, com fundamento no art. 184 da Lei n.º 14.133/2021, no que couber, e, ainda, mediante as cláusulas e condições a seguir enumeradas:

CLÁUSULA PRIMEIRA – (DO OBJETO)

1.1) O presente Convênio tem por objeto permitir o acesso, via WEB, a magistrados e servidores públicos do **TRF3**, da **JFSP** e da **JFMS** ao sistema eletrônico denominado “**Portal Jud**” da **VIVO**, possibilitando o fornecimento de informações de dados cadastrais da base móvel de seus clientes, conforme condições e fluxo estabelecidos neste Convênio.

1.1.1) Fazem parte integrante do presente instrumento o Anexo I – Termo de Aceite do Portal Jud ([10588330](#)), Anexo II - Termo de Tratamento de Dados Pessoais ([10588429](#)), Anexo III - Requisitos de Segurança ([10588449](#)) e Anexo IV – Especificações de Uso do Portal Jud - perfil magistrado e serventuário ([10588506](#)), 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 Convênio.

1.2) Os Convenientes 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 e servidores públicos, os quais serão autorizados mediante ofício encaminhado à **VIVO**, devidamente assinado pela Desembargadora Presidente do **TRF3** ou por quem venha a ser por ela designado, contendo as seguintes informações individualizadas: nome completo, RG, CPF, e-mail funcional e telefone de contato, nos termos do Anexo IV ([10588506](#)).

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 Convênio são:

- (i) Informatizar as solicitações judiciais oriundas do **TRF3**, da **JFSP** e da **JFMS** para fornecimento de informações de dados cadastrais dos clientes da Vivo;
- (ii) Reduzir/eliminar a troca de ofícios/correspondências em papel;
- (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 IV (Especificações de uso do Portal Jud - perfil magistrado e serventuário - [10588506](#)) do presente Convênio.

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

1.10) A **VIVO** é titular dos direitos, inclusive de propriedade intelectual, sobre o “Portal Jud”, e o presente Convênio não concede ao **TRF3**, à **JFSP** e à **JFMS** nenhum direito, título ou interesse de qualquer natureza em relação a esse sistema eletrônico, sendo que neste ato o **TRF3**, a **JFSP** e a **JFMS** reconhecem a titularidade acima mencionada.

CLÁUSULA SEGUNDA - (DAS OBRIGAÇÕES)

2.1) O **TRF3**, a **JFSP** e a **JFMS**, sem prejuízo das demais obrigações estabelecidas no presente Convênio e documentos anexos, possuem 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 **TRF3, da JFSP e da JFMS**, 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 Convênio, somente será possível quando emanadas de magistrado 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 1.3 da cláusula primeira, evitando a utilização indevida do sistema “Portal Jud”.

e) Utilizar as facilidades do presente Convênio exclusivamente nas atividades que, em virtude de lei, compete-lhe exercer, com rigorosa observância dos deveres de sigilo e confidencialidade que lhe são inerentes, sob pena de responsabilidade civil e criminal pelos danos causados, sem prejuízo da rescisão automática deste Convênio, 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 Convênio 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 à **VIVO**, bem como orientar a emissão de ofícios de forma 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 Convênio e documentos anexos:

- a) Manter em funcionamento o sistema objeto do presente Convênio.
- b) Disponibilizar acesso ao sistema aos magistrados e/ou servidores do **TRF3**, da **JFSP** e da **JFMS**, desde que previamente credenciados e autorizados na forma prevista neste Convênio.
- c) Fornecer ao **TRF3**, à **JFSP** e à **JFMS** 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 **TRF3**, à **JFSP** e à **JFMS** 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 Convênio.
- f) Compromete-se a promover, sempre que necessário e na medida de sua disponibilidade, capacitação aos magistrados e servidores usuários do sistema objeto deste convênio.

CLÁUSULA TERCEIRA – (DA VIGÊNCIA)

3.1) Este convênio entra em vigor na data de sua assinatura, sendo de 60 (sessenta) meses o prazo de vigência.

CLÁUSULA QUARTA – (DA DENÚNCIA)

4.1) O presente convênio poderá ser denunciado de pleno direito, por qualquer uma das partes convenientes 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 convenientes comunicarão a alteração nos 30 (trinta) dias subsequentes, sob pena de reputarem-se eficazes as correspondências remetidas para os endereços aqui referidos.

