TERMO DE COOPERAÇÃO PARA USO DO SISTEMA INFOTIM ACT Nº 6532/2026

Termo de Cooperação para Uso do Sistema INFOTIM que celebram entre si as Partes elencadas abaixo, a fim de disponibilizar via WEB, a magistrados e servidores públicos do **TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO**, o sistema eletrônico INFOTIM (doravante denominado Sistema), para acesso a dados de clientes e registros de fluxos telefônicos e de dados, que sejam necessários para instruir processos judiciais em conformidade com a legislação vigente.

I. **TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO**, localizado na rua Esteves Júnior, n o 395, bairro Centro, na cidade de Florianópolis, Estado de Santa Catarina, CEP 88015-905, inscrito no CNPJ sob o no 02.482.005/0001-23, neste ato representado pela sua Desembargadora do Trabalho Presidente, Exma. Senhora Teresa Regina Cotosky, daqui por diante designado meramente **"TRT12ª"** e/ou **"LICENCIADO"**,

E, de outro lado,

II. **TIM S/A**, inscrita no CNPJ sob o n° 02.421.421/0001-11, com sede na Avenida João Cabral de Mello Neto, n° 850, bloco 1, sala 1212, Barra da Tijuca/RJ, CEP 22775-057, neste ato representada por seu Diretor, Heros Fabiano dos Santos, portador da Carteira de Identidade RG nº 54.651.108-9, e do CPF nº 614.732.940-53, doravante denominada "**TIM"** e/ou **"LICENCIANTE"**,

Resolvem firmar o presente Termo, regido pela Lei n° 14.133/2021 e alterações posteriores, pelas cláusulas e condições que se seguem.

CLÁUSULA PRIMEIRA:
DO OBJETO

1.1. O presente Termo tem por objeto permitir o acesso, via WEB, para magistrados, desembargadores e servidores públicos do **TRT12ª**, ao sistema eletrônico INFOTIM, com objetivo de automatizar as solicitações de fornecimento de informações de dados cadastrais e de registros de fluxos telefônicos e de dados de clientes TIM, bem como o recebimento de respostas via sistema, conforme condições e fluxos estabelecidos neste Termo.

1.1.1. Para que seja franqueado qualquer acesso a dados e informações via INFOTIM a Magistrados, desembargadores e servidores, estes necessariamente precisarão estar desempenhando suas funções e estarem devidamente cadastrados como usuários do sistema na TIM e amparados em ordem judicial autorizadora.

1.1.2. Os objetivos do presente Termo são:

a) Informatizar as solicitações judiciais para o fornecimento de dados cadastrais e registros de fluxos telefônicos e de dados por magistrados, desembargadores e servidores na fruição de suas atribuições, mediante acesso ao Sistema por meio de *login* e *senha* previamente cadastrados nos termos do presente Termo, nos autos dos processos que tramitam perante este **TRT12ª**;

b) Otimizar a comunicação entre as partes conveniadas para recebimento e envio das informações relacionadas na alínea "a" deste parágrafo; e

c) Padronizar as consultas e respectivas respostas.

1.2. **Anexos:** Integram o presente instrumento para os devidos fins de direito os seguintes Anexos:

Anexo I – Termos e Condições de Uso e Política de Privacidade
Anexo II - Anexo técnico de segurança
Anexo III- Termo de Compromisso de Integridade

1.3. Em caso de contradição entre disposições deste termo e de qualquer de seus anexos, prevalecerão como mandatórias as disposições deste termo.

CLÁUSULA SEGUNDA:
VIGÊNCIA

2.1. A vigência do presente Termo é de 60 (sessenta) meses, a contar da data da publicação da respectiva súmula no Diário da Justiça Eletrônico, não devendo ser publicado o inteiro teor deste Termo.

CLÁUSULA TERCEIRA:
DAS ESPECIFICIDADES

3.1. As partes definem que todas as consultas realizadas por meio do Sistema obrigatoriamente serão originadas por determinação judicial específica proferida nos autos de processo judicial por magistrado competente.

3.1.1. **Acesso ao Sistema**: O acesso será disponibilizado aos magistrados, desembargadores e servidores públicos, os quais serão autorizados mediante ofício encaminhado à TIM, por meio do e-mail infotim@timbrasil.com.br, observando o seguinte:

I. O ofício deverá conter informações individualizadas, tais quais: nome completo, data de nascimento, matrícula funcional, RG, CPF, órgão de lotação, endereço, inclusive e-mail (funcional), e telefone de contato, nos termos do Anexo I.
II. Após o envio do ofício, a TIM realizará o cadastramento e a criação do novo usuário, de forma individualizada no Sistema, e enviará o seu respectivo "login" e link para criação de sua senha pessoal, via e-mail institucional. Após o recebimento, o usuário deverá realizar a criação da senha em seu primeiro acesso, além de sincronizar o token, através do Google Authenticator ou outro disponível que seja compatível com o sistema INFOTIM. Os dados de acesso são pessoais e intransferíveis, sendo de única e exclusiva responsabilidade do usuário a correta utilização do Sistema, pelo acesso às informações nos limites da determinação judicial específica, bem como pelo total sigilo das informações obtidas.
III. Qualquer mal-uso ou uso indevido do Sistema pelo usuário poderá, por liberalidade e sem necessidade de comunicação prévia por parte da TIM, ter seu acesso interrompido, responsabilizando-se civil e criminalmente por todos os danos diretos e indiretos, decorrentes da utilização inadequada ou indevida do Sistema.
IV. Serão criados perfis diferenciados no Sistema, conforme cargo público previsto no quadro de servidores e função do usuário no **TRT12ª**, que limitarão o acesso às informações conforme legislação vigente e definição entre as partes, ressaltando que os registros de fluxo telefônico e de dados somente serão permitidos a magistrados e desembargadores, segregados de acordo com a função do usuário no **TRT12ª**.

V. Os usuários do Sistema deverão se recadastrar semestralmente para que o acesso permaneça ativo, visando manter a base atualizada e garantir a integridade e a segurança. Na hipótese do usuário não acessar o sistema no prazo de 3 (três) meses o acesso será bloqueado, sendo necessária a realização do recadastramento, nos termos deste parágrafo Primeiro.

VI. O titular do login e senha é única e exclusivamente responsável pela sua guarda e segurança não sendo permitido em hipótese alguma o compartilhamento dessas informações a terceiros para acesso, sob pena de responsabilização cível e criminal.

VII. Na hipótese do usuário deixar de fazer parte do quadro de servidores/magistrados ou assumir função diversa no **TRT12ª** diferente daquela que justificou o acesso ao Sistema, a TIM deverá ser informada sobre tal evento, por escrito, pelo **TRT12ª**, no prazo de 24 (vinte e quatro) horas, através do e-mail infotim@timbrasil.com.br para a realização do cancelamento do perfil de acesso.

VIII. Na ausência de aviso pelo **TRT12ª** para a realização do cancelamento do perfil de acesso nos termos indicados no item "7" deste parágrafo, a TIM não se responsabilizará por qualquer acesso indevido feito por usuários que deixaram de fazer parte do quadro de servidores/magistrados ou que assumiram funções diversas no **TRT12ª** diferentes daquelas que justificaram seu prévio acesso ao Sistema.

3.2. Os servidores públicos cadastrados serão responsáveis pelo lançamento no Sistema das informações atinentes ao processo e à determinação judicial proferida por magistrado competente, para posterior validação e aceite do magistrado responsável pelo deferimento do pedido, conforme fluxo de aprovações e validações parametrizados no Sistema.

3.3. A consulta a dados cadastrais de clientes TIM, via sistema, dar-se-á mediante prévia autorização do magistrado competente, de acordo com as permissões concedidas pelo **TRT12ª**, nos autos do processo judicial a que se refere, ficando expressamente vedada a consulta para fins diversos, sob pena de responsabilização cível e criminal.

3.4. As requisições de registros de fluxo telefônico e de dados deverão ser realizadas somente pelo magistrado lotado na Vara de origem do processo objeto da solicitação, não sendo permitida a sua delegação em nenhuma hipótese, sendo obrigatório anexar uma cópia da ordem autorizativa ou da decisão judicial no sistema.

3.5. Consideram-se dados cadastrais para fins deste Termo a identificação do titular, as informações que encontrarem-se disponíveis na base de clientes da TIM, sendo necessário que o solicitante indique o período de consulta limitado a 5 (cinco) anos da data da solicitação, e nos exatos termos da determinação judicial específica.

3.6. Consideram-se registros de fluxo telefônico e de dados as seguintes informações:

a) chamadas telefônicas originadas e recebidas;

b) registro de SMS enviados e recebidos exceto o conteúdo;

c) identificação de uso de IMEI; e

d) registros de conexão, de acordo com os registros que se encontrarem disponíveis nas bases de dados da TIM.

3.7. Todas as solicitações e/ou acessos ao Sistema devem respeitar as instruções e especificações constantes no Anexo I do presente Termo.

3.8. Todos os usuários do Sistema deverão aceitar previamente à sua utilização, sem exceção, o "Termo de Uso", nos moldes do Anexo I do presente Termo. Tal aceite será realizado "on line", quando do primeiro acesso de cada usuário, que ficará registrado no banco de dados da TIM.
3.9. A TIM é titular das informações e do direito de uso do Sistema INFOTIM, sendo que o presente Termo não concede ao Poder Judiciário nenhum direito, título ou interesse de qualquer natureza a este Sistema, motivo pelo qual neste ato o **TRT12ª** reconhece a referida titularidade.

CLÁUSULA QUARTA:
DAS ATRIBUIÇÕES DO TRT12ª

4.1. Constituem atribuições do **TRT12ª**, sem prejuízo das demais obrigações estabelecidas no presente Termo e no Anexo I:

4.1.1. **Cumprimento de lei e normativos**: Cumprir, durante a execução do objeto do Termo, todas as leis, normas regulamentares vigentes e normativos da CONTRATANTE aplicáveis a execução do Termo, inclusive os relativos à: (i) segurança, (ii) higiene do trabalho, (iii) segurança do trabalho, (iv) NBR ISO IEC 27001, (v) privacidade, acesso a sistemas e aplicativos, incluindo legislação brasileira aplicável à coleta, tratamento e guarda de dados pessoais e sensíveis, eventualmente coletados, que não poderão ser utilizados para quaisquer fins diversos do previsto neste Termo, ainda que anonimizados, sendo a única responsável por perdas e danos de qualquer natureza decorrentes de infrações a que houver dado causa, bem como pelo pagamento das multas eventualmente aplicadas pelas autoridades competentes.

4.1.2. **Incidente de Segurança.** Comunicar a TIM imediatamente e não ultrapassando o prazo máximo de 48h (quarenta e oito horas) contadas da ciência da mera suspeita ou ocorrência de quaisquer incidentes de segurança no âmbito da prestação de Serviços objeto deste Termo, sem prejuízo de responder por eventuais danos causados à TIM na forma da legislação vigente.

4.1.2.1. Qualquer incidente de segurança envolvendo dados pessoais deve ser mantido em absoluto sigilo pelo **TRT12ª**, ficando expressamente proibido o **TRT12ª** divulgar, tornar públicas, notificar às autoridades ou aos titulares de dados quaisquer informações sobre o incidente. A comunicação de um incidente aos titulares e/ou às autoridades públicas, incluindo, mas não se limitando a Autoridade Nacional de Proteção de Dados, deve ser previamente avaliada e autorizada, por escrito, pela TIM.

4.1.3. Dispor de meios próprios, seguros e necessários para acesso ao Sistema INFOTIM, tais como computadores e provedor de acesso à Internet, única e exclusivamente por meio da rede interna do **TRT12ª**, a fim de obter acesso via WEB;

4.1.4. Enviar à TIM, nos termos dispostos no parágrafo primeiro da cláusula terceira deste instrumento, a relação de magistrados, desembargadores, servidores e funcionários públicos do **TRT12ª** autorizados a acessar o Sistema, bem como manter atualizada a referida relação, a fim de viabilizar o cadastro dos usuários, sempre que necessário.

4.1.5. Orientar os usuários a indicar em cada requisição no Sistema o número do processo judicial respectivo, bem como o magistrado ou desembargador responsável pelo deferimento da decisão que embasa o acesso;

4.1.6. Comunicar imediatamente a TIM a substituição ou exclusão de servidor(es) e/ou magistrado (s) credenciado(s) evitando a utilização indevida do Sistema, observado o disposto nos itens VII e VIII da cláusula 3.1.1acima;

4.1.7. Utilizar as facilidades do presente Termo 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, sem prejuízo do automático rompimento deste Termo, por parte da TIM, independentemente de prévio aviso;

4.1.8. Responsabilizar-se inteiramente pelo conhecimento, utilização e sigilo das informações objetos do Termo e constantes do Sistema, utilizando-as exclusivamente nos fins para os quais foram requisitadas.

4.1.9. Divulgar o presente Termo entre as unidades jurisdicionais de sua competência e estimular sua utilização, adotando os procedimentos necessários para reduzir/eliminar o envio de ofícios, alvarás, mandados físicos à TIM, relativos a dados cadastrais e de registros de fluxo telefônico e de dados, bem como orientar a emissão de referidos documentos de forma padronizada;

4.1.10. Promover as solicitações das informações do presente Termo sempre via sistema;

4.1.11. Não divulgar a terceiros estranhos ao Termo os procedimentos aqui previstos, bem como os canais de atendimento da GRAOP TIM.

CLÁUSULA QUINTA:
DAS ATRIBUIÇÕES DA TIM

5.1. Constituem atribuições da TIM, sem prejuízo das demais obrigações estabelecidas no presente Termo e no Anexo I:

5.1.1. Adotar todas as medidas que estiverem ao seu alcance para manter em funcionamento o Sistema, objeto do presente Termo, ressalvados os períodos de indisponibilidade do Sistema em virtude da necessidade de manutenção preventiva/corretiva, previamente informada ao **TRT12ª**;

5.1.2. Disponibilizar acesso ao Sistema aos magistrados, desembargadores e/ou servidores do **TRT12ª**, desde que previamente credenciados e autorizados na forma prevista neste Termo;

5.1.3. Fornecer ao **TRT12ª** relatórios estatísticos de acesso ao Sistema de consultas realizadas, sempre mediante prévio requerimento expresso e assinado por seu representante.

