Tribunal Regional Eleitoral de Santa Catarina

CONVÊNIO N. 001/2025
SEI N. 0000536-21.2025.6.24.8000

CONVÊNIO CELEBRADO ENTRE O TRIBUNAL E A VIVO PARA DISPONIBILIZAR, DE FORMA GRATUITA, O *PORTAL JUD*, PLATAFORMA QUE POSSIBILITARÁ A JUÍZES E SERVIDORES A REALIZAÇÃO DE CONSULTA DIRETA DE DADOS CADASTRAIS POR LINHA/CPF/CNPJ/NOME, DE FORMA A OTIMIZAR O TEMPO DAS PARTES.

O **TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA**, com sede, Rua Esteves Júnior 68, CEP 88015-130, Florianópolis/SC, inscrito no CNPJ sob o nº 05.858.851/0001-93, doravante denominado **TRE-SC,** representado por sua Presidente, Desembargadora Maria do Rocio Luz Santa Ritta e a **TELEFONICA 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, Daniel Willian Granado, inscrito no CPF ***.445.648-** e Patrícia Andrea Tedesco Godoi, inscrita no CPF ***.822.268-**, firmam o presente Convênio, mediante as cláusulas e condições a seguir discriminadas, com fulcro nos princípios e legislação aplicável à espécie.

CLÁUSULA PRIMEIRA – (DO OBJETO)

1.1) O presente Convênio tem por objeto permitir o acesso, via WEB, a magistrados e servidores públicos do **TRE-SC** 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 os Anexo I **–** Termo de Aceite do Portal Jud, Anexo II - Termo de Tratamento de Dados Pessoais, Anexo III - Requisitos de Segurança e Anexo IV **–** Especificações de Uso do Portal Jud, 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 Convenentes 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 pela Desembargadora Presidente do **TRE-SC**, 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 Convênio são:

(i) Informatizar as solicitações judiciais oriundas do PODER JUDICIÀRIO 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 I (Especificações de uso do Portal Jud) do presente Convênio.

1.9) Todos os usuários do "Portal Jud" deverão firmar, sem exceção, "Termo de Aceitação", nos moldes do Anexo II do presente Convênio. Tal aceite será realizado "on line", 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 Convênio não concede ao **TRE-SC** nenhum direito, título ou interesse de qualquer natureza com este sistema eletrônico, sendo que neste ato o **TRE-SC** reconhece a titularidade acima mencionada.

CLÁUSULA SEGUNDA - (DAS OBRIGAÇÕES)

2.1) o **TRE-SC**, sem prejuízo das demais obrigações estabelecidas no presente Convênio 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 clausula primeira, item 1.3., bem como manter atualizada a relação dos magistrados e servidores públicos do **TRE-SC,** 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 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 Convênio 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 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 a **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 **TRE-SC**, desde que previamente credenciados e autorizados na forma prevista neste Convênio.

c) Fornecer ao **TRE-SC** 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 **TRE-SC** 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 convenentes 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 convenentes 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 Convenentes 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 Convênio.

CLAÚSULA SEXTA (CUMPRIMENTO DAS LEIS DE COMBATE A CORRUPÇÃO)

6.1) o **TRE-SC** se compromete, reconhece e garante que:

a) 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;
b) Comunicará de imediato à **VIVO** eventual descumprimento de qualquer das obrigações descritas na letra (a) desta Cláusula. Caso ocorra tal descumprimento, a **VIVO** se reserva o direito de exigir do **TRE-SC** a adoção imediata de medidas corretivas apropriadas;
c) O objeto do presente Convênio não será cedido, transferido ou subcontratado;
d) Certificará periodicamente que cumpre com esta Cláusula sempre que solicitado pela **VIVO**.

6.2) 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, este contrato poderá ser imediatamente denunciado pela **VIVO**, e a **VIVO** não será obrigada a pagar qualquer valor devido ao **TRE-SC**;
b) Na medida do permitido pela legislação aplicável, o **TRE-SC** avaliará a possibilidade de indenizar e isentar 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 **TRE-SC** de suas obrigações contidas nesta Cláusula de "Cumprimento das Leis de Combate à Corrupção".