CLÁUSULA QUINTA – (DA GESTÃO E FISCALIZAÇÃO)

5.1) Os Convenientes indicarão representantes para acompanhar o desenvolvimento dos objetivos e metas deste Convênio e fiscalizar a fiel observância de suas disposições, os



quais se comunicarão por escrito, no curso da execução dos serviços, diretamente ou por quem vierem a indicar.

TRF3, JFSP e JFMS: SEJU - Secretaria Judiciária do Tribunal Regional Federal da 3º Região – servidor responsável: Alexandre do Nascimento da Silva

E-mail: ansilva@trf3.jus.br

Telefone: (11) 3012-1518

VIVO: Rodolfo Comar

E-mail: rodolfo.comar@telefonica.com

Telefone: (11) 3190-2355

5.2). Caberá aos gestores:

5.2.1) acompanhar e fiscalizar a execução da parceria;

5.2.2) informar ao seu superior hierárquico a existência de fatos que comprometam ou possam comprometer as atividades ou metas da parceria e de indícios de irregularidades, bem como as providências adotadas ou que serão adotadas para sanar os problemas detectados;

5.2.3) adotar as providências necessárias à eventual prorrogação ou renovação da avença, observada a antecedência mínima de 4 (quatro) meses.

CLÁUSULA SEXTA – (DOS PRAZOS)

6.1) Os prazos de execução serão ajustados de comum acordo entre os partícipes.

CLAÚSULA SÉTIMA (CUMPRIMENTO DAS LEIS DE COMBATE A CORRUPÇÃO)

7.1) o **TRF3, da JFSP e da JFMS** se compromete, reconhece e garante que:

a) Tanto o **TRF3, da JFSP e da JFMS**, 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, cumprirão a todo momento durante o Compromisso Relevante (incluindo, se for o caso, 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 **TRF3, da JFSP e da JFMS**, as sociedades ou pessoas que a 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”, a fim 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 **TRF3, da JFSP e da JFMS** 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 **TRF3, da JFSP e da JFMS** 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 **TRF3, da JFSP e da JFMS** a adoção imediata de medidas corretivas apropriadas;

e) as manifestações, garantias e compromissos do **TRF3, da JFSP e da JFMS** constantes nesta Cláusula serão aplicáveis na sua totalidade a qualquer terceiro sujeito ao controle e influência do **TRF3, da JFSP e da JFMS**, ou que atue em seu nome, com relação ao Compromisso Relevante; de forma que o **TRF3, da JFSP e da JFMS** 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 **TRF3, da JFSP e da JFMS** com relação ao Compromisso Relevante, será cedido, transferido ou subcontratado a qualquer terceiro sem o prévio consentimento por escrito da **VIVO**;

f) o **TRF3, da JFSP e da JFMS** certificará periodicamente que cumpre com esta Cláusula sempre que solicitado pela **VIVO**.

7.2) Descumprimento.

a) O descumprimento desta Cláusula de “Cumprimento das Leis de Combate à Corrupção” será considerado um descumprimento contratual grave. 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 **TRF3, da JFSP e da JFMS**.

b) Na medida do permitido pela legislação aplicável, o **TRF3, da JFSP e da JFMS** 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 **TRF3, da JFSP e da JFMS** de suas obrigações contidas nesta Cláusula de “Cumprimento das Leis de Combate à Corrupção”.

7.3) A **VIVO** terá o direito de auditar o cumprimento, por parte do **TRF3, da JFSP e da JFMS**, de suas obrigações e manifestações constantes na presente Cláusula de “Cumprimento das Leis de Combate à Corrupção”. O **TRF3, da JFSP e da JFMS** cooperará totalmente com qualquer auditoria, revisão ou investigação realizada pela **VIVO** ou em nome desta.

CLÁUSULA OITAVA - (DO ADITAMENTO)

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

CLÁUSULA NONA - (DOS RECURSOS FINANCEIROS)

9.1) Cada Conveniente arcará com o ônus relativo às suas respectivas obrigações.

9.2) De imediato, a implementação do presente Convênio não gera quaisquer ônus financeiros entre os convenientes.