5.1.4. Sempre que possível, comunicar ao **TRT12ª** qualquer problema sistêmico que possa impactar ou impossibilitar o atendimento às determinações judiciais, indicando o telefone (11) 4251-6633 para contato, além de possibilitar a abertura de chamados através do próprio Sistema, a ser realizado pela área técnica do **TRT12ª** junto à GRAOP TIM, para dirimir dúvidas técnicas e quanto ao cumprimento dos termos deste Termo. Não poderá incidir qualquer sanção à TIM, em decorrência de eventual inoperância corretiva ou de manutenção preventiva do Sistema ou em razão de seu uso irregular por qualquer parte dos usuários;

5.1.5. Compromete-se a promover, sempre que necessário e na medida de sua disponibilidade, capacitação aos magistrados, desembargadores e servidores usuários do Sistema objeto deste Termo;

5.1.6. Ressalva-se que a fidedignidade das informações prestadas pela TIM dependerá da correta indicação dos dados pelos usuários autorizados a utilizar o Sistema, sem que caiba à TIM qualquer responsabilidade sobre a fidedignidade e veracidade dos mesmos. Em relação aos registros de fluxo telefônico e de dados, a disponibilização das informações pela TIM via Sistema estará limitada às características técnicas relativas aos sistemas de telecomunicação aplicáveis e de mediação responsáveis pela coleta e armazenamento dos CDR's, bem como as informações estarão limitadas ao prazo de armazenamento legal.

CLÁUSULA SEXTA:
DO ÔNUS

6.1. As partes arcarão com o ônus relativo às suas respectivas obrigações derivadas deste Termo.

6.2. A implementação do presente Termo não gera quaisquer ônus financeiros entre as partes.

6.3. As partes declaram possuir as necessárias licenças, registros e autorizações internas para firmar o presente Termo.

CLÁUSULA SÉTIMA:
ETAPAS OU FASES DA EXECUÇÃO

7.1. O Cronograma de Execução do presente Termo descreve a implementação de um projeto em termos de metas, etapas ou fases, bem como prazos, conforme quadro abaixo:

META/Etapa	**ESPECIFICAÇÃO**	**DURAÇÃO**	
1) Cadastramento de usuários	Encaminhamento pelo **TRT12ª** à TIM, da relação inicial de Magistrados e Servidores a serem cadastrados como usuários do sistema	Em até 30 dias após a assinatura deste instrumento por ambas as partes	
2) Capacitação dos usuários cadastrados pela TIM		Em até 60 dias após a assinatura deste instrumento por ambas as Partes	

3) Divulgação	Expedição de ato divulgando e regulamentando a utilização do sistema no âmbito do **TRT12ª**.	Em até 90 dias após a assinatura deste instrumento por ambas as Partes	

CLÁUSULA OITAVA:
HIPÓTESES DE ENCERRAMENTO DA RELAÇÃO CONTRATUAL

8.1. **Rescisão Motivada.** Este Termo poderá ser considerado rescindido de pleno direito, independentemente de aviso ou notificação judicial ou extrajudicial, em qualquer uma das seguintes hipóteses:

i) Por motivo de caso fortuito ou força maior que impeça a execução do Termo, de forma definitiva, ou por tempo superior a 3 (três) meses;

ii) Em caso de falência, pedido de autofalência, recuperação judicial ou extrajudicial, deferida por Juízo competente ou insolvência de qualquer das Partes ou empresas do mesmo grupo;

iii) Ocorrência de fato que, por sua natureza e/ou gravidade, incidam sobre a confiabilidade do **TRT12ª** (e de qualquer de seus servidores ou administradores) ou que seja suscetível de causar danos ou comprometer, mesmo que indiretamente, a imagem da TIM, conforme critério desta;

iv) Em caso de violação de quaisquer das declarações e garantias constantes do Anexo III – Termo de Compromisso de Integridade deste Termo;

v) Utilização, pelo **TRT12ª**, em benefício próprio ou de terceiros, de informações confidenciais às quais tenha acesso por força de suas atribuições neste Termo,

8.2. **Denúncia (Rescisão Imotivada).** O presente Termo poderá ser rescindido 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 ambas.

8.3. **Distrato**. as Partes poderão, em comum acordo, distratar o presente Termo mediante assinatura do respectivo Instrumento.

CLÁUSULA NONA:
DO CUMPRIMENTO DAS LEIS DE COMBATE À CORRUPÇÃO

9.1. Integra este Termo, para todos os fins de direito, o Anexo III – Termo de Compromisso de Integridade, cujo conteúdo o **TRT12ª** reforça conhecer, concordar e aderir.

9.2. O **TRT12ª** ratifica o compromisso de utilizar o Canal de Denúncias da TIM, disponível em http://www.tim.com.br/canal-denuncia/?origin=RI, para submeter ali todo e qualquer tentativa tomar

conhecimento que enquadre-se em inobservância ao Código de Ética e Conduta, a Política Anticorrupção e de Conflito de Interesses e/ou legislações vigentes, em especial a de anticorrupção.

9.3. O **TRT12ª** indenizará e isentará a TIM de e contra qualquer perda, reivindicação, custa ou despesa incorrida pela TIM, baseadas em e/ou decorrentes de qualquer violação das declarações e garantias estabelecidas no Anexo III, e na presente Cláusula, em decorrência de qualquer ato, ativo ou omissivo, do **TRT12ª** e/ou de seus por magistrados, desembargadores, servidores e/ou representantes.

CLÁUSULA DÉCIMA:
DA CONFIDENCIALIDADE

10.1. As Partes, seus administradores, empregados e subcontratados (quando autorizados) guardarão absoluto sigilo sobre todas as informações recebidas da ou de qualquer forma pertinentes à outra Parte, ou a suas coligadas, controladas, controladoras e empresas sob controle comum, de forma direta ou indireta, independente da forma por meio da qual sejam divulgadas e de estarem ou não marcadas como "confidenciais", as quais venha a ter acesso após ser assinado o Termo, ou que lhe tenham sido divulgadas antes de sua celebração ("Informações Confidenciais").

10.1.1. Também são consideradas Informações Confidenciais a existência do Termo, seu Objeto e conteúdo, (b) informações relacionadas à execução do Objeto, e (c) quaisquer informações relativas ao conglomerado ou grupo econômico da TIM (aí incluídos dados e documentos relacionados, de qualquer forma, a seus acionistas, controladas, coligadas e de seus clientes).

10.1.2. As Partes não deverão usar quaisquer das Informações Confidenciais exceto para os propósitos deste Termo, e não poderão divulgá-las a terceiros, sem que a outra Parte, prévia e expressamente, autorize e aprove o conteúdo e a forma específicos de cada divulgação.

10.2. As Partes são responsáveis por qualquer revelação não autorizada, efetuada por qualquer um de seus empregados, prepostos, contratados, agentes e representantes que tenham recebido Informações Confidenciais, e tomarão todas as precauções necessárias para impedi-los de revelar ou utilizar, de forma proibida ou não autorizada, as Informações Confidenciais.

10.3. Não serão consideradas Informações Confidenciais: (i) informações que sejam ou se tornem domínio público, salvo se em razão de violação de obrigações de confidencialidade assumidas nos termos do Termo ou de qualquer documento que objetive a sua proteção; (ii) informações que forem divulgadas à PARTE receptora por terceiro sem a violação de qualquer obrigação de confidencialidade; (iii) informações que sejam desenvolvidas de maneira independente pela Parte, sem que para tanto recorra à utilização de Informações Confidenciais.

10.4. Na eventualidade de qualquer uma das Partes receber intimação para testemunhar ou depor, ou para prestar a autoridade judicial ou administrativa informações cujo teor implique a divulgação da totalidade ou de parte das Informações Confidenciais, ou ser obrigada a divulgar quaisquer das Informações Confidenciais para o fim de se defender em ação judicial instaurada contra si ou na qual seja parte, então a PARTE receptora concorda desde já em:

i) notificar imediatamente à outra Parte da existência dos termos e circunstâncias relativos à intimação ou da necessidade de defesa, conforme o caso, de forma que possibilite à outra PARTE,

a critério desta, adotar ou requerer qualquer medida cabível para evitar ou mitigar a revelação das Informações Confidenciais; e

ii) cooperar com a outra Parte, tanto quanto possível, na adoção de qualquer medida lícita, judicial ou não, que objetive garantir tratamento sigiloso às informações divulgadas.

10.5. As obrigações estabelecidas na presente Cláusula permanecem em vigor pelo prazo de vigência do Termo e pelo período adicional de 5 (cinco) anos após o seu término, qualquer que seja o motivo.

CLÁUSULA DÉCIMA PRIMEIRA:
DA PROTEÇÃO DE DADOS

11.1. As Partes declaram que cumprem toda a legislação aplicável sobre privacidade e proteção de dados, o que inclui a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet (Lei Federal n. 12.965/2014), seu decreto regulamentador (Decreto 8.771/2016), a Lei Geral de Proteção de Dados (Lei Federal n.13.709/2018), além das demais legislações correlatas vigentes, bem como orientações e diretrizes, regulamentos e procedimentos definidos pela Autoridade Nacional de Proteção de Dados e pelas demais autoridades competentes.

11.2. As Partes se comprometem em utilizar os dados pessoais recebidos no âmbito deste Contrato estritamente para as finalidades a que se destinam, bem como em realizar o expurgo de referidos dados após o período de vigência do Contrato, com exceção dos casos em que houver necessidade de cumprimento de obrigação legal ou regulatória, ou para garantir o exercício regular de direito das Partes.

11.3. As Partes declaram e garantem que adotam as melhores práticas de segurança da informação aptas a garantir a proteção dos dados pessoais contra a violação da confidencialidade, integridade e disponibilidade, incluindo perdas, destruições, alterações, divulgações, usos e acessos não autorizados, sejam esses acidentais ou não.

11.4. Para todos os efeitos, caso ocorra subcontratação pelas Partes, a subcontratada será considerada operadora dos dados, devendo cumprir, no mínimo, as obrigações estabelecidas no presente Contrato. Neste caso, cada Parte será integralmente responsável pelas atividades de tratamento de dados exercidas pela sua subcontratada, bem como por quaisquer incidentes ocorridos no contexto do tratamento, pela subcontratada.

11.5. Cada Parte será responsável pelo tratamento de dados pessoais por ela realizado no contexto do Contrato, mantendo a outra Parte indene de quaisquer danos ou prejuízos decorrentes de operações de tratamento de dados pessoais realizadas em desacordo com o Contrato e/ou com a legislação aplicável.

11.6. As Partes garantem que os dados pessoais eventualmente disponibilizados uma à outra foram obtidos de maneira lícita, legítima, e com base legal adequada, inclusive para o tratamento necessário para o objeto deste Contrato, nos termos da legislação aplicável.

11.7. O **TRT12ª** comunicará a TIM imediatamente, devendo prestar toda a colaboração necessária a qualquer investigação que venha a ser realizada, caso exista alguma quebra de segurança e/ou suspeita da mesma, no sistema utilizado e/ou no envio de e-mail à TIM, independentemente de colocar ou não em risco a segurança e integridade dos dados.

O **TRT12ª** assegurará que seus servidores e ou prestadores de serviços externos por ele contratados que venham a ter acesso aos dados no contexto deste Termo cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais, designadamente não cedendo ou divulgando tais dados pessoais a terceiros, nem deles fazendo uso para quaisquer fins que não os estritamente consentidos pelos respectivos titulares para a finalidade da prestação de serviços pela TIM.

11.8. Sempre que for realizada a transferência de dados pessoais para fora do território brasileiro, as Partes deverão garantir o cumprimento do art. 33 e seguintes da LGPD, em especial, que o tratamento seja realizado em localidade cujo nível de proteção de dados é igual ou superior ao previsto na lei.

11.9. As Partes declaram ciência da Resolução CD/ANPD nº 19/2024, sobre a Transferência Internacional de Dados Pessoais, e se comprometem a: caso o país para o qual os dados pessoais tenham sido transferidos não constar na lista de países adequados da ANPD, transferir os dados para um dos países da lista ou, quando não for possível, realizar aditivo contratual para inclusão da cláusula-padrão prevista na referida resolução.

CLÁUSULA DÉCIMA SEGUNDA
DA FISCALIZAÇÃO E DO ACOMPANHAMENTO

12.1. A fiscalização será exercida por parte do **TRT12ª,** com fundamento no art. 117 da Lei n° 14.133/2021, pela Corregedoria do **TRT12ª**, por meio de servidores por ela indicados:

Gestor: Mariáh Monique Hames	CPF: 084.260.089-25	Cargo: Técnica Judiciária, Coordenadora da Coordenadoria de Reunião de Execuções e Convênios
Gestor Substituto: Rogério Corrêa Borges	CPF: 930.619.860-49	Cargo: Técnico Judiciário, Chefe da Seção de Convênios Judiciais

12.2. O desenvolvimento dos objetivos e metas do presente Termo e a fiscalização da fiel observância das suas disposições serão acompanhados pelo gestor ou seu substituto, representante do **TRT12ª**, e pela **GRAOP**, representando a **TIM**.

CLÁUSULA DÉCIMA TERCEIRA:
DAS DISPOSIÇÕES GERAIS

13.1. Quaisquer comunicações entre as Partes referentes a este Termo só produzirão efeitos se feita por escrito e: (a) entregue em mãos, (b) enviada por correio com Aviso de Recebimento (AR), ou (c) encaminhada em horário comercial de dias úteis por e-mail com confirmação de recebimento do destinatário do e-mail. Para fins das comunicações relativas a este Termo devem ser considerados os seguintes dados e endereços das Partes:

Para a **TIM**:
Endereço: Av Alexandre de Gusmão, 29, Vila Homero Thon, Santo André/SP
Att.: GRAOP
E-mail: infotim@timbrasil.com.br

Para o **TRT12ª**:

Endereço: Rua Esteves Júnior, n o 395, bairro Centro, na cidade de Florianópolis, Estado de Santa Catarina, CEP 88015-905
Att.: Mariáh / Rogério
E-mail: convenios@trt12.jus.br

13.2. As informações contidas no sistema da TIM estão abrangidas pelo sigilo de dados, nos termos do artigo 5º, inciso X e XII 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.

