CONTRATO N.º 12468/2025 PARA PRESTAÇÃO DE SERVIÇOS NO TRATAMENTO DAS MANIFESTAÇÕES NO PORTAL RECLAME AQUI, QUE ENTRE SI FIRMAM, DE UM LADO, A CAIXA ECONÔMICA FEDERAL, E, DE OUTRO, A EMPRESA OBVIO BRASIL SOFTWARE E SERVIÇOS S/A.

Pelo presente instrumento, a **CAIXA ECONÔMICA FEDERAL - CEF,** instituição financeira sob a forma de empresa pública, por intermédio de sua Centralizadora Nacional Contratações – CECOT em Brasília, CNPJ(MF) nº 00.360.305/5614-83, situada no Setor Bancário Sul, Quadra 1, Lote 2, Bloco L, 7º andar - Asa Sul – Brasília, - CEP 70070-110, neste ato representada pelo Coordenador de Centralizadora **Oséias Dias Duarte**, portador do documento de identificação nº 3.170.838/SPTC/GO, inscrito no CPF(MF) sob o nº 692.472.421-34, conforme poderes estabelecidos no substabelecimento de procuração lavrada em 16/03/2018, à folha 193/194 do livro 00111-S, sob o protocolo nº 0082381, escrevente 0093, no Cartório Francisco Taveira, 4º Registro Civil e Tabelionato de Notas – Goiânia/GO**,** daqui por diante designada **CAIXA**, de um lado e, de outro, a empresa **OBVIO BRASIL SOFTWARE E SERVIÇOS S/A**, inscrita no CNPJ(MF) sob o nº 13.114.403/0001-03, com sede na Praça General Gentil Falcão, 108, 16°andar, Cidade Monções, 04571-150 - São Paulo – SP, por seu representante legal, devidamente identificado, que ao final subscreve este, doravante designada **CONTRATADA**, em face da autorização do Comitê de Compras e Contratações das Centralizadoras Nacionais de Contratação e Gestão Formal de Contratos da CAIXA**,** Resolução 22686 de 03/11/2025, constante do Processo Administrativo nº **5688.01.1241.0/2025** com base no Artigo 30 da Lei n° 13.303/16, têm justo e contratada prestação do serviço objeto deste instrumento, vinculado à proposta apresentada pela CONTRATADA, sujeitando-se as partes contratantes às normas constantes da Lei nº 13.303, de 30/06/2016 e suas alterações posteriores, do Regulamento de Licitações e Contratos da CAIXA e aos preceitos de Direito Privado), bem como às cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DO OBJETO

O presente contrato tem por objeto a contratação de soluções do portal Reclame AQUI, incluindo o acesso à base de dados digital do referido portal, visando à atuação da CAIXA na gestão do atendimento, monitoramento e tratamento de reclamações relacionadas aos seus produtos e serviços.

Parágrafo Único - A especificação pormenorizada do objeto contratado, os requisitos técnicos e as condições de prestação dos serviços, bem como as obrigações e responsabilidades específicas estão indicadas no Termo de Referência – Anexo I e Proposta apresentada, que integram e complementam este contrato.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA

São obrigações da CONTRATADA, além das previstas neste contrato e anexos:

I. Dispor-se a toda e qualquer fiscalização da CAIXA, no tocante à prestação dos serviços, assim como ao cumprimento das obrigações previstas neste contrato;

II. Fiscalizar o perfeito cumprimento dos serviços a que se obrigou, cabendo-lhe integralmente os ônus decorrentes;

III. Estruturar-se de modo compatível e prover toda a infraestrutura necessária à prestação dos serviços previstos neste contrato, com a qualidade e rigor exigidos, garantindo a sua supervisão desde a implantação;

IV. Prover todos os meios necessários à garantia da prestação dos serviços contratados e a plena execução do objeto contratado, inclusive nos casos de greve ou paralisação de qualquer natureza;