CLÁUSULA DÉCIMA – (DAS DISPOSIÇÕES GERAIS)

10.1) 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, no que couber, observadas as peculiaridades do exercício da atividade jurisdicional e o princípio da publicidade dos processos judiciais, sendo-lhes dado o tratamento estabelecido na legislação correlata e demais regulamentações.

10.2) 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.

10.3) O presente Convênio corresponde à totalidade do ajuste firmado entre seus Convenientes, não prevalecendo, para qualquer efeito, outras manifestações de vontade eventualmente expressas, salvo se decorrentes de lei ou norma regulamentar aplicável.



10.4) Caberá ao **TRF3**, à **JFSP** e à **JFMS** fiscalizar a fiel observância das disposições deste Convênio e das instruções constantes nos Anexos I, II, III, sem prejuízo da fiscalização a ser exercida pela **VIVO**.

10.5) 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 a responsabilidade sobre essas.

CLÁUSULA DÉCIMA PRIMEIRA – (DA PUBLICAÇÃO)

11.1) O extrato do presente Convênio será publicado pelo TRF3 no Diário Oficial da União, caso não seja possível sua publicidade no Portal Nacional de Contratações Públicas – PNCP, nos termos do 94, da Lei nº 14.133/2021, conforme orientação do Acórdão TCU nº 2458/2021 (Plenário).

11.2) O inteiro teor será publicado no Portal da Transparência.

CLÁUSULA DÉCIMA SEGUNDA – (DA LEGISLAÇÃO APLICÁVEL)

12.1) As Partes estão sujeitas, ainda, além de às Cláusulas deste CONVÊNIO, às normas da Lei Federal de Licitações e Contratos nº 14.133/2021 em sua redação atual, bem como, a toda a legislação que rege a matéria, no que couber e não conflitar com a citada lei.

CLÁUSULA DÉCIMA TERCEIRA - (DA SOLUÇÃO DAS CONTROVÉRSIAS E DÚVIDAS)

13.1) Os casos omissos ou quaisquer divergências decorrentes da execução deste Convênio serão resolvidos pelos Convenientes mediante conciliação, mediação ou outros métodos consensuais, observadas as disposições de leis e regulamentos aplicáveis e os princípios gerais de Direito.

CLÁUSULA DÉCIMA QUARTA – (DO FORO)

14.1) Para as que questões divergentes que surjam do presente Convênio, não resolvidas na esfera administrativa, os integrantes elegem o Foro da Justiça Federal, Seção Judiciária de São Paulo, 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 Convênio em meio eletrônico, conforme autorização constante do Processo Administrativo 0004893-35.2018.4.03.8002, para que surta seus jurídicos e legais efeitos.

São Paulo, 31 de julho de 2025.

Daniel Willian Granado

DANIEL WILLIAN GRANADO

PATRICIA ANDREA TEDESCO GODOI

PATRÍCIA ANDREA TEDESCO GODOI

TELEFONICA BRASIL S.A. (VIVO)

Marta Fernandes Marinho Curia

MARTA FERNANDES MARINHO CURIA

Diretora-Geral - TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO





TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
Av. Paulista, 1842 - Bairro Cerqueira César - CEP 01310-936 - São Paulo - SP - www.trf3.jus.br

ANEXO NI - MINUTA Nº 1/2024

ANEXO I - TERMO DE ACEITAÇÃO DO "PORTAL JUD"

AO CLICAR NO BOTÃO "CONCORDO" NA TELA DE ACESSO AO "PORTAL JUD" PARA A UTILIZAÇÃO DOS SERVIÇOS, O USUÁRIO ESTARÁ ADERINDO E ACEITANDO AUTOMÁTICA E INTEGRALMENTE OS TERMOS E CONSIDERAÇÕES DE USO ABAIXO DESCRITOS:

Considerando:

- a) os termos do Convênio firmado entre o TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO e a TELEFÔNICA BRASIL S.A, doravante denominada "VIVO", com a interveniência da JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM SÃO PAULO e da JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM MATO GROSSO DO SUL, para permitir o acesso, via "web", a magistrados e servidores, ao sistema denominado "Portal Jud" da VIVO, possibilitando o fornecimento de informações de dados cadastrais dos clientes de telefonia móvel ("Convênio");
- b) que a utilização das senhas e as consultas realizadas são de exclusiva e integral responsabilidade dos autorizados, detentores das "senhas"; e
- c) que a senha, pessoal e intransferível, é elemento que determina o reconhecimento e autenticação da identidade do usuário perante os sistemas da VIVO;