CLÁUSULA SÉTIMA - (DO ADITAMENTO)

JURÍDICO VICE-PRESIDÊNCIA VIVO

CONSULTORIA E CONTRATOS PLLMM VIVO

7.1) 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 OITAVA - (DO ÔNUS)

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

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

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 Convênio corresponde à totalidade do ajuste firmado entre seus Convenentes, 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 Convênio serão resolvidos pelos Convenentes 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 **TRE-SC** fiscalizar a fiel observância das disposições deste Convênio e das instruções constantes nos Anexos I, II e III, 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)

10.1) Para as que questões divergentes que surjam do presente Convênio, não resolvidas na esfera administrativa, os integrantes elegem o Foro da Comarca da Capital de Santa Catarina, renunciando a qualquer outro, por mais privilegiado que seja.

E, por estarem de pleno acordo, é firmado o presente instrumento pelos partícipes abaixo, dele sendo extraídas as cópias necessárias para sua publicação e execução.

Florianópolis, 12 de fevereiro de 2025.

JURÍDICO VICE-PRESIDÊNCIA VIVO

CONSULTORIA E CONTRATOS PLLMM VIVO

Documento assinado digitalmente
MARIA DO ROCIO LUZ SANTA RITTA
Data: 19/03/2025 18:37:51-0300
Verifique em https://validar.iti.gov.br

_____]

MARIA DO ROCIO LUZ SANTA RITTA - DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA

Documento assinado digitalmente
DANIEL WILLIAN GRANADO
Data: 24/03/2025 14:56:37-0300
Verifique em https://validar.iti.gov.br

_____

DANIEL WILLIAN GRANADO - TELEFONICA BRASIL S.A. (VIVO)

Documento assinado digitalmente
PATRICIA ANDREA TEDESCO GODOI
Data: 21/03/2025 09:16:54-0300
Verifique em https://validar.iti.gov.br

_____

PATRÍCIA ANDREA TEDESCO GODOI - TELEFONICA BRASIL S.A. (VIVO)

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:

Deste modo:

Considerando:

a) os termos do instrumento firmado entre o **TRE-SC** e a **VIVO**, para permitir o acesso, via "web", a magistrados e servidores nos termos do instrumento, ao sistema denominado "Portal Jud" da **VIVO**, possibilitando o fornecimento de informações de dados cadastrais dos clientes de telefonia móvel ("instrumento");

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 judicias. 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 (versão2000 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 o navegador ("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 V**IVO** 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 a vontade da **VIVO** e/ou de seus prestadores de serviço, incluindo, sem limitação, fornecimento de energia e queda de conexão discadas ou dedicadas, com as companhias de acesso à internet ou quaisquer outros terceiros que prestem tais serviços.

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 divulga-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, 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 instrumento 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 do quais a República Federativa do Brasil seja signatária.

As Partes elegem o Foro estabelecido no termo de convênio firmado entre as partes e, na ausência do mesmo, estabelecem que serão observadas as regras de competência de cada estado da Federação, com menção 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).

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 para acesso, via web, a magistrados e servidores públicos do **TRE-SC** ao sistema eletrônico denominado "Portal Jud" da **VIVO** ("Contrato"), celebrado por e entre as Partes definidas no preâmbulo do Contrato, e o integra para todos os fins de direito.

2 DEFINIÇÕES

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.

"Anonimização": utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

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

"Dado Pessoal Sensível": dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

"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.

"Incidente de Segurança": o estabelecido na Cláusula 3.3.1.

"**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.

"Requisitos de Segurança": requisitos mínimos de segurança da informação estabelecidos pela VIVO para Tratamento seguro dos Dados Pessoais. Estarão consolidados em documento anexo ao Contrato, caso a VIVO julgue aplicável.