13.3. O acesso ao sistema 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

13.4. O presente Termo corresponde à totalidade do ajuste firmado entre as Partes, não prevalecendo, para qualquer efeito, outras manifestações de vontade eventualmente expressas, salvo se decorrente de lei ou norma regulamentar aplicável.

13.5. Os casos omissos ou quaisquer divergências decorrentes da execução deste Termo serão resolvidos pelas Partes por meio de consulta e mútuo entendimento, observadas as disposições de leis e regulamentos aplicáveis e os princípios gerais de Direito.

13.6. Caberá ao **TRT12ª** fiscalizar a fiel observância das disposições deste Termo e das instruções constantes no Anexo I, sem prejuízo da fiscalização a ser exercida pela TIM.

13.7. A TIM não se responsabilizará por qualquer desconformidade das informações constantes de seu cadastro, uma vez que composto por informações de terceiros, a quem cabe responsabilidade sobre as mesmas.

13.8. A TIM se reserva ao direito de divulgar as estatísticas de consultas realizadas pelo **TRT12ª**, em relatórios de qualquer natureza e aos seus usuários.

13.9. As Partes concordam em alterar o presente Termo para atender exigência da ANATEL – Agência Nacional de Telecomunicações, da Lei Geral de Proteção a Dados (LGPD) ou de qualquer legislação a respeito do objeto aqui contemplado, a cujo cumprimento a TIM esteja obrigada, e ainda, caso seja editada legislação que proíba a TIM de executar o objeto aqui consignado.

13.10. O presente instrumento obriga as Partes, seus sucessores a qualquer título, tendo automaticamente sua titularidade transferida à entidade superveniente, e eventuais cessionários autorizados, sendo que qualquer outra alteração ou modificação contratual só terá validade mediante a celebração de termo aditivo, o qual deverá ser devidamente assinado pelos representantes legais das Partes.

13.11. As Cláusulas deste Termo consolidam o completo entendimento das Partes e prevalecem sobre quaisquer entendimentos firmados anteriormente a respeito do objeto ora contratado.

13.12. As Partes reconhecem e anuem expressamente a veracidade, autenticidade, integridade, validade e eficácia deste instrumento nos termos dos artigos 104 e 107 do Código Civil, assinado pelas Partes em formato eletrônico e/ou por meio de certificados eletrônicos, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

13.13 As Partes concordam que o presente Instrumento constitui título executivo extrajudicial, dispensada a assinatura de duas testemunhas conforme §4º, do Art. 784, do Código de Processo Civil Brasileiro.

13.14 O **TRT12ª** reconhece que todos os documentos apresentados pela TIM que guardem relação com este Contrato (sejam eles Pedidos de Compras, políticas internas, etc), são integrantes deste, e quando aceitos sistemicamente pelo **TRT12ª**, esse aceite equivale a assinatura por seu representante, não podendo o **TRT12ª** alegar qualquer vício de validade para tal documento.

CLÁUSULA DÉCIMA QUARTA:
LEGISLAÇÃO E FORO

14.1. O presente Termo é regido pelas leis brasileiras.

14.2. Fica eleito o Foro de Florianópolis, com expressa renúncia a qualquer outro, por mais privilegiado que seja, para dirimir qualquer dúvida ou litígio oriundos deste Termo.

E, por estarem justas e contratadas, o presente Termo é assinado em quantidade equivalente à das Partes integrantes da relação, em vias de iguais teor e forma.

Florianópolis, 08 de junho de 2026

TERESA REGINA COTOSKY:1345
Assinado de forma digital por TERESA REGINA COTOSKY:1345
Dados: 2026.06.12 13:43:30 -03'00'

TERESA REGINA COTOSKY
DESEMBARGADORA DO TRABALHO-PRESIDENTE
TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO

DocuSigned by:
Heros Fabiano dos Santos
D843819E21A0449...

HEROS FABIANO DOS SANTOS
TIM S/A

JURÍDICO Joyce Franco TIM

ANEXO I AO TERMO Nº 6532/2026
TERMOS E CONDIÇÕES DE USO E POLÍTICA DE PRIVACIDADE
INFOTIM

Seja bem-vindo ao INFOTIM e muito obrigado por fazer uso deste serviço.

O INFOTIM é uma plataforma desenvolvida para a TIM S/A (CNPJ nº 02.421.421/0001-11 por fornecedor contratado por ela e é destinada exclusivamente ao atendimento de servidores e magistrados, amparados em ordens judiciais, na rotina de obtenção de informações de clientes desta operadora para subsidiar processos judiciais em andamento. Esse sistema será utilizado especificamente por servidores e magistrados atrelados à Tribunais de Justiça, à Justiça Federal e à Justiça do Trabalho que possuam Termo para utilização dessa plataforma firmado com a TIM S/A.

Estes Termos e Condições de Uso e Política de Privacidade ("Termo") possuem como objetivo orientar o acesso e a utilização da plataforma INFOTIM.

Este Termo poderá ser alterado a qualquer momento. Nestas condições, o usuário deverá verificar o conteúdo deste documento sempre que possível, certificando-se que se trata da versão mais atualizada, conforme data informada ao fim do documento.

Leia atentamente o conteúdo deste Termo e, em caso de dúvidas, entre em contato com a TIM S/A, através do e-mail infotim@timbrasil.com.br. Ao clicar no botão "aceito", você concordará com a integralidade das condições aqui contidas e considerará válido este Termo como qualquer outro Termo escrito e assinado por Você.

Caso não concorde com todas as condições deste Termo, clique no botão que indica que você não concorda em aceitar as condições deste Termo (se aplicável) e cesse qualquer uso do INFOTIM.

1. **Quem pode utilizar o INFOTIM?**
   Os Magistrados e os servidores públicos alocados em funções nos cartórios judiciais dos Tribunais de Justiça, da Justiça Federal e/ou do Trabalho que necessariamente mantenham vigente Termo para utilização dessa plataforma firmado com a TIM S/A. O Acesso à plataforma somente deverá ocorrer enquanto os usuários exercerem as suas funções e que tenham sido previamente cadastrados, sendo o acesso suspenso imediatamente caso sobrevenha aposentadoria, exoneração ou remanejamento para atividade diversa.

   Importante ponderar que qualquer mal-uso ou uso indevido da plataforma pelo usuário poderá, por liberalidade e sem necessidade de comunicação prévia por parte da TIM S/A, ter seu Acesso interrompido, se submetendo as consequências aplicáveis.

2. **Cadastro e Dados**
   No momento do cadastramento do usuário para uso da plataforma, o servidor do Tribunal de Justiça, da Justiça Federal e/ou do Trabalho, deverá fornecer informações precisas, fidedignas e completas para que o Acesso ao INFOTIM seja liberado, mantendo-as sempre atualizadas, através do e-mail

infotim@timbrasil.com.br. Sendo concluído seu cadastro, lhe serão concedidos **login e senha para uso pessoal e intransferível da plataforma**, sendo que você, neste ato, concorda e aceita com essa condição.

Enquanto estivermos de posse de suas informações, estas poderão ser fornecidos às autoridades competentes para colaboração em investigações ou procedimentos judiciais, ainda que preparatórios ou cautelares, desde que requeridos e permitidos por lei.

Você concorda, ainda, que o seu acesso ao INFOTIM somente se dará através do usuário a você destinado e que não compartilhará seu login e senha com terceiros. O uso ou acesso por qualquer pessoa que não esteja vinculado ao usuário é terminantemente proibido, e você concorda que poderá se submeter as consequências aplicáveis em caso de não observância dessa disposição.

3. A Plataforma

A TIM S/A se reserva ao direito de interromper, a qualquer tempo, parcial ou integralmente o INFOTIM bem como modificá-lo sem previa comunicação.

Este Termo, ou o uso do INFOTIM, não concedem ao usuário quaisquer direitos de propriedade intelectual sobre o INFOTIM. Ao aceitar o presente documento, o usuário reconhece que a licença concedida em sede deste Termo somente lhe fornece direito de utilização limitada do INFOTIM, de acordo com os termos aqui estabelecidos. Assim, o usuário concorda em não modificar, adaptar, traduzir o INFOTIM, nem fazer engenharia reversa, descompilar ou realizar qualquer atividade com o objetivo de descobrir o código-fonte do programa. Por fim, no mesmo sentido, o usuário não poderá remover ou alterar qualquer aviso ou identificação de direito autoral ou quaisquer outros avisos de propriedade intelectual em qualquer cópia do INFOTIM.

4. Segurança

A TIM S/A encontra-se plenamente engajada na segurança dos usuários desta plataforma bem como das informações acessadas. Por esse motivo, solicitamos que, caso note alguma evidência de utilização indevida e/ou não autorizada de seu usuário, nos comunique **imediatamente** através do endereço eletrônico infotim@timbrasil.com.br.

Você concorda e aceita que as informações que poderão ser extraídas através do INFOTIM são sensíveis e de titularidade de terceiros, e que o acesso e uso devem seguir única e exclusivamente o que determina a ordem judicial respectiva. Você deve acessar os dados através do INFOTIM se restringindo apenas no que previu a ordem judicial

O usuário concorda que será o único responsável (e que a TIM S/A não tem qualquer responsabilidade perante o usuário ou terceiros) por qualquer descumprimento de suas obrigações em relação aos Termos e Condições de Uso e Política de Privacidade aqui apresentados, inclusive no que se refere à eventual responsabilização em âmbito civil, penal e/ou administrativo, bem como danos causados a terceiros.

5. Da Responsabilidade

Todos os direitos relacionados ao INFOTIM, bem como todo o conteúdo da plataforma, são de propriedade da TIM S/A.

Você não pode modificar, divulgar, reproduzir, adaptar, explorar ou gravar, vender, distribuir cópias, reproduzir, doar, transferir total ou parcialmente os dados e o conteúdo disponibilizado através do INFOTIM.

Você também não pode realizar engenharia reversa, decompilar, desmontar ou tentar, por qualquer meio, extrair o código fonte ou outras informações confidenciais da TIM S/A. Se, por ação ou omissão, você incorrer nesses tipos de violação, será responsável, perante à TIM S/A e terceiros, por todos e quaisquer danos, multas, custas e despesas decorrentes da violação, sem prejuízo das medidas judiciais cabíveis a serem adotadas pela TIM S/A.

Você deverá manter a confidencialidade das senhas fornecidas, não as compartilhando com terceiros, mesmo que servidores lotados em sua unidade de trabalho.

Deve evitar registrar as senhas em papel ou deixá-la exposta a terceiros e alterá-la periodicamente ou sempre que existir qualquer dúvida quanto a sua confidencialidade;

Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força dos acessos ao sistema INFOTIM.

Não se ausentar da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;

Não acessar e/ou divulgar informações não motivadas por necessidade de serviço e amparadas em ordem judicial.

O usuário concorda em não utilizar o INFOTIM para:

- Quaisquer fins ilícitos ou pessoais, de modo ilegal, prejudicial, ameaçador, abusivo, tortuoso, difamatório, vulgar, obsceno, invasivo da privacidade ou de direitos de propriedade, odioso, ou racial, étnico ou censurável, que possa ferir a privacidade ou outros direitos de terceiros, que prejudique menores de idade de qualquer forma;
- Transmitir qualquer conteúdo (tais como informação privilegiada, propriedade intelectual ou informação confidencial) que o usuário não tem o direito de transmitir sob qualquer lei ou sob relações contratuais ou fiduciárias;
- Transmitir qualquer publicidade não solicitada ou não autorizada, materiais promocionais, "junk mail", "spam", "correntes" e "esquemas de pirâmide";
- Transmitir qualquer material que contenha vírus ou qualquer outro código malicioso, arquivos ou programas projetados para interromper, danificar ou limitar a funcionalidade de qualquer software, hardware ou equipamento de telecomunicações, ou elementos nocivos em dispositivos e no INFOTIM, bem como qualquer conteúdo apto a prejudicar o sistema da Provedora, do Desenvolvedor, dos demais usuários e/ou terceiros; e
- Clonar, alugar, emprestar, arrendar, vender, modificar, descompilar, fazer engenharia reversa ou desmontar o INFOTIM, criar produtos derivados baseados no INFOTIM ou em

qualquer parte dele, reconhecendo, o usuário, que não poderá reduzir qualquer parte do INFOTIM a um formato legível, nem permitir que terceiros o façam.

6. Modificação e Término dos Serviços

Os serviços disponibilizados pela TIM S/A estão em constante atualização e sempre em processo de melhoria. Funções, recursos ou necessidades podem ser adicionados ou modificados. O serviço prestado através do INFOTIM poderá, ainda, ser suspenso ou interrompido completamente sem a necessidade de qualquer comunicação prévia. A TIM não garante a fruição e disponibilização ininterrupta do INFOTIM.

7. Limitação de Responsabilidade

A TIM S/A não se responsabiliza pela aquisição, disponibilização, funcionamento, atualização ou manutenção de quaisquer equipamentos necessários fora da sua rede para a realização do acesso e utilização do INFOTIM, sendo que todos os custos e despesas relacionados aos mesmos são de responsabilidade do Tribunal de Justiça, da Justiça Federal e/ou do Trabalho a qual você esteja afeto.

Sem prejuízo de outras isenções de responsabilidade descritas neste documento, a TIM S/A não poderá ser responsabilizada:

- Por quaisquer indisponibilidades, erros ou falhas do INFOTIM, bem como por qualquer defraudação da utilidade que o usuário possa ter atribuído a este, pela falibilidade do mesmo, nem por qualquer dificuldade de acesso;

- Por qualquer incompatibilidade do INFOTIM com o hardware e/ou componentes de programas instalados em seu hardware ou *device*;

- Pelos danos e prejuízos de toda natureza que possam decorrer do conhecimento que terceiros não autorizados possam ter de quaisquer das informações fornecidas pelo INFOTIM, em decorrência de falha exclusivamente atribuível ao usuário ou a terceiros que fujam a qualquer controle da TIM S/A.