V. Manifestar-se quanto a aceitação ou não, nas mesmas condições contratuais, de acréscimos ou supressões que se fizerem necessárias, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado deste contrato, podendo a supressão exceder o limite estabelecido quando houver acordo entre as partes;

VI. Manter, durante o prazo contratual, todas as condições de habilitação e qualificação exigidas no procedimento;

VII. Manter perante a CAIXA, durante a vigência do contrato, seu endereço comercial completo (logradouro, cidade, UF, CEP) e eletrônico, telefone, fax e nome dos seus representantes sempre atualizados, para fins de comunicação e encaminhamento de informações e documentos, inclusive os relativos a tributos, em face da condição da CAIXA de substituta tributária;

VIII. Não manter relação de emprego/trabalho, de forma direta ou indireta, com menor de 18 anos de idade em trabalho noturno, perigoso ou insalubre, nem menor de 16 anos de idade em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 anos;

IX. Assegurar a não utilização de trabalho em condições degradantes ou em condições análogas à escravidão, bem como a não utilização de práticas de assédio moral ou sexual e discriminatórias em razão de crença religiosa, raça, cor, sexo, deficiência, orientação sexual, partido político, classe social, nacionalidade;

X. Manter uma conduta pautada por elevados padrões de ética e integridade, capaz de assegurar relações sustentáveis, compatíveis com a legislação e o interesse público, observando com rigor as premissas norteadoras de comportamento estabelecidas no Código de Conduta do Fornecedor CAIXA, entregue à Contratada no ato da assinatura deste instrumento contratual.

XI. Tomar conhecimento dos termos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais - LGPD e de suas regulamentações, zelando pela sua estrita observância, assim como garantindo que seus prestadores conheçam e observem o disposto na LGPD no exercício de suas atividades.

XII. Providenciar assinatura de Termo de Responsabilidade de Segurança da Informação, anexo a este contrato, de todos os seus prestadores que tiverem acesso a sistemas e informações internas da CAIXA e entregar ao Gestor Operacional (CETRS/BH), por meio definido pela CAIXA, no prazo de 5 (cinco) dias uteis após a assinatura do contrato, devendo comunicar a CAIXA e realizar o mesmo procedimento quando houver novos prestadores na execução do serviço.

XIII. Aceitar alterações das condições dos serviços inicialmente pactuados no caso de eventuais mudanças estruturais da CAIXA, inclusive transferência da posição contratual para terceiros, quando essas não trouxerem impactos no equilíbrio financeiro do contrato, ou negociar com a CAIXA ou eventual instituição de transição ou para um adquirente definitivo, garantindo a continuidade da prestação do serviço até o final do contrato.

XIV. Tomar conhecimento dos termos da Lei nº 12.846/2013 e de suas regulamentações, reconhecendo sua responsabilidade objetiva pelos atos praticados em seu interesse ou benefício, por qualquer pessoa que o represente, bem como adotar as medidas pertinentes no seu âmbito de atuação e influência, para combater a prática de atos lesivos à Administração Pública.

XV. Atuar de acordo com Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo da CAIXA (PLDFT), disponível em: https://www.caixa.gov.br/Downloads/caixa-governanca/Politica-Prevencao-Lavagem-Dinheiro-e-Financiamento-Terrorismo.pdf e dar ciência a seus empregados do folder (flyer) sobre a PLDFT disponível no Portal de Licitações da CAIXA http://licitacoes.caixa.gov.br.

XVI. Atender às obrigações da Responsabilidade Social, Ambiental e Climática, dispostas na Cláusula Quinta.

XVII. Tomar conhecimento da Política de Prevenção e Combate ao Assédio Moral e Sexual e à Discriminação, disponível no site da CAIXA, no endereço: https://www.caixa.gov.br/Downloads/caixa-governanca/Politica-de-Combate-ao-Assedio-Moral-Sexual-Discriminacao.pdf (ou pelo site www.caixa.gov.br, aba “Downloads”, no link “A CAIXA – Governança Corporativa”), zelando pela sua estrita observância, assim como garantindo que seus prestadores a conheçam e a observem no exercício de suas atividades.