O Usuário declara, para todos os fins de direito, que ACEITA as condições de uso do "Portal Jud" da VIVO, assumindo integralmente as responsabilidades que decorrem deste ato, conforme cláusulas abaixo:

1. OBJETO

Permitir consulta "on line" de modo seguro de dados cadastrais (nome completo, endereço, CPF/CNPJ, RG) da base móvel via página "web" ("Portal Jud") nos termos das ordens judiciais proferidas nos autos dos processos judiciais. O "Portal Jud" permitirá ao usuário o acesso às informações cadastrais constantes nos sistemas operacionais/gerenciais da VIVO.

2. CONDIÇÕES DE ACESSO AO "PORTAL JUD"

Para acesso ao "Portal Jud" o sistema operacional deve ser o Windows 32 bits (versão 2000 ou superior), sendo que a utilização de quaisquer outros sistemas operacionais será de total e exclusiva responsabilidade do usuário.

Os sistemas utilizados pela VIVO contêm recursos de segurança compatíveis com os navegadores ("browsers"), todavia fica reservado à VIVO, após lançamento do "Portal Jud" e em razão de avanço tecnológicos, o direito à disponibilização de outras versões compatíveis com os dispositivos de segurança.

Eventuais problemas que o usuário possa ter e que estejam relacionados com os navegadores ("browsers") ou com equipamentos utilizados para acesso ao "Portal Jud" deverão ser solucionados pelos respectivos fornecedores dos equipamentos, ficando o usuário desde já comprometido a acessar o "Portal Jud" por meio de computador seguro, mantendo atualizados seus sistemas de segurança tais como: antivírus, *antispyware* e *firewall*.

A VIVO não se responsabiliza pela descontinuidade na prestação do serviço, em decorrência da utilização pelo usuário, de equipamentos incompatíveis.



O "Portal Jud" será disponibilizado ao usuário 24 horas por dia durante os 7 dias da semana, ininterruptamente, não obstante, a VIVO poderá interromper e/ou modificar o funcionamento do serviço do "Portal Jud" para manutenção técnica, atualização e otimização do mesmo, ou para dar cumprimento a eventuais determinações oriundas do regulador ou do Poder Judiciário.

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

Caso o usuário tenha problemas de conexão estes deverão ser solucionados diretamente junto aos seus respectivos provedores de acesso à internet, não tendo a VIVO qualquer ingerência sobre tais questões.

O usuário desde já reconhece e expressamente aceita que a VIVO não será responsável por quaisquer problemas de interrupção dos serviços disponibilizados por meio do "Portal Jud", por motivos alheios à vontade da VIVO e/ou de seus prestadores de serviço, incluindo, sem limitação, queda no fornecimento de energia ou de conexão discadas ou dedicadas, problemas com as companhias de acesso à internet ou quaisquer outros terceiros que prestem tal serviço.

O usuário deverá observar os alertas de segurança contidos na página de obtenção do cartão de segurança.

3. NÃO DIVULGAÇÃO A TERCEIROS

O usuário deste sistema deverá considerar como confidenciais e sigilosas as informações obtidas através dele, ficando **impedido**, assim, de divulgá-las a terceiros, bem como de utilizá-las com finalidade diversa da respectiva ordem judicial autorizadora ou instrumento, ficando obrigado a zelar pela informação como se fosse seu titular.

4. ACESSO OU CONSULTA INDEVIDA

O usuário deste sistema será responsável pelo acesso ou consulta não autorizada ou fora do próprio conteúdo contido na ordem judicial autorizadora, sendo obrigatória a identificação, em cada consulta, do número dos autos nos quais autorizada a pesquisa.

5. PENALIDADES

O usuário compromete-se com o fiel cumprimento das disposições contidas neste termo de aceitação.

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, à responsabilização civil, criminal e administrativa decorrentes da violação deste termo, bem como pela violação de direitos e garantias fundamentais de clientes desta operadora, 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 convênio firmado, sem que lhe seja imputada qualquer responsabilidade.