Você reconhece que a TIM S/A não poderá ser responsabilizada por qualquer erro ou mau funcionamento do INFOTIM em caso de violação do descrito no presente documento.

8. Término

Este Termo, bem como todas as eventuais modificações feitas, é válido até o término ou rescisão do Termo firmado entre a TIM S/A e os respectivos Órgãos de Justiça.

Tanto os Órgãos de Justiça quanto a TIM S/A poderão, a qualquer tempo e por qualquer motivo, rescindir o vínculo existente nos termos previstos no Termo de adesão firmado entre as partes.

Ainda, o usuário poderá perder definitivamente o acesso ao INFOTIM em determinadas hipóteses, sem qualquer indenização ou ressarcimento em razão desta finalização de acesso:

- Quando expirado o prazo da licença de uso do INFOTIM;
- A partir de 90 (noventa) dias sem uso ou acesso ao INFOTIM;
- Quando solicitado o cancelamento do acesso pelo Tribunal;
- Caso seja identificada qualquer irregularidade na utilização do INFOTIM ou o não cumprimento deste Termo, bem como de qualquer disposição legal, regulamentar ou normativa, sem que lhe seja devida, pela TIM S/A, qualquer forma de ressarcimento em razão disso.

9. Revisão dos termos

A TIM S/A se reserva o direito de rever, atualizar, alterar, modificar, adicionar, complementar ou excluir determinados aspectos e condições deste termo. Se quaisquer alterações futuras forem inaceitáveis para você ou fizerem com que não esteja mais de acordo ou em conformidade com este termo, a TIM S/A se reserva no direito de rescindir automaticamente este Termo bem como suspender imediatamente seu acesso ao INFOTIM.

10. Política de Privacidade

Garantir a privacidade é de extrema importância para a TIM S/A. Para que a relação com os usuários do INFOTIM seja transparente e segura, apresentamos-lhe esta política.

Esta política se destina a esclarecer quais informações suas são coletadas e como as utilizamos.

1) Quais informações coletamos?

Seus dados Cadastrais são coletados para que possamos criar o usuário que permitirá que você tenha acesso ao INFOTIM e faça uso de suas funcionalidades.

Além dos seus dados cadastrais, também iremos coletar e armazenar os dados de LOG, que é a informação gerada e gravada automaticamente pelo servidor a cada utilização do INFOTIM.

Os dados gerados são, por exemplo, seu número de IP, a data e horário de acesso e saída do sistema (login e logout) além de informações sobre as consultas realizadas e o tempo gasto dentro do sistema.

2) Para que coletamos os seus dados?

Os dados descritos no item anterior são coletados e armazenados para garantir uma maior segurança na disponibilização das informações garantindo que somente servidores e magistrados, previamente cadastrados, acessem as informações confidenciais.

Já os Logs são coletados e armazenados para eventuais questionamentos e/ou auditorias no sistema que venham a ser requeridos pelas autoridades competentes.

Além disso, as informações coletadas podem ser utilizadas para que realizemos modificações e melhorias no INFOTIM para que sua experiência seja mais eficiente e efetiva.

3) Da Segurança

Todas as informações, sejam as suas ou as que possam ser acessadas através do INFOTIM, são de extrema importância e merecem toda a atenção e segurança.

Por esse motivo, o INFOTIM foi desenvolvido com a utilização de recursos de segurança sólidos visando a proteção constante dos dados.

Não poupamos esforços para que o nível de segurança seja o mais elevado possível e para tanto contamos com sua colaboração, que é essencial.

Não divulgue ou compartilhe seu login e senha de acesso ao sistema e após a obtenção dos dados desejados garanta sua proteção mantendo-as a salvo de acessos indevidos e/ou não autorizados.
Após a utilização do INFOTIM sempre realize o logout do sistema para que outras pessoas não sejam capazes de realizar nenhuma ação no sistema através de seu usuário.

4) Alterações desta Política de Privacidade

A TIM S/A se reserva no direito de rever, atualizar, modificar, adicionar, complementar ou excluir determinados itens e condições desta política.
As alterações serão previamente comunicadas e serão efetivas após seu aceite. Se alguma alteração futura à presente política for inaceitável para você ou fizer com que você não esteja mais de acordo com este documento, a TIM S/A se reserva no direito de rescindir automaticamente o seu acesso.

11. Legislação e foro

A presente relação jurídica é regida exclusivamente pelas leis brasileiras, inclusive eventuais ações decorrentes de violação dos seus termos e condições.

Fica eleito o Foro da Cidade onde encontra-se localizada a sede do Tribunal de Justiça, do Tribunal Regional Federal ou do Tribunal Regional do Trabalho a qual você se encontra vinculado para dirimir quaisquer dúvidas, questões ou litígios decorrentes dos presentes Termos, renunciando as partes a qualquer outro, por mais privilegiado que seja.

Florianópolis, 08 de junho de 2026

DocuSigned by:
Heros Fabiano dos Santos
D843819E21A0449...

HEROS FABIANO DOS SANTOS
TIM S/A

ÍNDICE

OBJETIVO E CAMPO DE APLICAÇÃO

Este documento tem o objetivo de formalizar os requisitos de segurança lógica e física (doravante, Requisitos) para a proteção das informações e Ativos TIC/infraestrutura da TIM (doravante, TIM), determinando as regras a serem incluídas no anexo técnico do contrato/contrato de serviços com os fornecedores (doravante, Terceiro).

Os requisitos estão agrupados de acordo com os seguintes temas:

A	Proteção de informação
B	Requisitos de Eventos e Incidentes de Segurança
C	Segurança Física para os Escritórios de Terceiro
D	Estações de Trabalho, Servidores e demais dispositivos de terceiros
E	Sistemas de Informação de Terceiros
F	Infraestrutura de Rede de Terceiros
G	Segurança Física para os Escritórios da TIM
H	Estações de Trabalho da TIM
I	Sistemas de informação da TIM – Acesso e Uso

J	Acesso Local à Infraestrutura de Rede da TIM
K	Acesso Remoto à Infraestrutura de Rede da TIM
L	Serviço de e-mail da TIM
M	Serviço de Conexão à Internet da TIM
N	Continuidade de Negócios
O	Desenvolvimento Seguro de Aplicativos de Software
P	Avaliação de Vulnerabilidade
Q	Serviços em Cloud (Cloud Service Provider)

REQUISITOS PARA TERCEIRO

A política de segurança e outros documentos normativos da TIM devem ser seguidas por terceiro que estejam dentro das dependências da TIM. Os itens relacionados aos capítulos G, H, I, J, K, L e M representam uma parte das orientações.

A. Proteção da informação

No que diz respeito à TIM, informação significa qualquer agregação de dados que tenha um valor e um significado para a TIM, qualquer que seja a forma e as tecnologias usadas para seu processamento e armazenamento. A definição de informação inclui qualquer notícia ou comunicação em forma escrita ou verbal, ou qualquer conjunto de "dados estruturados" processados, comunicados, armazenados (manualmente ou por meios automáticos) e utilizados na execução do trabalho, bem como dados em um arquivo ou código de programa.

1) O terceiro deve garantir que as informações proprietárias da TIM sejam processadas, de acordo com os princípios de "*Need to know*" e "Segregation of Duties", exclusivamente dentro do serviço contratual, evitando a divulgação para/ou na presença de pessoas não autorizadas;

2) O terceiro é obrigado a processar as informações da TIM, seja em TI e/ou em forma de papel, salvaguardando a sua Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade, bem como em conformidade com as leis atuais;

3) O terceiro deve ter completa rastreabilidade dos acessos realizados nas informações da TIM, com o objetivo de identificar origem, autor, data/hora e informação acessada, com tempo mínimo de retenção de 02 (dois) anos;

4) O terceiro que presta serviços, produtos ou equipamentos para à TIM deve obrigatoriamente possuir Política de Segurança Cibernética, preferencialmente, tendo seu resumo publicado em seu Web Site;

5) O terceiro que presta serviços, produtos ou equipamentos para as infraestruturas críticas da TIM deve realizar periodicamente, auditorias independentes e comprová-las de acordo com a solicitação da TIM;

6) O terceiro que manipula, armazena ou fornece informações de dados pessoais da TIM, deve obrigatoriamente, criptografar os dados em repouso e em trânsito;

7) Os terceiros que possuem base de dados com informações confidenciais de propriedade da TIM devem possuir cláusulas de confidencialidade firmadas em contrato.

B. Requisitos de Eventos e Incidentes de Segurança

1) O terceiro deve identificar, internamente, uma estrutura/figura de referência para garantir a segurança do serviço prestado, que tem a tarefa de assegurar as relações entre o terceiro e a TIM para realizar a gestão transversal de todos os aspectos de segurança, comunicando previamente a TIM;

2) O contato com a área de segurança da TIM, para todos os itens abaixo, deve ser realizado através do e-mail csoc@timbrasil.com.br;

3) O terceiro, através do seu Representante de Segurança deve informar imediatamente a TIM em caso de danos, roubo ou perda de ativos de TI contendo informações proprietárias e credenciais de acesso a TIM. Em relação aos casos que envolvem dispositivos de autenticação fortes, o terceiro deve também prever a revogação do certificado contido no dispositivo;

4) O terceiro é obrigado a notificar a TIM sobre todos os eventos, sem discriminação, inclusive os acidentais, e sobre as informações detalhadas relativas, que podem ser consideradas como violações de dados pessoais. Esta comunicação deve ser feita estritamente dentro de até 24 horas a partir do conhecimento dos eventos acima mencionados e enviada por e-mail para a pessoa de contato da TIM a quem o terceiro geralmente se refere na prestação de serviços e ao e-mail da área de Cyber Security citado no item 2. Neste sentido, o terceiro deve preparar ações internas adequadas para garantir essas obrigações (por exemplo, definindo procedimentos apropriados / instruções de operação) e deve garantir assistência a TIM fornecendo prontamente todas as informações adicionais que possam ser solicitadas pela própria, para avaliação e gestão corretas dos casos de potencial violação de dados pessoais;

5) As atividades de gerenciamento e resolução de incidentes devem ser devidamente documentadas e arquivadas, provendo toda linha do tempo do processo de tratamento;

6) Caso seja previsto em cláusulas contratuais, a possibilidade de utilização de outras empresas para execução do contrato, o terceiro deve garantir que esta empresa siga os requisitos expressos neste anexo técnico.

C. Segurança Física para os Escritórios de Terceiro

1) O terceiro, em suas instalações utilizadas para os serviços prestados a TIM, deve adotar proteções preventivas de segurança física e, quando possível, separar fisicamente as instalações utilizadas exclusivamente para prestação do serviço contratado e sendo obrigatório quando for um serviço de atendimento que utilizam dados pessoais, cliente e colaboradores da TIM;

2) O terceiro deve manter um controle de acesso físico às instalações da empresa para colaboradores e visitantes;

3) O terceiro deve possuir um sistema de CFTV com gravação e armazenamento das imagens por pelo menos 30 dias on-line.

D. Estações de Trabalho, Servidores e demais dispositivos de terceiros

Para as estações de trabalho, servidores e demais dispositivos utilizados pelo terceiro, incluindo qualquer mídia de armazenamento removível (como pen drives USB, discos rígidos externos etc.), usada para o desempenho das atividades de trabalho previstas no contrato/acordo firmado com a TIM, o terceiro deve assegurar que:

1) Não devem ser usadas de maneira que possam causar danos às informações da TIM;

2) O acesso deve ser realizado por meio de credenciais de acesso individual, composto por combinação de uma credencial de identificação (UserID) e uma credencial de autenticação (senha forte, sempre que viável, com a utilização de duplo fator de autenticação, como: PIN);

3) As atualizações de software do sistema e de aplicativos necessárias para corrigir defeitos e evitar vulnerabilidades devem ser instaladas, mensalmente, com o objetivo de manter esses equipamentos sempre atualizados e protegidos. Para os casos de atualização de software de alta criticidade, a mesma deve ser realizada imediatamente;

4) Devem estar equipados com software antivírus, atualizados constantemente e com a função "monitor" sempre ativo, inclusive com Light Scan diário e Full Scan semanal. Além disso, a menos que tenham alguma restrição técnica, a possibilidade de desativar o antivírus pelo usuário deve ser inibida. Caso ocorra algum incidente com vírus, o usuário do fornecedor ou parceiro comercial deve comunicar o incidente ao contato de segurança;

5) Os dados de propriedade da TIM não devem ser salvos, exceto nos casos em que isso é previsto por contrato para atender às finalidades do serviço/atividade. Caso haja necessidade, prevista em contrato, de armazenamento das informações em mídias removíveis, as mesmas deverão ser criptografadas e devem ser removidas de todos os equipamentos no final da atividade;

6) A função de proteção de tela protegida por senha deve ser sempre ativada nas estações de trabalho de terceiros;

7) As estações de trabalho de terceiro quando conectadas às redes que lidam com os recursos da TIM:

   - Devem estar equipadas com Firewalls Pessoais ativos, sendo desejável também Host IPS ou EDR/XDR;
   - Devem estar livres de software contendo ferramentas capazes de permitir que sistemas certificados na Internet interajam, acessem ou gerenciem sistemas corporativos, por meio de fluxos de comunicação encapsulados no tráfego transmitido por proxies corporativos (por exemplo, Log Me In, Go to my PC);
   - Elas não devem ser usadas como dispositivos de ponte (chamadas pontes) para a interconexão de redes logicamente ou fisicamente segregadas, em particular em estações de trabalho de terceiros equipadas com mais de uma interface de conexão (por exemplo, placa de rede e modem presente em uma estação de trabalho de terceiro móvel). Elas nunca devem ser usadas simultaneamente;
   - Devem ter acesso a internet restrito e controlado por proxy com políticas de proteções a sites maliciosos, a fim de proteger qualquer tipo de acesso indevido que exponha a estação de trabalho ou ambiente em risco;
   - Devem estar com patches atualizados semanalmente.