XVIII A CONTRATADA responderá pecuniariamente por danos e/ou prejuízos que forem causados à CAIXA, ou a terceiros, decorrentes de falha dos serviços ora contratados, inclusive os motivados por greves ou atos dolosos de seus empregados.

XIX Assume a CONTRATADA, nesse caso, a obrigação de efetuar a respectiva indenização até o 5º (quinto) dia útil após a comunicação, que lhe deverá ser feita por escrito.

XX Conceder a Licença e executar os Serviços ofertados com elevados padrões de qualidade técnica.

XXI Executar, dentro dos melhores padrões técnicos e sistêmicos, os serviços ofertados, observando toda a legislação e normas aplicáveis ao objeto.

XXII Executar todos os serviços sob a sua total responsabilidade e administração, com profissionais competentes e capazes, para garantir um processo eficiente e resultados eficazes e com a melhor qualidade possível relativamente aos serviços ora ofertados.

XXIII Assumir todos e quaisquer riscos inerentes à sua atividade, inclusive todos os encargos trabalhistas, previdenciários, tributários e fiscais de sua responsabilidade, e a mão-de-obra empregada para a realização dos serviços ora ofertados.

XXIV Guardar estrita observância aos preceitos éticos e profissionais ligados às atividades por ela desenvolvidas.

XXV Cumprir o NDS (Nível de Disponibilidade do Serviço) especificado no Termo de Referência, quando aplicável.

XXVI Responsabilizar-se por todo e quaisquer prejuízos e danos causados e comprovados à Empresa em virtude, especificamente dos serviços prestados.

XXVII Observar as disposições legais e regulamentares que disciplinam a concessão da Licença e eventual prestação dos Serviços.

CLÁUSULA TERCEIRA – DAS RESPONSABILIDADES DA CONTRATADA

São responsabilidades da CONTRATADA, além das demais previstas neste contrato e anexos:

I Responder por todo e qualquer dano que causar à CAIXA ou a terceiros, ainda que culposo, praticado por seus prepostos, empregados ou mandatários, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pela CAIXA, assegurado o contraditório e a ampla defesa;

II Responder por qualquer tipo de autuação ou ação que venha a sofrer em decorrência da prestação dos serviços, bem como pelos contratos de trabalho de seus empregados, mesmo nos casos que envolvam eventuais decisões judiciais, assegurando à CAIXA o exercício do direito de regresso, eximindo a CAIXA de qualquer solidariedade ou responsabilidade;

III Arcar com quaisquer multas, indenizações ou despesas impostas à CAIXA, por autoridade competente, em decorrência do descumprimento de lei ou de regulamento a ser observado na execução do contrato pela CONTRATADA, as quais serão reembolsadas à CAIXA.

IV Responder, por força da lei, civil e penal, pela indevida divulgação e descuidada ou incorreta utilização dos dados, informações ou documentos de qualquer natureza, exibidos, manuseados, os quais deve guardar sigilo, sem prejuízo da responsabilidade por perdas e danos a que der causa.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CAIXA

A CAIXA obriga-se a:

I Indicar os locais e horários em que deverão ser prestados os serviços, permitindo, quando for o caso, o acesso dos empregados da CONTRATADA nas dependências da CAIXA;

II Notificar formalmente a CONTRATADA de qualquer irregularidade encontrada no fornecimento contratado, oportunizando justificativa;

III Efetuar os pagamentos devidos nas condições estabelecidas neste contrato.

IV Indicar o representante da CAIXA responsável pela fiscalização e acompanhamento da execução do contrato.

V Exercer a fiscalização e acompanhamento do contrato por meio do representante especialmente designado.