6. LEI APLICÁVEL E FORO

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

As Partes elegem o Foro estabelecido no termo de convênio firmado entre as partes, com renúncia expressa a qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas ou questões que dele possam surgir.

Após leitura e plena concordância deste termo, o cartão de segurança será enviado para que Vossa Senhoria tenha acesso, via WEB, ao "Portal Jud" da VIVO, nos termos da(s) respectiva(s) ordem(ns) judicial(is) ou instrumento que lhe autoriza(m).





Documento assinado eletronicamente por **Jane Eire de Sousa Malfinati, Assessora Jurídica**, em 19/02/2024, às 17:59, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **10588330** e o código CRC **DF48D319**.

0004893-35.2018.4.03.8002

10588330v3





TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
Av. Paulista, 1842 - Bairro Cerqueira César - CEP 01310-936 - São Paulo - SP - www.trf3.jus.br

ANEXO NI - MINUTA Nº 2/2024

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 do Convênio para acesso, via web, de magistrados e servidores públicos do TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO (“TRF3”), da JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM SÃO PAULO e da JUSTIÇA FEDERAL DE PRIMEIRO GRAU EM MATO GROSSO DO SUL, ao sistema eletrônico denominado “Portal Jud” da VIVO (“Convênio”), celebrado por e entre as Partes definidas no preâmbulo do Convênio, e o integra para todos os fins de direito.

2. DEFINIÇÕES

No caso de qualquer ambiguidade ou conflito entre os Anexos do Convênio e este 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 Convênio.

“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 a pessoa natural identificada ou identificável, inclusive números identificativos, dados locais 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 Convênio.

“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, tendo em vista o Tratamentos de Dados Pessoais para os fins específicos discriminados na cláusula primeira do Convênio, assumirão, ambas, o papel de Controladores de Dados Pessoais, não respondendo uma a outra, sob nenhuma hipótese, como Operador.

3.1.1. É vedada ao TRF3, à JFSP e à JFMS a utilização de todo e qualquer dado pessoal repassado em decorrência da execução do Convênio para finalidade distinta daquela do objeto do Convênio, bem como por pessoas não autorizadas ou terceiros, sob pena de responsabilização, inclusive por força de atuação de qualquer autoridade fiscalizadora ou agência governamental de proteção de dados.

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), no que couber, respeitadas as peculiaridades da atividade jurisdicional e o princípio da publicidade dos processos judiciais.

3.2.2. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução do Convênio, no que couber, ressalvadas as peculiaridades decorrentes da atividade jurisdicional e o princípio da publicidade dos processos judiciais, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do Convênio.

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.

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.

3.3. Caberá ao TRF3 comunicar à VIVO, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, suspeita ou conhecimento de qualquer comprometimento ou qualquer forma de tratamento inadequado ou ilícito, bem como se tiver ocorrido qualquer descumprimento significativo ou substancial deste Termo e do Convênio.

3.3.1. Na incidência da hipótese acima, deverá ainda o TRF3 cooperar integralmente com a VIVO para a investigação do fato.



Documento assinado eletronicamente por **Jane Eire de Sousa Malfinati, Assessora Jurídica**, em 19/02/2024, às 17:59, conforme art. 1º, III, "b", da Lei 11.419/2006.





A autenticidade do documento pode ser conferida no site
[http://sei.trf3.jus.br/sei/controlador_externo.php?](http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) informando o código verificador **10588429** e
o código CRC **9AC55C26**.

0004893-35.2018.4.03.8002

10588429v2





TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
Av. Paulista, 1842 - Bairro Cerqueira César - CEP 01310-936 - São Paulo - SP - www.trf3.jus.br

ANEXO NI - MINUTA Nº 3/2024

ANEXO III - de Segurança Digital

1. Políticas, Normas e Procedimentos de Cibersegurança

A CONTRATADA é responsável por assegurar e garantir a segurança das informações, a integridade e a confidencialidade dos seus respectivos sistemas, tanto fisicamente quanto logicamente, implementando todas as medidas de segurança necessárias para segurança deste ambiente. 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 o software utilizado pela CONTRATANTE, onde A CONTRATADA foi o desenvolvedor).

Os custos relacionados à manutenção do sistema de gestão e controles de segurança da informação e, caso aplicável, recuperação de informações, sistemas ou infraestruturas, serão de total responsabilidade da CONTRATADA.