"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, tendo em vista o Tratamentos de Dados Pessoais para os fins específicos discriminados na cláusula primeira do Contrato, assumirão, ambas, o papel de Controladores de Dados Pessoais, podendo, a depender do contexto fático, responder uma à outra, como Operador.
3.1.1 São vedados ao **TRE-SC** e à **VIVO** a utilização e o compartilhamento de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, bem como por pessoas não autorizadas ou terceiros, sob pena de responsabilização na medida de sua culpabilidade, administrativa, civil e criminal, inclusive para as hipóteses ocorridas 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).
3.2.2 Manter sigilo e confidencialidade de todas os dados pessoais repassados em decorrência da execução contratual, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contrato.
3.2.3 Competem às Partes garantir, por si próprias ou quaisquer de seus empregados, prepostos, sócios, diretores, representantes ou terceiros contratados, a confidencialidade dos dados processados, assegurando que todos os seus colaboradores prepostos, sócios, diretores, representantes ou terceiros contratados que lidam com os dados pessoais sob responsabilidade da outra Partes assinaram Acordo de Confidencialidade com as Parte, bem como a manter quaisquer dados pessoais estritamente confidenciais e de não os utilizar para outros fins. Ainda, treinarão e orientarão as suas equipes sobre as disposições legais aplicáveis em relação à proteção de dados.
3.2.4 Nomear um Encarregado, de acordo com os critérios estabelecidos pelas Leis Aplicáveis.
3.2.5 Estabelecer e cumprir medidas técnicas e organizacionais internas para o tratamento, visando o cumprimento dos requisitos legais para o tratamento.
3.2.6 Respeitar e atender aos direitos dos Titulares, sendo cada parte responsável pela comunicação e respostas referentes ao seu Tratamento de Dados Pessoais. Exceto quando uma Parte atuar como Operadora dos Dados Pessoais, situação na qual ela deverá, antes de responder diretamente ao Titular, comunicar à Controladora dos Dados Pessoais.
3.2.7 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.
3.2.8 Se responsabilizar, integralmente, por Subcontratações que possam existir, respondendo à outra parte pelos atos de seus subcontratados, com se seus fossem.
3.2.9 Competem as Partes manter registro do tratamento de dados pessoais realizados no âmbito da execução do presente contrato, providenciando o descarte dos dados cadastrais fornecidos pelas Partes, de forma irrecuperável, após o término da vigência deste instrumento, respeitados os prazos legais aplicáveis. O referido registro deverá conter:
a) A descrição dos processos de Tratamento de Dados Pessoais realizados.
b) A relação de transferências de Dados Pessoais para fora do Brasil, quando expressamente autorizada por uma Parte à outra, incluindo a identificação (i) dos países destino e (ii) do mecanismo de transferência utilizado para realização da transferência internacional.
c) Descrição geral das medidas técnicas e organizacionais utilizadas pela Parte, conforme descrito nos Requisitos de Segurança, caso aplicável.
d) Nome e dados de contato do Subcontratado, caso aplicável, assim como seus representantes ou Encarregado.
3.2.10 Cabe e à **VIVO**, de igual modo, eliminar imediatamente os dados cadastrais de usuários que por qualquer motivo percam seu acesso ao "Portal Jud" por deixarem de existir as condições necessárias para utilização do Sistema, sob pena de se sujeitar às penalidades especificadas na LGPD. Assim como cabe ao **TRE-SC** informar à **VIVO** todos os usuários que, por qualquer motivo, perderem acesso ao "Portal Jud".
3.2.11 Utilizar os dados de servidores e magistrados exclusivamente para permitir o acesso ao "Portal Jud".
3.2.12 Cabe ao **TRE-SC** manter um controle rígido sobre todos os acessos que fizer junto ao "Portal Jud" para o cumprimento de decisões judiciais, devendo encaminhar, sempre que solicitado pela **VIVO** documentação que suporte referidos acessos.