CLÁUSULA QUINTA: DA RESPONSABILIDADE SOCIAL, AMBIENTAL E CLIMÁTICA

A CONTRATADA deve incorporar a responsabilidade social, ambiental e climática na estratégia, gestão, negócios, produtos, serviços, processos, operações, atividades e no relacionamento com as partes interessadas, no intuito de promover a sustentabilidade e o desenvolvimento sustentável e obriga-se à:

I Realizar o engajamento e o incentivo a boas práticas socioambientais de seus funcionários, clientes, fornecedores e demais stakeholders.

II Cumprir as leis, decretos, regulamentos, portarias e normas Federais, Estaduais e Municipais, instruções e resoluções, direta e indiretamente, aplicáveis ao objeto do contrato, inclusive por suas subcontratadas, no que tange as atividades voltadas à responsabilidade social, ambiental e climática e ao gerenciamento do risco social, ambiental e climático.

III Observar os impactos decorrentes das suas atividades, processos, produtos e/ou serviços, com relação à(ao):

a) Combate ao trabalho análogo a escravo, ao trabalho infantil, à exploração sexual e à violação dos direitos e garantias fundamentais e atos lesivos ao interesse comum;

IV Participar das iniciativas de engajamento em mudanças climáticas e/ou segurança hídrica, quando convidado pela CAIXA.

a) A CAIXA realizará convite formal para que a CONTRATADA se comprometa a participar, como forma de incrementar os seus conhecimentos sobre responsabilidade social, ambiental e climática, e possa incorporar progressivamente tais políticas à estratégia e gestão de seus negócios, produtos, serviços e processos.

V Responder a pesquisa implementada pelo CDP – CARBON DISCLOSURE PROJECT, que trata sobre mudanças climáticas e segurança hídrica ou outra que vier a substitui-la futuramente, sempre que convocado pela CAIXA.

a) A CAIXA viabilizará, junto ao CDP, agenda(s) anuais com a CONTRATADA para esclarecimentos sobre o preenchimento do questionário.

VI Atuar na prevenção de impactos ambientais e climáticos gerados por seus processos, produtos e serviços e na mitigação, correção ou compensação, quando identificados.

VII Proteger e preservar o meio ambiente, prevenindo práticas danosas e executando seus serviços em observância à legislação vigente pertinente à responsabilidade social, ambiental e climática, principalmente no que se refere aos crimes ambientais.

VIII Autorizar a CAIXA a realizar visitas de vistoria às instalações da CONTRATADA, quando solicitado pela CAIXA ou em decorrência de suspeita e/ou denúncia relativas ao descumprimento de obrigações de responsabilidade social, ambiental e climática, assumidas pela CONTRATADA para a execução do objeto contratual.

CLÁUSULA SEXTA – DOS PREÇOS E SUA REVISÃO

Pela perfeita prestação dos serviços, objeto deste contrato, e obedecidas as demais condições estipuladas neste instrumento, a CAIXA pagará à CONTRATADA os preços unitários abaixo indicados, perfazendo o valor global de R$ **1.401.860,00 (um milhão, quatrocentos e um mil, oitocentos e sessenta reais) pelo prazo de 12 (doze) meses, conforme detalhamento a seguir:**

Prazo	Itens	Custo Total
-	Implantação API*	R$ 15.164,00
12 meses	Planos e Licenças	R$ 1.386.696,00
Valor Global da Contratação		**R$ 1.401.860,00**