Para isso a CONTRATADA deve possuir um modelo de gestão de segurança da informação, que aborde minimamente os temas cobertos neste anexo.

2. Privacidade e Proteção de Dados

A CONTRATADA deve garantir as premissas básicas de segurança da informação (confidencialidade, integridade e disponibilidade) para todos os sistemas e/ou aplicações próprias para cumprimento do objeto deste contrato que manipulem dados ou informações da CONTRATANTE.

Toda a base de dados e informações da Vivo a que a CONTRATADA tiver acesso no exercício das suas obrigações do presente Contrato, são de propriedade exclusiva da Vivo. Estes dados e informações são estritamente confidenciais, de acordo com os termos deste anexo.

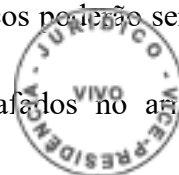
A CONTRATADA deverá utilizar os dados somente para a finalidade de execução deste contrato não podendo, em nenhum caso, utilizar esses dados para benefício próprio e/ou de terceiras partes.

Cooperar com a CONTRATANTE para responder às solicitações que tenham por objetivo o exercício dos direitos dos titulares dos dados, que inclui o direito de: transparência, informação, acesso, retificação e exclusão (direito ao esquecimento), limitação e oposição do tratamento, portabilidade entre outros que estão especificadas na legislação vigente de proteção de dados.

A CONTRATADA não compartilhará nem de outra forma divulgará os dados e informações da CONTRATANTE, nem permitirá o tratamento destes por seus representantes ou terceiros, exceto (a) se 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) conforme permitido segundo os contratos aplicáveis e formalizados e (d) se for exigido de acordo com a legislação aplicável. Caso exista necessidade da CONTRATADA transferir, compartilhar, divulgar ou permitir o tratamento de dados da CONTRATANTE por terceiros, a CONTRATADA notificará prontamente a Vivo antes de tal exigência.

A CONTRATADA deverá indicar o(s) país(es) e a região(ões) onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

Os dados pessoais e sensíveis da CONTRATANTE devem ser criptografados no armazenamento e transporte.



As informações e dados da CONTRATANTE devem ser armazenados em diretórios exclusivos e segregados.

Armazenamento em Nuvem está autorizado somente na modalidade Privada.

A transferência internacional de dados pessoais e sensíveis somente é permitida de acordo com as regras da legislação aplicável e diante da autorização expressa da CONTRATANTE, que poderá ser formalizada, inclusive, mediante contrato.

Quando da rescisão do Contrato ou mediante solicitação por escrito da Vivo, o que ocorrer primeiro, a CONTRATADA cessará imediatamente e garantirá que seus subcontratados cessem imediatamente, todo e qualquer uso dos dados e informações da CONTRATANTE, devolvendo-os, descartando-os, destruindo-os ou tornando-os anônimos de forma permanente, utilizando, em cada caso, as medidas de segurança aplicáveis. Se a legislação aplicável não permitir que a CONTRATADA destrua ou descarte os dados e 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.

3. Requisitos de Segurança Digital

A CONTRATADA deve seguir padrões e arquiteturas de referência adequadas de acordo com os requisitos de Segurança Digital. Os requisitos poderão ser acessada através do site institucional na parte de provedores/políticas de fornecedores (Disponível aqui: <https://www.telefonica.com.br/servlet/Satellite?c=Page&cid=1386090998763&pagename=InstitucionalVivo/Page/TemplateDestques>). 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.

Todos os entregáveis, incluindo o desenvolvimento, produzido para e/ou fornecido para a Vivo 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 Vivo.

4. Gestão de Incidentes de Segurança

A CONTRATADA notificará, através do canal de denúncias: CSIRT Vivo Brasil (csirt.br@telefonica.com), prontamente a Vivo 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 tomará todas as medidas necessárias para corrigir a situação e manter a segurança de todas as informações da Vivo, durante e após a vigência do Contrato.

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

A Vivo 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.

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

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

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

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.