8) As mídias físicas usadas no servidor que hospedam o sistema devem passar por um processo de

destruição das informações antes de serem descartadas;

9) Deve existir uma rotina de manutenção adequada dos servidores que hospedam o sistema;

10) As manutenções dos equipamentos (servidores que hospedam o sistema) devem ser realizadas:
    - com intervalos indicados pelo fornecedor de hardware;
    - somente por pessoal autorizado e identificado.

E. Sistemas de Informação de Terceiros

Sistemas de informação de terceiros são os sistemas, plataformas ou, mais geralmente, as ferramentas tecnológicas físicas e lógicas dos terceiros através das quais a informação/dados da TIM são processados. Para estes sistemas de informação, o terceiro deve assegurar que:

1) Eles sejam mantidos em instalações protegidas e com acesso controlado;

2) Qualquer software instalado em sistemas de informação deve ser legalmente licenciado;

3) Exista um software antivírus atualizado sempre que houver versões disponíveis;

4) Os sistemas operacionais e aplicações, devem estar sempre atualizados, seguindo no mínimo as recomendações de Segurança do Padrão OWASP TOP10, sempre que aplicável. Sejam efetuadas reconfigurações apropriadas para a modificação/eliminação das configurações da aplicação e padrões do sistema, como senhas, comunidade SNMP, contas e serviços desnecessários;

5) Deve ocorrer a resolução de vulnerabilidades de segurança conhecidas de acordo com os padrões de proteção;

6) Todo ambiente deve ser protegido por Firewalls e IDS, assim como ter as devidas segregações de redes, a fim de proteger a infraestrutura, deixando exposto apenas o front-end e a camada de exposição. Além disso, para sistemas expostos na internet deve ter WAF (Web Application Firewall);

7) Os Patches críticos (de SO, BD, Web, etc.), que obrigatoriamente devem ser aplicados no sistema, devem ser testados antes da aplicação para garantir que não haja interrupção do funcionamento do sistema;

8) Sejam adotados procedimentos de backup e restore adequados que contemplem dados da TIM, em concordância com o gestor do contrato. Estes procedimentos devem ser documentados e conter pelo menos a indicação da frequência, dos métodos de execução, do arquivamento e da retenção dos backups. Os dados devem ser mantidos apenas pela duração do período contratual, após isso, os mesmos devem ser entregues a TIM e eliminados;

9) No caso de danos ou incidentes nos seus sistemas de informação, devem ser adotados procedimentos operacionais específicos para a execução das atividades de restauração, que devem incluir tempos de implementação acordados com o gestor do contrato e que garanta a continuidade do serviço contratado pela TIM;

10) Para sistemas de informação que processam dados pessoais de propriedade da TIM, o

armazenamento, e transmissão de dados devem ser realizados de forma criptografada, garantindo que não haja vazamento de informações;

11) Todos os usuários de acesso (incluindo os sistemas técnicos e M2M) devem ser identificados e gerenciados de acordo com procedimentos definidos e documentáveis seguindo melhores práticas de segurança de mercado, que permitam fornecer evidências das autorizações emitidas para usuários individuais;

12) Em caso de Webservices disponíveis para internet ou no Front-End do sistema, devem ser considerados autenticação com certificado digital e protocolo seguro (HTTPS – HTTP Secure).

13) Todos os usuários devem receber credenciais de acesso individuais, contendo um UserID e uma senha. Os UserIDs de um usuário não devem ser atribuídos novamente a outros usuários, mesmo em momentos diferentes, devem ser desativados para manter todo o histórico dos usuários. Para usuários técnicos, o histórico documentado de liberação/uso deve ser fornecido;

14) A utilização de credenciais de acesso para usuários sistêmicos M2M deve ser utilizada apenas em caráter de Troubleshooting, de forma monitorada e após o uso, a senha deve ser alterada;

15) Caso o terceiro possua servidores em sua infraestrutura que vão se comunicar com os servidores da Tim, o mesmo deverá ter um cofre de senhas;

16) Os perfis de autorização definidos, para acesso aos dados do Ativo TIC, devem ser atribuídos com os privilégios proporcionais às necessidades mínimas para o desempenho das atividades/serviços contratados pela TIM (*Need to Know e* Segregation of Duties) esses perfis devem ser identificados e configurados antes do início do processamento para documentar os perfis que podem ser associados para cada usuário ou para um conjunto de usuários que executam a mesma função;

17) A administração de contas de usuários do sistema e manutenção de perfis deve ser realizada através de perfis de acessos distintos;

18) Os usuários devem utilizar diferentes perfis, com nomes distintos para cada ambiente, de forma que se diminua risco de erro acidental;

19) Uma verificação periódica de credenciais e perfis de acessos à sistemas devem ser realizada, pelo menos a cada três meses, e documentada em relação à necessidade de manter válidos os perfis definidos e às autorizações concedidas aos usuários;

20) Os acessos dos usuários que não estiverem mais atribuídos ao serviço da TIM ou que não precisem mais acessar os dados da TIM devem ser imediatamente removidos, a fim de impedir acessos indevidos as informações. Além disso, os acessos devem ser:

- Removidos, devido à inatividade, após 3 meses do último acesso realizado;
- Suspenso, após várias tentativas de logon incorretos;
- Suspenso como resultado de uso ilegal ou daqueles que colocam em risco a segurança. podendo ser solicitado também pelas empresas da TIM;
- Removido na data de expiração especificada na solicitação de autorização (a menos que seja

estendida).

21) Em casos de sistemas, a senha de acesso aos seus sistemas de informação deve atender, no mínimo, às seguintes características:

- Composta por pelo menos 8 caracteres (pelo menos 1 caractere numérico, pelo menos 1 caractere alfabético, pelo menos 1 caractere especial, e não pode conter 3 ou mais caracteres idênticos consecutivos);
- Deve ser alterada no primeiro acesso;
- Deve ser substituída pelo menos a cada três meses (somente logins nominais atribuídos a um indivíduo) e a nova senha deve diferir das dez anteriores;
- Deve possuir um segundo fator de autenticação;
- As senhas devem ser armazenadas de forma criptografada (não em texto claro);
- Controle de Sessão: Deve existir um tempo limite para sessões inativas no sistema;
- O sistema deve bloquear o usuário após 10 tentativas incorretas de acesso.

22) Para as senhas dos acessos S2S, não visualizadas através dos sistemas de mascaramentos, o sistema deve exigir que seja definida uma senha contendo no mínimo 8 caracteres;

23) Medidas adequadas sejam implementadas para o rastreamento dos usuários e administradores do sistema de terceiros. Essas medidas devem incluir a geração, coleta e armazenamento de registros de acesso (login e logout) e todas as demais ações realizadas por esses acessos para os quais a integridade, a não repetibilidade e o não-repúdio devem ser garantidos. Além disso, estas informações devem ser armazenadas por um período mínimo de 2 anos;

24) Todo sistema e infraestrutura de atendimento para a TIM sejam avaliados semestralmente por meio de testes de Invasão e análise de vulnerabilidades, assim como todos os controles e ferramentas de proteção devem ser medidos e reportados para a TIM;

25) Documentações do sistema devem ser guardadas de forma segura onde somente pessoas autorizadas tenham o acesso;

26) O acesso ao código fonte do sistema deve ser estritamente controlado com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais;

27) As informações referentes a autenticação do usuário (login e senha) devem ser trafegadas de forma segura através de criptografia;

28) Deve existir controle de mudanças (Change Management) adequado que contemple itens como:

- Identificação e registro de mudanças significativas que ocorreram com identificação de data, horário, autores e razão;
- Planejamento e teste de mudanças;
- Avaliação de impactos potenciais de mudanças;

- Comunicação das mudanças com as pessoas envolvidas;
- Procedimentos de recuperação ou reversão de mudanças para o caso de eventos inesperados".

29) Deve ser verificado se a capacidade do sistema suportado pelos recursos de hardware/software disponibilizados para execução é apropriada para a carga de trabalho atual;

30) Devem ser feitas projeções futuras sobre necessidades de capacidade que o sistema possa vir a ter e, com isso, planejar as alterações de recursos de hardware/software necessárias;

31) Os relógios dos servidores que hospedam o sistema devem estar sincronizados com um relógio central do domínio e caso o sistema conte com seu próprio relógio, este deverá estar sincronizado com um relógio central do domínio;

32) Os dados de entrada no sistema devem ser validados para garantir que são corretos e apropriados e devem ser verificados valores fora de faixa, caracteres inválidos em campo de dados, dados incompletos ou faltantes, volume dados excedendo limites superiores ou inferiores e procedimentos para tratar erros de validação.

F. Infraestrutura de Rede de Terceiros

A infraestrutura de rede de terceiros refere-se ao conjunto de equipamentos/plataformas de Ativos TIC localizados nos escritórios do terceiro, dentro dos quais os Ativos TIC/estações de trabalho de terceiros que lidam com informações/dados de propriedade da TIM são atestados.

O terceiro, que realiza atividades em nome da TIM exclusivamente dentro de sua própria infraestrutura de rede, deve garantir que:

1) A parte da rede na qual os sistemas de informação e as estações de trabalho de terceiros são identificados e autorizados a acessar/processar os recursos da TIM, deve ser mantida isolada de outras redes, pelo menos em um nível lógico;

2) Os sistemas de informação e dados relacionados residam em redes (ou partes da rede) protegidas por um ou mais firewalls e IDS, nos quais a implementação de regras destinadas a combater tentativas de acesso não autorizado é garantida;

3) Exista um sistema para monitorar o acesso à sua parte da LAN na qual as estações de trabalho de terceiros de seus usuários que trabalham para a TIM são atestadas, a fim de detectar quaisquer anomalias ou ameaças que possam comprometer a segurança dos Recursos da TIM;

4) Caso seja necessário, apenas para fins do serviço/atividade contratada, interconectar a rede de acesso aos recursos da TIM com a rede pública (Internet), essa interconexão não pode ocorrer diretamente. Ela deve incluir mecanismos de proteção, como por exemplo, proxy ou gateway de acesso. Sob nenhuma circunstância, os recursos de rede de terceiros, responsáveis pelo acesso / processamento dos Recursos da TIM, podem ser exibidos diretamente na Internet.

G. Segurança Física para os Escritórios da TIM

1) O terceiro deve seguir os processos de segurança física da TIM.

H. Estações de Trabalho da TIM

As Estações de Trabalho fornecidas pela TIM para executar as atividades de trabalho exigidas pelo contrato/acordo. As estações de trabalho de terceiros são tipicamente equipadas com uma configuração básica padrão que pode variar dependendo da tarefa específica coberta pelo terceiro. A responsabilidade pelo uso e custódia corretos das estações de trabalho de terceiros é do terceiro, que:

1) Não deve modificar de forma independente a configuração padrão de hardware/software presente na estação de trabalho da TIM. Além disso, não deve instalar outro software além daqueles fornecidos e/ou autorizados pela TIM para a realização de tarefas de trabalho;
2) Não deve usar a estação de trabalho de maneira diferente do estabelecido no contrato firmado entre as partes;
3) Não deve impedir ou atrasar a atualização centralizada do software. Se não houver atualizações automáticas para um software específico, ele deve ser atualizado manualmente, de acordo com as instruções fornecidas pela TIM;
4) Não deve instalar software/ferramentas além daquelas fornecidas e/ou autorizadas pela TIM, incluindo:
    - Software de comunicação VoIP (Voice over IP);
    - Ferramentas de controle remoto (por exemplo, Log Me In etc.);
    - Software destinado a criar uma rede compartilhada (como as redes virtuais peer-to-peer).
5) Deve garantir que o protetor de tela seja protegido por senha e o Personal Firewall esteja sempre ativado nas estações de trabalho da TIM usadas por seus usuários.

I. Sistemas de informação da TIM – Acesso e Uso

Os *sistemas de informações* da TIM são sistemas gerenciados/próprios da TIM nos quais as informações são acessadas pelo terceiro.

1) A TIM comunica as credenciais para acessar os seus sistemas de informações, consistindo em um UserID e uma Senha (*autenticação padrão*) ou um código de autenticação de dois fatores (*autenticação forte*), quando necessário, para a pessoa de contato terceirizada que deve garantir a confidencialidade. Essas credenciais podem ser suspensas pela TIM e, posteriormente, encerradas:
    - Devido à inatividade;
    - Após várias tentativas de acesso incorretas;

- Como resultado de uso ilegal ou daqueles que colocam em risco a segurança dos Recursos da TIM, a critério exclusivo da TIM;
- Na data de expiração especificada na solicitação de autorização (a menos que seja estendida);
- Caso o usuário tenha saído do terceiro ou foi avisado pela TIM para remover.

2) Todo os envolvidos no processo de gerenciamento de acessos deve garantir que a entrega de cada credencial de acesso aos respectivos usuários, seja realizado através de um procedimento adequado que associe cada usuário a uma credencial, garantindo que não seja atribuído a outros usuários mesmo em momentos diferentes. O terceiro deve garantir a confidencialidade da entrega (exemplo: uso de envelope fechado ou e-mail interno do fornecedor).

   Além disso, o terceiro, sem prejuízo da presença de controles automáticos nos sistemas da TIM, deve dar instruções apropriadas aos seus usuários sobre como compor senhas fortes e de difícil adivinhação para acessar os sistemas da TIM.

   O terceiro é obrigado a fazer com que seus usuários mantenham as credenciais de acesso atribuídas a eles, para tratar/acessar os Ativos TIC da TIM, a fim de garantir a absoluta confidencialidade e impedir seu compartilhamento.

3) O terceiro deve solicitar ao gestor do contrato a remoção imediata dos acessos em caso de desligamento ou transferência de função do usuário.

4) O terceiro deve realizar uma auditoria periódica e documentada, pelo menos trimestral, sobre a necessidade de manter as credenciais válidas para os usuários conectados a ele, informando imediatamente a TIM sobre a necessidade de suspender/encerrar os usuários dispositivos correspondentes a pessoal não designado ao serviço da TI, ou que, em qualquer caso não precisa mais acessar os dados da TIM. Além disso, os dispositivos de autenticação devem ser devolvidos à TIM quando não forem mais necessários para executar a atividade de trabalho (por exemplo, para uma mudança de funções) ou no final do contrato de serviço.