**Parcela única*

Item	Produto	Quant.	Parcela	Valor Mês	Valor Global
I	HugMe (RA) Iniciante - Plano 60.000 + 1 PA Gerente	1	Mensal	R$ 21.285,70	R$ 255.428,40
II	HugMe (RA) - PA Gerente (Planos 1000+) - Avulsa	12	Mensal	R$ 19.676,40	R$ 236.116,80
III	HugMe (RA) - PA Atendente (Planos 1000+) - Avulsa	60	Mensal	R$ 35.055,00	R$ 420.660,00
IV	Brand Page (Premium) - Plano 2.500.000	1	Mensal	R$ 23.120,15	R$ 277.441,80
V	RA API (Conector HugMe) - para até 60.000 reclamações (12 meses)	1	Mensal	R$ 8.266,00	R$ 99.192,00
VI	SETUP - Serviço de liberação de dados para contas com até 35.000+ reclamações (12 meses)	1	Única	R$ 15.164,00	R$ 15.164,00
VII	HugMe - Pedido de avaliação pelo WhatsApp (até 8.000 disparos)	1	Mensal	R$ 7.345,75	R$ 88.149,00
VIII	RA Data Hub Plano 5 - Consulta de 5 empresas por dia	1	Mensal	R$ 809,00	R$ 9.708,00
Valor Global Total (12 meses)					**R$ 1.401.860,00**

Parágrafo Primeiro – É admitida a revisão de preços deste contrato, para mais ou para menos, limitada à variação obtida pelo IGP-M (Índice Geral de Preços – Mercado), observados os preços vigentes no mercado para a prestação do serviço, desde que respeitado o intervalo mínimo de 1 (um) ano, a ser aplicado sobre os preços unitários conforme quadro abaixo:

Item	Produto	Quant	Parcela	Valor
I	HugMe (RA) Iniciante – Plano 60.000 + 1 PA Gerente	1	Mensal	R$ 21.285,70
II	HugMe (RA) – PA Gerente (Planos 1000+) – Avulsa	12	Mensal	R$ 1.639,70
III	HugMe (RA) – PA Atendente (Planos 1000+) – Avulsa	60	Mensal	R$ 584,25
IV	Brand Page (Premium) – Plano 2.500.000	1	Mensal	R$ 23.120,15
V	RA API (Conector HugMe) – para até 60.000 reclamações (12 meses)	1	Mensal	R$ 8.266,00
VI	HugMe – Pedido de avaliação pelo WhatsApp (até 8.000 disparos)	1	Mensal	R$ 7.345,75
VII	RA Data Hub Plano 5 – Consulta de 5 empresas por dia	1	Mensal	R$ 809,00

Parágrafo Segundo – Na primeira revisão, o prazo de 12 (doze) meses será a contar da data de apresentação da proposta. As revisões subsequentes observarão o mesmo intervalo mínimo de 12 (doze) meses, contados a partir do último reajuste aplicado.

I Caso a CONTRATADA não efetue o pedido de revisão dos preços do contrato até a data da assinatura do aditamento de prorrogação contratual, ocorrerá a preclusão do direito à revisão de preços referente ao período imediatamente anterior à data da assinatura do aditamento de prorrogação.

II Ocorrerá a preclusão do direito à revisão se o pedido for apresentado depois de extinto o contrato.

III Em nenhuma hipótese será permitida a majoração superior ao índice do *caput*, sendo, portanto, o limitador da revisão;

IV O índice a ser aplicado será a variação apurada dos últimos 12 (doze) meses anteriores à data do direito.

Parágrafo Terceiro – A variação do valor contratual para fazer face à revisão de preços prevista no próprio contrato dispensa a celebração de termo aditivo, podendo ser formalizado por apostilamento.

Parágrafo Quarto - A contratada pode interpor recurso administrativo, sem efeito suspensivo, sobre os cálculos efetuados pela CAIXA para a concessão da revisão de preços, no prazo de 10 (dez) dias úteis a contar da notificação do ato.

CLÁUSULA SÉTIMA – DA FORMA DE PAGAMENTO

A **CAIXA**, após a aceitação dos serviços e verificação do cumprimento de todas as cláusulas contratuais, efetuará o pagamento à **CONTRATADA**, mensalmente, até o 15º (décimo quinto) dia útil do mês subsequente ao da efetiva prestação dos serviços, mediante crédito em conta corrente de titularidade da **CONTRATADA**, mantida em agência da **CAIXA** – **AG 4284 – Produto 1292 – conta 579.799.586-3**, ou, excepcionalmente, por meio de boleto/fatura.