3.3 INCIDENTE DE SEGURANÇA
3.3.1. Uma Parte deverá, dentro de até 48 (quarenta e oito) horas úteis, notificar a outra Parte: (i) se tiver conhecimento ou suspeitar de qualquer comprometimento, divulgação a pessoas não autorizadas ou uso de Dados Pessoais de maneira não autorizada; (ii) se tiverem sido apresentadas quaisquer reclamações sobre as práticas de tratamento pela Parte notificante; ou (iii) se tiver ocorrido qualquer descumprimento significativo ou substancial deste Termo (cada um denominado individualmente "Incidente de Segurança").
3.3.2. Caberá ao **TRE-SC** comunicar à **VIVO**, diante de alguma evidência, incidentes de acesso não autorizado aos dados pessoais obtidos partir da utilização do "Portal Jud", e aos dados cadastrais de magistrados e servidores públicos, que serão utilizados exclusivamente como elementos de autenticação para acesso ao "Portal Jud", que acarrete perda, destruição, alteração, compartilhamento, suspeita ou em qualquer forma de tratamento inadequado ou ilícito, e que possa comprometer o fiel cumprimento deste Termo e do Contrato.
3.3.3. Caberá à **VIVO** comunicar ao **TRE-SC**, no menor tempo possível mas nunca superior à 48 (quarenta e oito) horas úteis, diante de alguma evidência, incidentes de acesso não autorizado à base de dados do Sistema "Portal Jud" que acarrete perda, destruição, alteração, compartilhamento, suspeita ou em qualquer forma de tratamento inadequado ou ilícito, e que possa comprometer as informações já acessadas pelo TRE-SC ou os dados cadastrais de magistrados e servidores públicos, que serão utilizados exclusivamente como elementos de autenticação para acesso ao "Portal Jud", afetando o fiel cumprimento deste Termo e Contrato.
3.3.4. Nas situações descritas nesta cláusula 3.3., deverão as Partes: (i) cooperar integralmente uma com a outra para a investigação do Incidente de Segurança incluindo, sem limitação, a disponibilização de recursos humanos de uma Parte

à outra ou ao representante por ela designado, para investigação forense com o intuito de determinar o escopo de qualquer Incidente de Segurança; e (ii) preservar todas as informações e evidências relacionadas ao Incidente de Segurança incluindo, entre outros, a suspensão de limpeza (*overwriting*) ou exclusão rotineiras de dados ou arquivos de log.
3.3.5. As partes responderão, na medida de sua culpabilidade, administrativa e judicialmente, em caso de comprovadamente causarem danos patrimoniais, morais, individual ou coletivo aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD.

4. SUBCONTRATAÇÃO
4.1. É vedado às Partes compartilhar com, ou permitir o Tratamento por terceiros de Dados Pessoais a que tiver acesso, em decorrência do Contrato, salvo se prévia, expressa e formalmente autorizado pela outra Parte.
4.2. Caso haja subcontratação autorizada pela outra Parte, a Parte que subcontratar permanecerá responsável por todas as obrigações contidas neste Termo, incluindo:
4.2.1. Informar à outra Parte a identidade e localização do Subcontratado, bem como a descrição do Tratamento pretendido.
4.2.2. Tomar as medidas cabíveis para garantir o cumprimento deste Termo pelo Subcontratado, aplicando a ele as mesmas obrigações e responsabilidades aqui dispostas.
4.3. A Parte que subcontratar é solidariamente responsável pelo Tratamento de Dados Pessoais realizados pelo Subcontratado, respondendo por eventuais danos causados por este.

ANEXO III - DA 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/TemplateDestaques). 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 da 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 integro.
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 ininterrupção dos seus serviços ao grande público, a CONTRATADA garante:

- Disponibilidade de seus ambientes, conforme contratado, considerando o tipo de atividade a ser exercida:
  - 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.
  - Deverá ser fornecida pela CONTRATANTE uma avaliação quanto aos negócios elegíveis e prioridade de recuperação das atividades CONTRATADA.
  - 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 [illegible]

infraestrutura que suporta a as atividades a partir das decisões tomadas na negociação, a fim de implementar melhorias e, consequentemente, 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.

*****FIM DO ANEXO *****