5) Toda automação RPA (Robotic Process Automation) desenvolvida interna ou externamente deverá seguir o processo oficial da TIM, garantindo dentre outras coisas, a gestão de acesso e perfil, o inventário e avaliação de impacto da TI da aplicação.

J. Acesso Local à Infraestrutura de Rede da TIM

O acesso direto à infraestrutura de rede da TIM, a partir de um escritório da TIM, pode ser feito conectando o dispositivo à rede Wi-Fi dedicada ao pessoal externo ou conectando o dispositivo à infraestrutura de rede TIM através de um cabo de rede e seguindo os processos de validação da TIM. No acesso local, o terceiro:

1) Não deve instalar seus próprios pontos de acesso, criar redes paralelas e configurar sua própria rede Wi-Fi para estabelecer uma conexão com a rede TIM. A conexão a serviços Wi-Fi só é permitida por meio de sua placa wireless, usando a infraestrutura Wi-Fi fornecida pela TIM;

2) Não deve usar simultaneamente múltiplos pontos LAN fornecidos pela TIM através do uso de

dispositivos de rede (por exemplo: HUB, switch, roteador). O possível uso desses dispositivos pode ser permitido somente em casos limitados de emergência real e com autorização formal prévia e documentada da pessoa de contato de segurança da TIM;

3) Não deve realizar qualquer tipo de atividade que possa danificar o serviço ou a infraestrutura da rede TIM. Abaixo estão listadas, a título de exemplo, algumas atividades consideradas ilegais:

- Varredura de portas: identificação dos sistemas conectados à rede TIM;
- Varredura de vulnerabilidades: identificação de vulnerabilidades presentes nos sistemas de informação;
- Identificação de senhas: atividades destinadas a violar as credenciais definidas no sistema de informações de destino (ataque de força bruta, adivinhação de senha, captura de senha hash);
- Sniffing: atividade que consiste em interceptar, através de ferramentas apropriadas, o tráfego de rede nos segmentos da rede interna, definindo no modo promíscuo a placa de rede;
- Spoofing: uma atividade que consiste em forjar a identidade de um sistema de informações na rede, adquirindo o endereço IP associado ou seu endereço MAC;
- Descoberta de rede: atividade que permite derivar, com ferramentas específicas, a topologia de uma rede e a presença nela dos diferentes sistemas (roteador, switch, firewall, host);
- Fingerprinting do sistema operacional: atividade que permite estabelecer o tipo de sistema operacional de um sistema de informação;
- Footprinting: visa descobrir nos ativos da rede, qualquer informação que possa ser válida para posteriormente realizar um teste de invasão;
- Testes de penetração: uma atividade que consiste em avaliar a robustez dos ataques de um sistema de informação;
- Redirecionamento e modificação de tráfego: redirecionamento ou modificação de fluxos de tráfego de rede para sistemas de informação ou sistemas que não sejam os definidos pelas funções competentes.

K. Acesso Remoto à Infraestrutura de Rede da TIM

A infraestrutura de rede da TIM refere-se ao conjunto de equipamentos/plataformas de Ativos TIC que permitem conexões à parte da rede de terceiros, que devem acessar os sistemas da TIM.

1) A interconexão remota de um escritório de terceiros para a infraestrutura de rede TIM é permitida através dos seguintes tipos de conexões: Rede Privada Virtual cliente – para - Rede (VPN C2L) ou Rede Privada Virtual – para – Rede (VPN L2L).

2) O terceiro deve garantir que o canal de comunicação das conexões VPN (C2L e L2L) está equipado com proteção criptográfica dos dados em trânsito.

3) Nas conexões VPN C2L, o cliente de terceiros deve ser configurado de tal forma que:

   - Encapsulamento dividido seja proibido, ou seja, não é permitida a capacidade de enviar tráfego para fora do gateway IPsec;
   - Somente a interface de rede usada para a conexão VPN esteja habilitada. Se isso não for viável, um firewall pessoal deve ser configurado no cliente para bloquear tráfego de rede desnecessário e não autorizado em todas as interfaces.

4) Em conexões VPN L2L, é necessário que:

   - O terceiro deve fornecer ao representante de segurança da TIM a documentação técnica específica relacionada à sua infraestrutura de rede, a fim de permitir a preparação, pelos departamentos de engenharia relevantes da TIM, de um documento técnico que especifique, em detalhes, as condições/modo da conexão (por exemplo, IP público do gateway de terminador de VPN, plano de IP/endereçamento de origem, número das estações de trabalho do terceiro conectadas em VPN, criptografia). Este documento deve ser aprovado e assinado pelo terceiro, como parte integrante e substancial do relacionamento (contrato de fornecimento, licitação, NDA, etc.) que foi assinado entre o terceiro e a TIM;
   - O terceiro deve garantir que a parte da rede, na qual as estações de trabalho identificadas estão autorizadas a acessar a infraestrutura de rede da TIM, esteja isolada das outras redes, pelo menos em um nível lógico. Esta LAN também deve ser protegida por um Firewall de terceiros, o que garante a implementação das regras necessárias apenas para o fornecimento do objeto do serviço.

5) O terceiro deve formular (através de sua pessoa de contato da TI) uma solicitação para habilitar o acesso remoto à infraestrutura da Rede da TIM, de acordo com as instruções da TIM.

6) O terceiro não deve executar qualquer tipo de atividade que possa causar danos ao serviço ou infraestrutura de rede da TIM (por exemplo, varredura de portas, varredura de vulnerabilidades, identificação de senhas, sniffing, spoofing, descoberta de rede, impressão digital do sistema operacional, testes de penetração, redirecionamento e modificação de tráfego).

7) O terceiro deve realizar, internamente, atividades de verificação periódica, com o objetivo de averiguar a implementação de medidas de segurança para conexões entre sua própria rede e a rede da TIM.

L. Serviço de e-mail da TIM

Caso o terceiro receba conta(s) de acesso ao domínio de e-mail da TIM, o mesmo deve utilizá-las exclusivamente para o desempenho da atividade de trabalho decorrente das obrigações contratuais, observadas as obrigações legais vigentes e de acordo com as seguintes regras comportamentais:

1) Não deve compartilhar sua caixa de correio com outros usuários;

2) Não deve executar programas recebidos como anexos de mensagens de e-mail, baixando-os de sites ou usando mídia removível;

3) Não deve clicar em links de origens desconhecidas;

4) Não deve inserir seus dados de login clicando diretamente nos links oferecidos em um e-mail;

5) Reportar através do botão "**Denunciar Phishing**" ou enviar como anexo para DL_phishing e excluir imediatamente, sem abri-los, e-mails de origem desconhecida e/ou com conteúdo suspeito.

M. Serviço de Conexão à Internet da TIM

Caso o terceiro acesse a Internet por meio de conexões da TIM, ele deve utilizá-la exclusivamente para o cumprimento da atividade de trabalho decorrente das obrigações contratuais, excluindo-se a navegação de sites não relacionados a essas atividades, no cumprimento das obrigações da lei em vigor e de acordo com as seguintes regras comportamentais:

1) Usar software ou outras ferramentas para compartilhar arquivos apenas para os propósitos contratuais;

2) Não deve modificar/mascarar as configurações de rede (por exemplo: endereço IP ou endereço MAC) ou ignorar/desabilitar os dispositivos responsáveis pelo gerenciamento de segurança e comunicações de rede (por exemplo: Firewall, Proxy, Roteador);

3) Não é permitido baixar arquivos executáveis se a fonte for desconhecida;

4) Não deve usar a conexão para executar qualquer atividade que possa, mesmo que potencialmente, causar mau funcionamento, reduzir a eficiência do serviço ou causar danos de qualquer tipo (por exemplo: uso de software ponto-a-ponto);

5) A utilização da Internet é permitida apenas para fins lícitos, de acordo com as disposições legais vigentes e aplicáveis ao Código de Ética e Conduta do Grupo TIM no Brasil;

6) O acesso à Internet disponibilizado pela TIM para desenvolver sua atividade profissional, é de propriedade da Empresa e tem natureza exclusiva de ferramenta de trabalho. Assim, a utilização da Internet deve ser feita de forma correta, exclusivamente para fins profissionais, voltada somente para o acesso às informações relacionadas com as atividades de interesse da TIM;

7) Não é permitido utilizar a conexão à internet para:

   - Trocar e/ou divulgar dados, áudio, vídeo, foto ou arquivos executáveis desnecessários ou incompatíveis com a atividade de trabalho;
   - Contornar ou tentar desabilitar os sistemas automáticos implantados pela empresa para garantir a segurança da navegação e controle de conteúdo;
   - Manifestar-se em nome e por conta da TIM, salvo autorização prévia.

8) Transferir através da Internet informações corporativas sem a prévia autorização da empresa, exceto as informações classificadas como **públicas**, já divulgadas na imprensa.

N. Continuidade de Negócios

Em relação à Continuidade de Negócios, o terceiro deve apresentar:

1) Planos de recuperação para a continuidade dos serviços prestados à TIM, para casos de ocorrência de interrupção/incidente, devendo prever, no mínimo, os casos de indisponibilidade de Ativos TIC, indisponibilidade de escritórios e indisponibilidade de pessoal;

2) Evidências de que os respectivos planos foram testados ao menos semestralmente;

3) Identificação de canais e formas de comunicação imediata de incidentes que geram interrupção dos serviços, podendo ser de acordo com o item B - 1;

4) Devem ser realizados periodicamente testes de recuperação (“Restore”) sobre as cópias de segurança.

O. Desenvolvimento Seguro de Aplicativos de Software

A TIM considera que a mitigação de vulnerabilidades de segurança é fundamental para todos os tipos de aplicativos adquiridos por terceiros, tanto do tipo "Buy" - software para o qual a TIM não tem acesso direto ao código - quanto do tipo "Make" - software dos quais a TIM possui a propriedade intelectual do código-fonte.

Esse conjunto de requisitos deve ser considerado aplicável a todos os tipos de software, incluindo aplicativos móveis desenvolvidos para diferentes plataformas (por exemplo: Android, iOS e Windows Phone).

Deve existir documentação formal de procedimentos de operação no sistema relacionados a formas que o sistema processa e trata as informações, objetivo do sistema, rotinas de backup no sistema, instruções para tratamento de erros que possam ocorrer no sistema, dados para contato de suporte para eventos operacionais inesperados ou dificuldades técnicas, gerenciamento de logs e procedimentos para reinício e recuperação em caso de falha.

Deve existir separação lógica entre ambientes de desenvolvimento, teste e produção.

As regras para transferência do sistema do ambiente de desenvolvimento para os ambientes de teste e produção devem ser documentadas

Os requisitos, listados abaixo, também são divididos de acordo com o diferente nível de exposição dos sistemas de TI ou dos aplicativos de software fornecidos.

Para todos os tipos de aplicativos de software fornecidos, o terceiro deve garantir:

1) A ausência de vulnerabilidade no código, para todos os módulos de software que compõem o objeto de aplicativo de software do suprimento (mesmo aqueles que não foram desenvolvidos diretamente) e, em qualquer caso, das seguintes categorias que se referem aos padrões internacionais "OWASP" e "SANS Institute":

   - OWASP Top10 / OWASP MOBILE Top10: eles representam os 10 riscos mais críticos para a

segurança de aplicativos da web:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- SANS Top25: representam os erros mais comuns e críticos que podem levar a sérias vulnerabilidades no software, geralmente fáceis de encontrar e de explorar. Esses erros frequentemente permitem que os invasores assumam os dados ou impedem o funcionamento do software:

https://www.sans.org/top25-software-errors/

2) As atividades de análise do código fonte tenham sido realizadas e todas as vulnerabilidades detectadas tenham sido removidas. Isto deve ocorrer por meio de processos baseados nos padrões do setor, para todos os módulos de software do aplicativo que estão sendo fornecidos (mesmo aqueles que não foram desenvolvidos diretamente). Em particular, em cada versão do software, ele deve produzir documentação adequada indicando:

- Lista de módulos / bibliotecas que compõem o software lançado;
- As ferramentas utilizadas para a análise (código estático e dinâmico);
- Número de linhas de código digitalizadas;
- Número de vulnerabilidades identificadas divididas em classes de criticidade;
- Evidência das ações de reembolso realizadas.

5) O Fornecimento à TIM das licenças para uso de todos os módulos de software que compõem o objeto aplicativo do fornecimento;

6) Caso tenham dados de cartão de créditos, os aplicativos de software devem ser desenvolvidos de acordo com o padrão PCI-DSS.

Para sistemas internos de TI e sistemas expostos na Internet, o terceiro deve garantir:

1) Quando exigido, que:

- Sejam fornecidas à TIM todas as versões e pacotes dos principais lançamentos de software;

Adicionalmente, o terceiro deve garantir que estejam disponíveis as evidências que atestam:

- A ausência de vulnerabilidade após verificações de todos os componentes de software do tipo "Make" ou "Buy" que estão sendo fornecidos (por exemplo: componentes Web Application, APP Móvel, API gateway, interfaces de IoT, componentes de back-end), incluindo estruturas de código aberto;
- A realização das análises de vulnerabilidades e testes de invasão antes da entrada em produção e, periodicamente, realizar a apresentação do report. dos resultados para a TIM e as eventuais correções aplicáveis.

2) Que sejam realizadas atividades de análise de risco, por meio de processos baseados em padrões de mercado, incluindo sistemas expostos na internet e aplicativos móveis. Estes sistemas devem

atender aos seguintes requisitos, em particular:

- O licenciamento de componentes de código aberto não deve ser do tipo "Strong Copyleft";
- Os componentes não devem ser usados sem o licenciamento declarado;
- As "obrigações" subjacentes a cada licença sempre devem ser cumpridas.

P. Avaliação de Vulnerabilidade

Caso sejam identificadas vulnerabilidades técnicas durante os testes de segurança realizados pela TIM ou mesmo incidentes tecnológicos de segurança e privacidade, identificados por qualquer outro meio (imprensa, fóruns de segurança, programas de Bug Bounty, etc) na plataforma de sistemas desenvolvida pelo terceiro, esta, após informada oficialmente (por e-mail) pela TIM, deve saná-las no período sinalizado, de acordo com o previsto nas Tabelas 1 e 2- Tempo previsto de correção, onde a classificação de criticidade é indicada através do modelo CVSS (Common Vulnerability Scoring System) ou comprovar tecnicamente a não aplicabilidade para a correção. O Terceiro será responsável pelos custos da implementação das vulnerabilidades identificadas.