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
Vulnerabilidade V0 (*)	24 horas
Crítica	5 dias
Alta	8 dias
Moderado	30 dias
Médio	60 dias
Leve	90 dias

(*) Vulnerabilidades V0 é a categoria criada pela Vivo 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

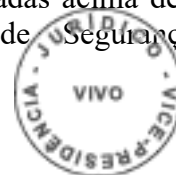
Para sistemas em que a Vivo fornecerá acesso a CONTRATADA, as regras serão as mesmas utilizadas nas políticas vigentes para a CONTRATANTE. Para sistemas que a própria CONTRATADA faz a gestão de acessos deverão ser implantados os controles de acessos que garantam não repúdio dos acessos e logs para investigação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

As regras de controle de acesso devem respeitar revisões periódicas de acessos e perfis, senhas complexas, revogação de acesso e logs. 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.

7. Gerenciamento de ativos e configuração de sistemas

A utilização ou integração de robô (RPA – Robotic Process Automation) 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 das da CONTRATANTE, que podem ser, Tecnologia da Informação, Segurança Digital e/ou 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.

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.



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.

Os recursos da CONTRATADA que irão realizar atividades, objeto deste contrato, em sites/prédios administrativos da Vivo 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.

7.1. Gestão de Log's

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

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

- a) Login do usuário;
- b) Data;
- c) Hora;
- d) Tipo do evento;
- e) Endereço do IP e Hostname do equipamento.

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.

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

8. Segurança de rede

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:

- Monitorar desvios de acesso a dados pessoais e sensíveis, ou seja, identificar as pessoas não-autorizadas (quando, quem e o que foi feito).
- Poder controlar o que se pode fazer com a informação (leitura, cópia, impressão e modificação) de forma individualizada.

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

- Prover um segmento de rede exclusivo e segregado para os serviços contratados pela CONTRATANTE.
- Controlar e restringir os acessos de outras redes para a rede exclusiva utilizada na prestação do serviço, através de regras restritivas de firewall.
- 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.
- Implementar regras de controle de comunicação com a internet de acordo com a necessidade de operação.
- Proteger as conexões de rede da empresa de outras redes externas, de acordo com as melhores práticas de Segurança da Informação.

- Os ativos da CONTRATADA devem prover proteção contra códigos maliciosos, tais como antivírus e personal firewall (manter atualizados diariamente);
 - A instalação e utilização de pontos de acesso sem fio deve ser controlada e configurada conforme as melhores práticas do mercado nos padrões segurança.
- Os ativos envolvidos na prestação do serviço para a CONTRATANTE devem ser contemplados por um processo de Hardening.
- Deve haver um método de Backup das informações da CONTRATANTE, e o mesmo deve ser testado periodicamente.
 - A CONTRATADA deve restringir o acesso físico aos pontos de rede acessíveis publicamente, pontos sem fio, gateways e dispositivos portáteis.
 - 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.
 - 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.

9. Gestão de ameaças e vulnerabilidades

A CONTRATADA deverá manter um processo de gestão de vulnerabilidade que abranja totalmente o escopo de serviços prestados para a Vivo, 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 íntegro.

Patches deverão ser aplicados em janelas programadas a todos os ativos no inventário.

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.

Os resultados também devem ficar disponíveis para consulta da contratante.

10. Conscientização e treinamento de Cibersegurança

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

11. Gestão de Continuidade de Negócios e Gestão de Crise

Estando a CONTRATANTE obrigada ao cumprimento dos regulamentos da ANATEL - Agência Nacional de Telecomunicações, notadamente as Leis 9472, de 16/07/1997, também conhecida por “Lei Geral das Telecomunicações” e Resolução N. 460, de 19/03/2007, também conhecida como “Regulamento Geral de Portabilidade” (RGP) no que tange à ininterruptão dos seus serviços ao grande público, a CONTRATADA garante:

- Disponibilidade de seus ambientes, conforme contratado, considerando o tipo de atividade a ser exercida:
- o 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.
 - o Deverá ser fornecida pela CONTRATANTE uma avaliação quanto aos negócios elegíveis e prioridade de recuperação das atividades CONTRATADA.
 - o Quando solicitado pela CONTRATANTE, a CONTRATADA deverá informar os custos referentes à implantação da contingência, processos e prazos de recuperação para cada módulo de negócio, que serão objeto de negociação entre as partes. A CONTRATADA se compromete a fazer as alterações na

infraestrutura que suporta a as atividades a partir das decisões tomadas na negociação, a fim de implementar melhorias e, conseqüentemente, assegurar a continuidade de suas operações.