A TIM se reserva no direito de realizar testes de vulnerabilidade e invasão a qualquer tempo, sem necessidade de aviso prévio ao terceiro.

Para fins de validação por parte da TIM, um novo teste é realizado para comprovação das correções. Os testes são repetidos até que todas as vulnerabilidades sejam totalmente sanadas pelo terceiro.

O terceiro também deve realizar testes independentes e sanar, preventivamente, vulnerabilidades identificadas ou informadas por fabricantes, com o objetivo de manter sua infraestrutura atualizada e segura, seguindo as melhores práticas de cibersegurança mundiais e em linha com o item **O. Desenvolvimento Seguro de Aplicativos de Software**, constante neste documento.

O não cumprimento destes itens podem ser considerados como um descumprimento contratual ou omissão na prestação de serviços.

Sendo a tabela abaixo, aplicada exclusivamente para vulnerabilidades encontradas através de testes de invasão **em aplicações expostas na Internet:**

Nível	Tempo de correção/mitigação	Exceção
Crítica	Responder ao e-mail imediatamente, assim que informada. Sendo que a mitigação não pode ultrapassar o período de 4 horas.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).

Alta	Responder ao e-mail imediatamente, assim que informada. Sendo que a mitigação não pode ultrapassar o período de 48 horas.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Média	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar 15 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.
Baixa	Responder ao e-mail imediatamente, assim que informada. Não podendo ultrapassar os 30 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.

Tabela 1 - Tempo previsto de correção (aplicações expostas)

Sendo a tabela abaixo aplicada para as **demais aplicações**:

Nível	Tempo de correção/mitigação	Exceção
Crítica	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar o período de 15 dias.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Alta	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar o período de 30 dias.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM. Neste caso, há avaliação por parte da TIM sobre a possibilidade de desativação temporária do Ativo TIC, até que a correção seja realizada (ficando sob responsabilidade

		do terceiro as penalidades previstas em contrato pela quebra do SLA de disponibilidade).
Média	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar 45 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.
Baixa	Responder ao e-mail imediatamente, assim que informada. Sendo que a correção não poderá ultrapassar os 60 dias corridos.	Em casos de comprovação de impossibilidade técnica e aprovada pela TIM.

Tabela 2 - Tempo previsto de correção demais aplicações

Q. Serviços em Cloud (Cloud Service Provider)

Caso o terceiro seja um CSP (Cloud Service Provider) ou o serviço prestado utilize um CSP para o armazenamento das informações, a TIM solicita que:

1) O CSP (Cloud Service Provider) forneça todas as respostas ao CCM do CSA.

   O Cloud Security Alliance (CSA) mantém o Registro de Segurança, Confiança e Garantia (STAR). Trata-se de um registro gratuito e acessível ao público, no qual os provedores de serviços de nuvem podem publicar suas avaliações relacionadas ao CSA. A Certificação STAR consiste em três níveis de garantia alinhados aos objetivos de controle no Cloud Controls Matrix (CCM) do CSA. O CCM abrange princípios fundamentais de segurança em 16 domínios para auxiliar os clientes na nuvem a avaliarem o risco geral de segurança de um serviço em nuvem.

2) Além do item acima, o CSP deve atender aos requisitos abaixo, de acordo com o tipo de infraestrutura utilizada IaaS, PaaS ou SaaS:

   - Toda plataforma contratada deve possuir serviços de proteção anti-DDoS;
   - Um termo de Non Disclosure Agreement deve ser assinado entre a TIM e o CSP sempre que houver processamento de dados confidenciais;
   - O CSP deve possuir ferramenta de Cloud Security Posture Management. (CSPM). Para monitoramento da postura de Cyber Security e compliance com regulamentações. Caso o CSP não possua solução nativa o mesmo deve prover a TIM uma lista de parceiros que tenham soluções integradas nativamente e homologada para monitorar a sua Cloud;
   - Deve haver segregação de funções nas atividades administrativas das consoles e ferramentas

providas pelo CSP, por exemplo: Administração de coleta de log, de IPS, de FW etc;

- Os processos de hardening e patching;

  (*) Exceto para SaaS.

- Toda atividade de autenticação de usuários de toda plataforma provida pelo CSP deve ser registrada em arquivos de log. Esses logs devem ser disponibilizados em tempo real para monitoramento da TIM através da ferramenta SIEM;
- Todos os acessos na console de gerenciamento providas pelo CSP devem ser realizados através de métodos de autenticação forte, envolvendo pelo menos dois fatores de autenticação;
- A máquina virtual/Storage dos ambientes com dados classificados como confidencialidade alta devem ser criptografados;
- Todas as máquinas virtuais devem ser catalogadas (rotulagem/marcação), usando ferramentas automatizadas, indicando função, funcionalidade e criticidade;
- Toda comunicação entre o CSP e a TIM deve ocorrer através de um canal encriptado ou exclusivo. Canais homologados pela TIM: VPN ou conexão privada;
- Todos os dados em repouso classificados como confidenciais devem ser criptografados. (máquina virtual/ armazenamento);
- Todos os backups (máquina virtual/armazenamento) devem ser criptografados no conteúdo e no canal de comunicação entre o cliente e o servidor de mídia;
- Nos processos de migração de dados de sistemas On-Premises para Cloud os dados classificados como confidenciais devem ser criptografados para transferência / cópia para o CSP. O CSP deve prover mecanismos tecnológicos para atendimento deste requisito;
- As chaves criptográficas de backup devem estar em posse e gerenciadas pela TIM;
- Contas privilegiadas de servidores Windows e Linux devem ser gerenciadas por cofre de senhas para garantir a rastreabilidade das ações;

  (*) Exceto para PaaS e SaaS.

- O CSP deve possuir ferramentas de gerenciamento de logs (*) capazes de centralizar os logs dos colaboradores, terceiros, a fim de garantir sua integridade e não repúdio e facilitar qualquer possível análise posterior. Esses logs devem ser disponibilizados para a TIM processá-los em suas ferramentas de gerenciamento de eventos de segurança para serem monitorados pela TIM em tempo real;

  Todos os logs de administração da Cloud devem ser disponibilizados tais como:

  - Identity and Access Management;
  - Compute;
  - Storage;
  - Networking;

- Business Applications;
- Security Functions (FW, IPS, WAF etc.).

(*) A administração deve ser de responsabilidade da função de segurança da TIM.

- Cada Ativo TIC, dispositivo ou componente de software deve sincronizar o relógio com o Network Time Protocol Server seguro;
- Toda plataforma provida pelo CSP deve ser desenvolvida seguindo as recomendações de desenvolvimento recomendada pelo OWASP. O processo de validação de código seguro deve ser garantido;
- Procedimentos de controle e rastreabilidade dos dados críticos devem ser implementados, esses logs devem, se solicitado pela TIM, ser disponibilizados em tempo real para a TIM e preservados por um período mínimo a ser definido pela TIM;
- O CSP deve garantir o envio por e-mail de notificações/alertas na presença de acesso anômalo ou suspeito feito por colaborador, fornecedor ou parceiro comercial TIM (por exemplo, acesso ao Ativo TIC e/ou console de gerenciamento feito de dispositivos ou locais não usados anteriormente). Além disso, o sistema deve permitir a configuração de alertas na presença de uso anormal de funções particularmente críticas para os negócios. Esses alarmes devem ser preferencialmente integrados e correlacionados no SIEM da TIM;
- Deve ser garantido o gerenciamento comum dos aspectos de segurança, bem como o gerenciamento de eventos de segurança decorrentes de emergências e/ou incidentes de segurança e privacidade. O CSP deve nomear um responsável pela segurança do serviço prestado e notificar a TIM;
- O CSP deve garantir que a senha para acessar seus Ativos TIC, Consoles de gerenciamento e Interface de aplicativo atenda pelo menos às seguintes características (ou critérios de robustez equivalentes):

  - Parametrização de senha: Comprimento mínimo: 8 caracteres;
  - A senha deve conter pelo menos um caractere alfabético maiúsculo;
  - A senha deve conter pelo menos um caractere alfabético minúsculo;
  - A senha deve conter pelo menos um caractere numérico;
  - A senha deve conter pelo menos um caractere especial.

  Expiração periódica: 90 (noventa) dias.
  Troca inicial obrigatória: Ao primeiro acesso a senha temporária é desabilitada e deve ser substituída.
  Controle de Sessão: A sessão do usuário deve encerrar (Logoff), após um período de 10 (dez) minutos de inatividade.
  Histórico da senha: A nova senha não pode ser igual às 10 senhas anteriores.

- O CSP deve fornecer mecanismos de autenticação forte para o acesso de colaborador, fornecedor ou parceiro comercial que processam dados classificados como críticos (confidencial e/ou exclusiva), para os negócios com um alto grau de Confidencialidade e/ou

Integridade;

- O CSP deve fornecer acesso utilizando autenticação mútua, com credenciais baseadas em criptografia assimétrica para todos os acessos M2M (Machine to Machine) que processam dados classificados como críticos (confidencial e/ou exclusiva), para os negócios com um alto grau de Confidencialidade e/ou Integridade;
- Serviços em nuvem diretamente acessíveis pela internet devem possuir um método de autenticação que impeça ações maliciosas de "quebra" de senha (por exemplo: implementar tempo de suspensão do acesso ao portal após um número limitado de tentativas de autenticação com falha ou a solicitação para verificar um código Captcha);
- Qualquer usuário, seja colaborador, fornecedor ou parceiro comercial quando gerenciado pelo CSP deve:
  - Verificar constantemente os usuários inativos para suspensão imediata (exceto usuários previamente autorizados para fins de gerenciamento técnico para os quais uma autorização foi concedida);
  - Conservar as requisições de cancelamento até o final do contrato com a TIM.
- O CSP deve garantir a adoção de procedimentos adequados (por exemplo, backup, replicação etc.) que garantam um ponto de recuperação (RPO) de até 01 (um) dia de informações/dados da TIM, em caso de perda de dados em Ativos TIC. As informações/dados devem ser mantidas apenas durante o período contratual, quando não, devem ser excluídos;

  Obs.: O RPO é definido de acordo com a solução.
- O CSP deve garantir que, em caso de mau funcionamento ou incidente em seus sistemas de TI, sejam adotados procedimentos operacionais específicos para a execução das atividades de restauração, que devem fornecer tempos de implementação alinhados com os SLAs contratados;
- As chaves criptográficas nunca devem ser armazenadas/transmitidas de forma clara. A propriedade e a gerência das chaves criptográficas são de responsabilidade da TIM;
- O CSP deve garantir que as atualizações do sistema operacional, middleware e software de aplicativo necessárias para corrigir defeitos e prevenir vulnerabilidades sejam instaladas em tempo hábil, de acordo com os padrões internacionais (por exemplo, OWASP, CERT). O CSP deve garantir testes adequados a fim de que a atualização não cause impacto na solução;

  (*) Exceto para IaaS.
- Os logs gerados e coletados pela TIM devem possuir mecanismos que garantam autenticidade, imutabilidade e a correta configuração de data e hora (sincronizado com uma fonte de tempo oficial do Brasil);
- O CSP deve garantir que qualquer software instalado seja licenciado legalmente;
- O acesso aos registros de atividades de colaborador, terceiro, inclusive usuário M2M que trocam dados da TIM deve ser garantido, com a possibilidade de serem enviados às

infraestruturas da TIM. Acesso aos registros dos usuários do CSP também deve ser garantido, nos casos em que são realizadas atividades de gerenciamento dos Ativos TIC da TIM;

- Todos os acessos e operações de leitura, gravação, modificação e exclusão de dados críticos devem ser rastreados nos sistemas de informações do CSP (por exemplo, dados classificados como críticos para os negócios com um alto grau de Confidencialidade e/ou Integridade, configurações de administração, informações privilegiadas) realizado colaborador, fornecedor ou parceiro comercial da TIM, inclusive usuários M2M e funcionários do CSP, nos casos em que são realizadas atividades de gerenciamento Ativo TIM. Os logs devem permitir identificar:
  - O sistema de destino e qualquer aplicativo acessado;
  - A referência do usuário que executou as atividades;
  - Qualquer detalhe dos recursos ou parâmetros de acesso (por exemplo, endereço IP do cliente);
  - As referências de tempo para a execução das atividades individuais;
  - Uma indicação dos tipos e características das atividades realizadas.
- Além do requisito **CSA IAM-08**, o CSP deve adotar uma solução técnica ou processual que permita o rastreamento inequívoca do colaborador, fornecedor ou parceiro comercial que utiliza logins sistêmicos/usuários técnicos (por exemplo, usuários root).

  O uso desses utilitários deve ser limitado em casos de necessidade operacional real e somente pelo tempo estritamente necessário, sempre com autorização da TIM;
- O CSP deve cumprir a cláusula contratual do Direito de Auditoria que permite à TIM realizar atividades de controle processual e técnico (por exemplo, Avaliação de Segurança), para verificar a presença e a eficácia das contramedidas de segurança que foram declaradas;
- Em caso de incidentes de segurança e privacidade ou potencial tentativa de ataque cibernético, o CSP deve realizar análise forense e reportar a TIM em um tempo máximo de até 01 (uma) semana sobre as vulnerabilidades exploradas e os dados comprometidos;
- A política, o controle da infraestrutura para os componentes de infraestrutura e os pré-requisitos de arquitetura adotados no datacenter on-premises devem ser garantidos como valores mínimos na nuvem;
- Todo ambiente exposto na Internet deve ser protegido por ferramentas de NGX Firewall, IPS e para aplicações Web deve ser protegido por WAF;
- As plataformas de segurança de NGX Firewall, microssegmentação, IPS e WAF deve ser administrado pela TIM.
  Quando aplicável tecnicamente a TIM se reserva o direito de utilizar a sua ferramenta de microssegmentação para garantir o controle de tráfego dos seus ativos e a proteção de ataques.
  A TIM se reserva o direito de utilizar os appliances de segurança de sua escolha caso o CSP não possua as soluções ou as soluções providas pelo CSP não atendam aos requisitos mínimos de segurança e governança requeridos;

(*) Exceto para as aplicações em SaaS.

- Todos os pontos de Interconexão de tráfego mesmo que interno devem ser protegidos por Firewall e IPS para filtragem de pacotes e tráfegos anômalos entre essas redes;
- Deve-se monitorar em tempo real os eventos e a correlação de informações por meio do SIEM (*), eventos relacionados a:
  - Anomalias de tráfego;
  - Eventos de segurança gerados por elementos de proteção (FW, IPS, Antivírus, autenticações etc.);
  - Eventos de acesso de usuários e clientes;
  - Eventos e atividades administrativas nas consoles.

  (*) A administração deve ser de responsabilidade da função de segurança da TIM.
- As políticas de configuração de equipamentos de segurança devem ser implementadas e documentadas seguindo os devidos fluxos de aprovações e logs de alterações de configurações;

  (*) A administração deve ser responsável pela função de segurança da TIM.
- As políticas e controles de segurança para os componentes de sistema/Ativos TIC adotados no datacenter local devem ser garantidos como medida mínima também na nuvem;
- Os sistemas devem estar segregados dos ambientes de produção, FQA e Desenvolvimento;
- Os acessos ao sistema operacional são realizados através de Gateway de sessão. As comunicações entre os componentes de sistema devem ser criptografadas;

  (*) Quando aplicável, a TIM se reserva o direito de utilizar o seu próprio Gateway de sessão.
- É necessário realizar o monitoramento em tempo real dos eventos para detectar ataques cibernéticos e um processo de resposta a incidentes, no caso de um incidente de segurança e privacidade;
- Em ambientes em nuvem, os ambientes devem obedecer às regras de segregação de ambiente definidas para o datacenter (micro segmentação), usando os recursos fornecidos pelo Cloud Service Provider (CSP). Adicionalmente a TIM se reserva o direito de utilizar a sua ferramenta de microssegmentação para garantir o controle de tráfego dos seus ativos e a visibilidade de ataques.
  A segregação dos aplicativos deve ser garantida usando o pool de recursos (VM, armazenamento de dados etc.) separados uns dos outros, respeitando o conceito de segregação horizontal e vertical de aplicativos;
- O movimento de dados horizontal (Leste-Oeste) deve ser regulado através do uso de infraestruturas que garantam a microssegmentação.
  Quando aplicável tecnicamente a TIM se reserva o direito de utilizar a sua ferramenta de microssegmentação para garantir o controle de tráfego dos seus ativos e a visibilidade de ataques;

- Todos os acessos na console de gerenciamento providas pelo CSP devem ser realizados através de métodos de autenticação forte, envolvendo pelo menos dois fatores de autenticação;
- O armazenamento/bancos de dados de ambientes com dados classificados com confidencialidade alta devem ser criptografados;
- As verificações de vulnerabilidade de Ativos TIC devem ser realizadas regularmente através de análise e/ou exploração de vulnerabilidade;
- Toda aplicação WEB e APIs devem ser disponibilizadas através de canais de comunicação criptografados através do uso de protocolos seguros e protegidas por solução de Web Application Firewall (WAF), por exemplo: SSL/TLS;
- Os servidores web que hospedam aplicações com acesso direto da Internet deve ser segregada dos servidores web que disponibilizam somente serviços as redes privadas da TIM.
  Os serviços web acessados via internet não devem ser acessados de forma direta, mas através de solução de Web Application Firewall e balanceadores de carga;
- Todo processo de autenticação deve ser criptografado;
- No caso de serviços em nuvem diretamente acessíveis na Internet (por exemplo, com navegador da Web sem VPN), o rastreamento de acesso e atividade deve incluir:
  - IP público do navegador e porta de origem;
  - indicações de tempo para o início e o fim da sessão de acesso;
  - Identificação da conta que efetuou login;
  - Identificação das atividades realizadas, em termos de URL das páginas navegadas, dos atributos sendo carregados, das funções relativas ativadas, das indicações de tempo correspondentes.

  Esses rastreamentos devem ser mantidos pelo CSP por um período mínimo de 6 meses com o objetivo de detectar incidentes ou comportamento anômalo, fraude ou abuso do serviço;
- Todas as consoles de administração ou gerencia do CSP devem ser criptografados;
- Deve ser prevista alta disponibilidade do ambiente, de forma a garantir menor impacto aos serviços/Ativos TIC TIM;
- Deve ser prevista a definição do DRP (Disater Recovery Plan), em caso de ocorrer um incidente nível desastre que impacte o ambiente da nuvem previsto na contratação. Os Ativos TIC previstos para DRP devem ser definidos pela TIM;
- A comunicação entre redes virtuais de diferentes ambientes/contextos deve ser autorizada, segundo o processo vigente na TIM. Exemplo: VPN;
- Todos os acessos realizados nas consoles providas pelo CSP devem ter sua rastreabilidade garantida por meio de logs, obedecendo os requisitos mínimos de rastreabilidade. Tais logs devem ser disponibilizados a TIM para a TIM processá-los em suas ferramentas de gerenciamento de eventos de segurança para serem monitorados pela TIM em tempo real;

- É desejável que o CSP possua certificações de mercado, como por exemplo: Atestado CSA-STAR, Certificação CSA-STAR, Autoavaliação da CSA-STAR, ISO 20000-1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, SOC, WCAG, PCI DSS, SOX (ISAE 3402 - Tipo 01 e 02), NIST 800-171, NIST CSF, União Europeia-US Privacy Shield, Regulamentação da SEC SCI, GDPR, LGPD, HIPAA/ALTA TECNOLOGIA). Essas certificações devem ser apresentadas à TIM;

Termo de Compromisso de Integridade
("**Termo**")

A TIM e a **Compromissada**, em processo de qualificação como fornecedora da TIM, através de seu(s) representante(s) legal(is), declaram e se comprometem com o que segue:

1. **Declaram** possuir Programa de Integridade e Código de Conduta em observância das boas práticas nacionais e internacionais, que visam garantir:

(a) o cumprimento das leis, códigos, regulamentos, regras, políticas e procedimentos anticorrupção de qualquer governo ou autoridade competente, considerando a jurisdição onde as atividades de seu objeto social serão conduzidas ou realizadas em favor de empresa do Grupo TIM, em especial, a legislação brasileira que, de qualquer modo, trate ou sancione atos contra a administração pública e seus regulamentos, incluindo, mas não se limitando, à Lei Brasileira de Combate à Corrupção (Lei Federal nº 12.846/2013), o Decreto Brasileiro de Anticorrupção (Decreto nº 11.129/2022), à Lei de Conflitos de Interesse (Lei Federal nº 12.813/2013), à Lei Federal de Improbidade Administrativa (Lei Federal nº 8.429/1992) e à Lei Federal de Licitações e Contratos Públicos (Lei Federal nº 8.666/1993), bem como às leis antitruste e anti-lavagem de dinheiro aplicáveis, e as legislações internacionais que eventualmente podem ser aplicáveis, incluindo, mas não se limitando, ao United States Foreign Corrupt Practices Act of 1977 ("FCPA") ou ao UK Bribery Act 2010;

(b) a disseminação da cultura de integridade e o treinamento de seus administradores e colaboradores; e

(c) a identificação de desvios de conduta de seus administradores, empregados e demais colaboradores, direta ou indiretamente vinculados.

2. Se **comprometem** a não permitir em suas operações, bem como nos contratos com seus terceirizados, a utilização de mão de obra escrava ou infantil, e **comprometem-se** ainda a respeitar todas as normas de direito trabalhistas (incluindo diretrizes atreladas à saúde, segurança do trabalho), direitos humanos e ambientais na medida do aplicável à sua atividade.

3. **Têm conhecimento** de que a TIM repudia e condena todo e qualquer ato de assédio ou discriminatório em suas relações de trabalho, inclusive na definição de remuneração, acesso a treinamento, promoções, demissões ou aposentadorias, seja em função de raça, origem étnica, nacionalidade, religião, sexo, identidade de gênero, orientação sexual, idade, deficiência física ou mental, filiação sindical ou que atente contra a valorização da diversidade.

4. **Declaram** ter tomado conhecimento na íntegra do Código de Ética e Conduta, bem como das Políticas TIM, em especial Política Anticorrupção e de Conflito de Interesses, que se encontram disponíveis no site da internet: http://www.tim.com.br/ri, menu "ESG", submenu "Regulamentos e Políticas".

JURÍDICO Joyce Franco TIM

4.1 Se **comprometem** em atuar respeitando os princípios e condutas definidos pelo Código de Ética e Conduta e demais políticas mencionados no item anterior, e, garante que seus colaboradores e administradores respeitem este compromisso.

5. **Declaram** que não praticaram ou praticarão qualquer ato lesivo a administração pública em especial, atos de corrupção ativa ou passiva, bem como **declaram**, em especial, a ciência da responsabilidade administrativa e cível da pessoa jurídica prevista no artigo 2º, da Lei nº 12.846/2013, e garantem a idoneidade de sua operação independentemente dos seus administradores, funcionários e prepostos estarem diretamente vinculados à contrato com alguma empresa do Grupo TIM.

6. Se **comprometem** a utilizar o Canal de Denúncias da TIM, disponível em http://www.tim.com.br/canal-denuncia/?origin=RI, para submeter ali todo e qualquer tentativa tomar conhecimento que enquadre-se em inobservância ao Código de Ética e Conduta, às Políticas Anticorrupção e de Conflito de Interesses da TIM e/ou às legislações vigentes, em especial a de anticorrupção. Se compromete, ainda, a divulgar a existência desse canal a seus administradores, funcionários e prepostos que estejam executando projeto em favor de qualquer empresa do Grupo TIM.

9. Se **comprometem** a, sempre que solicitada, prestar (i) declaração de conformidade com as obrigações assumidas na presente cláusula e/ou (ii) esclarecimento acerca de eventual questionamento referente à fato ou evento relacionado às obrigações contidas na presente cláusula, compartilhando eventuais documentos solicitados.

10. **Declaram** que sua operação está adequada a Lei Geral de Proteção de Dados (Lei nº. 13.709/2018), que todo tratamento de dados realizado nos projetos que executa possui uma base legal que o respalda e respeita os princípios da finalidade e necessidade.

A **Compromissada** assume este compromisso para todas as relações que vierem ser estabelecidas com empresas do Grupo TIM no Brasil, e concorda que referido **Termo** será considerado parte integrante de todo e qualquer contrato assinado entre a **Compromissada** e alguma empresa do Grupo TIM**.**

O(s) signatário(s) do presente **Termo**, declara(m), para os devidos fins e sob as penas da lei, que possui(em) poderes constituídos nos moldes dos atos constitutivos da **Compromissada** para atuar como representante(s) legal(is).

Rio de Janeiro 11 de junho de 2026

TERESA REGINA COTOSKY:1345

Assinado de forma digital por TERESA REGINA COTOSKY:1345
Dados: 2026.06.18 18:49:36 -03'00'

Representante Legal 1

Representante Legal 2

JURÍDICO Joyce Franco TIM

Certificado de Conclusão

Identificação de envelope: 08B32C5C-50A9-8738-82CD-AD625D414BB0
Status: Concluído
Assunto: Termo de Cooperação - TRT 12 - INFOTIM
Envelope fonte:
Documentar páginas: 46
Assinaturas: 2
Certificar páginas: 4
Rubrica: 0
Assinatura guiada: Ativado
Selo com EnvelopeId (ID do envelope): Ativado
Fuso horário: (UTC-03:00) Brasília

Remetente do envelope:
Danielle Alonso Langella
Av. João de Cabral de Mello Neto, 850
Rio de Janeiro, Rio de Janeiro 22775-055
dlangella@timbrasil.com.br
Endereço IP: 163.116.228.135

Rastreamento de registros

Status: Original
25/06/2026 13:45:30
Portador: Danielle Alonso Langella
dlangella@timbrasil.com.br
Local: DocuSign

Eventos do signatário	Assinatura	Registro de hora e data
Heros Fabiano dos Santos hfsantos@timbrasil.com.br Diretor de Segurança TIM S.A. Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	DocuSigned by: Heros Fabiano dos Santos D843819E21A0449... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 163.116.228.108	Enviado: 25/06/2026 13:54:58 Visualizado: 25/06/2026 14:14:03 Assinado: 25/06/2026 14:14:39

Termos de Assinatura e Registro Eletrônico:
Aceito: 31/01/2019 11:18:55
ID: 04084b79-63ca-48d3-8c2f-b5514273e714

Eventos do signatário presencial	Assinatura	Registro de hora e data

Eventos de entrega do editor	Status	Registro de hora e data

Evento de entrega do agente	Status	Registro de hora e data

Eventos de entrega intermediários	Status	Registro de hora e data

Eventos de entrega certificados	Status	Registro de hora e data

Eventos de cópia	Status	Registro de hora e data

Eventos com testemunhas	Assinatura	Registro de hora e data

Eventos do tabelião	Assinatura	Registro de hora e data

Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	25/06/2026 13:54:58
Entrega certificada	Segurança verificada	25/06/2026 14:14:03
Assinatura concluída	Segurança verificada	25/06/2026 14:14:39
Concluído	Segurança verificada	25/06/2026 14:14:39

Eventos de pagamento	Status	Carimbo de data/hora

Termos de Assinatura e Registro Eletrônico

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Tim Celular S.A. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Tim Celular S.A.:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: alandrade@timbrasil.com.br

To advise Tim Celular S.A. of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at alandrade@timbrasil.com.br and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from Tim Celular S.A.
To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to alandrade@timbrasil.com.br and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.
To withdraw your consent with Tim Celular S.A.

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an e-mail to alandrade@timbrasil.com.br and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows2000? or WindowsXP?
Browsers (for SENDERS):	Internet Explorer 6.0? or above
Browsers (for SIGNERS):	Internet Explorer 6.0?, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	• Allow per session cookies

	• Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I Agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Tim Celular S.A. as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Tim Celular S.A. during the course of my relationship with you.