· A CONTRATADA deverá informar a CONTRATANTE toda e qualquer alteração em seu ambiente de trabalho e nos ambientes de contingência que atuarem ou fizerem qualquer referência ao objeto ora contratado para o perfeito cumprimento desta cláusula.

11.1. Requisitos Mínimos Para A Continuidade De Negócios E Recuperação De Desastres

- a) O prestador de serviços deve garantir os backups das informações, bem como realizar periodicamente Testes de restauração.
- b) A empresa deverá realizar o Sistema de Gestão de Continuidade Negócio: Plano de Administração de Crise, Plano de Gestão de Crise (exemplo: crise hídrica e elétrica), Plano de Gestão de Incidente, Plano de Recuperação de Desastre, Plano de Teste e Validação e Plano de comunicação;
- c) Deve estar documentado entre a CONTRATANTE e o fornecedor de serviços o prazo/tempo máximo e mínimo para recuperação dos dados e/ou serviços em caso de desastres;
- d) Deve possuir site alternativo para o caso de indisponibilidade de acesso ao prédio principal.
- e) Deverão ser realizados testes dos planos periodicamente, de 6 em 6 meses, com coletas de evidências;
- f) Deve possuir infraestrutura de contingência: geradores, nobreak, redundância de links, equipamentos críticos para operação, refrigeração, reservatórios de água etc;

11.2. Estratégia de Continuidade

Devem ser identificadas as soluções táticas para suportar a restauração das atividades exigidas dentro de um tempo de recuperação desejado. Em cada caso, devem ser avaliadas as alternativas a fim de minimizar a probabilidade de um mesmo incidente afetar a solução de continuidade do negócio.

11.3. Comunicação de Incidente

Todo e qualquer incidente que comprometa a Continuidade dos Serviços, deve ser comunicado de imediato ao Gestor da Continuidade de Negócios responsável, para as providências necessárias e o acionamento dos respectivos planos de Continuidade.

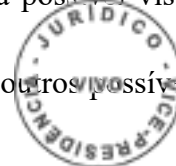
11.4. Resposta e Operações de Emergência

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

12. Segurança física e ambiental

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

- Disponibilizar um ambiente logicamente reservado com controles de segurança físicos e/ou eletrônicos que garantam acesso individual e controlado.
- As portas e janelas devem ser mantidas fechadas quando não utilizadas e dotadas de proteções externas, principalmente quando estiverem localizadas no andar térreo.
- 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.
- Monitorar rigorosamente o ambiente interno por CFTV, de forma que seja possível visualizar todas as PAs (independente do mobiliário existente) e acessos.
- Monitorar rigorosamente por CFTV e alarmes, os acessos de emergência e outros possíveis acessos (ex.: janelas).



- Prover armazenamento das imagens gravadas pelo sistema de CFTV por, no mínimo, 90 dias e disponibilizá-las em até 24 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.
- Assegurar que as fitas das gravações de voz e das imagens sejam armazenadas em locais seguros.
- 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.
- Prover acesso às imagens de CFTV, em tempo real, para monitoramento pela CONTRATANTE.
- Atender às normas e leis reguladoras de Segurança, Detecção e Combate a Incêndio (Sistema de Segurança, Brigada de Incêndio, Bombeiro Civil residente, etc.).
- Apresentar Auto de Vistoria do Corpo de Bombeiros (AVCB), ou seu congênere para o site, com a devida aprovação para as operações do site.
- Deve apresentar procedimento formal de solicitação de acesso físico e controle da retirada de equipamentos.

13. Encerramento do Contrato

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

- Garantia da revogação dos acessos;
- 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);
- Entrega de todas as gravações telefônicas e logs armazenados a CONTRATANTE;

14. Penalidades

A CONTRATANTE poderá efetuar a aplicação das multas descritas no item de Penalidades na seção 6 do item “Contrato de Prestação de Serviços”

15. Vigência e Derrogações

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 poderá rescindir o contrato devido a incumprimentos em matéria de segurança dos requisitos definidos neste anexo.



Documento assinado eletronicamente por **Jane Eire de Sousa Malfinati, Assessora Jurídica**, em 19/02/2024, às 17:59, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **10588449** e o código CRC **9ACA9A72**.