Parágrafo Primeiro - O correspondente documento fiscal deve ser apresentado pela **CONTRATADA** à **CAIXA** no mês subsequente ao da prestação dos serviços, na data definida e informada pela **CAIXA**, prorrogando-se o prazo de pagamento na mesma proporção de eventual atraso ocorrido na entrega do documento fiscal, cabendo à contratada emitir o correspondente documento fiscal em conformidade com a legislação aplicável e regulamentações dos órgãos competentes.

Parágrafo Segundo – O documento fiscal deve conter todos os elementos exigidos na legislação aplicável, cabendo à CONTRATADA a sua correta emissão, em conformidade com a legislação tributária pertinente, devendo, ainda, constar no seu corpo e apresentar juntamente:

I A identificação completa da CAIXA, para o CNPJ informado pelo gestor operacional do contrato no momento de solicitação do faturamento, na qualidade de contratante, bem como o número do processo administrativo que originou a contratação e número do contrato;

II Descrição de todos os serviços/itens que compõem a respectiva nota fiscal/fatura de forma clara, indicando, inclusive, os valores unitários e totais, o período a que se refere, bem como, a unidade da CAIXA contemplada.

Parágrafo Terceiro – O documento fiscal não aprovado pela CAIXA será devolvido à CONTRATADA para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo de pagamento da data de sua reapresentação. A devolução do documento fiscal não aprovado pela CAIXA, em hipótese alguma, autorizará a CONTRATADA a suspender a execução dos serviços ou a deixar de efetuar os pagamentos devidos aos seus empregados.

Parágrafo Quarto – A CAIXA fará as retenções dos tributos e contribuições sociais/previdenciárias, quando exigidas legalmente, em conformidade com a legislação vigente. As retenções não serão efetuadas caso a CONTRATADA, comprovadamente, se enquadre em hipótese excludente prevista em legislação, devendo, para tanto, apresentar a documentação pertinente ou declaração que comprove essa condição. Também não ocorrerá a retenção caso a CONTRATADA esteja amparada por medida judicial, que determine a suspensão do pagamento dos referidos tributos e/ou das contribuições previdenciárias, devendo apresentar à CAIXA, a cada pagamento, a documentação que comprove essa situação.

Parágrafo Quinto – Quando houver a prestação de serviço em município, cuja Lei Municipal atribua à CAIXA a responsabilidade pela retenção do ISSQN na fonte e, por conseguinte, o respectivo repasse, a CONTRATADA é obrigada a faturar os serviços, separadamente, por Município, emitindo quantos documentos fiscais forem necessários, independentemente de a CONTRATADA estar ou não nele estabelecida e da sua situação cadastral na localidade onde os serviços estão sendo prestados.

Parágrafo Sexto – Os encargos sofridos pela CAIXA por atraso no repasse de obrigações tributárias de qualquer natureza, bem como das contribuições à Previdência, quando for o caso, decorrentes do atraso na entrega do documento fiscal pela CONTRATADA, serão cobrados diretamente da CONTRATADA.

Parágrafo Sétimo – A CONTRATADA, além de manter as condições de habilitação durante toda a vigência do contrato, deverá se manter regular no Sistema de Cadastramento Unificado de Fornecedores - SICAF, para verificação da sua regularidade fiscal, no âmbito Federal, e trabalhista, bem como da regularidade com a Seguridade Social (INSS) e Fundo de Garantia por Tempo de Serviço (FGTS), exigidas no procedimento de contratação.

Parágrafo Oitavo - A critério e conveniência da CAIXA, será efetuada consulta ao Sistema de Cadastramento Unificado de Fornecedores - SICAF, para verificação da regularidade da CONTRATADA.

Parágrafo Nono - Constatada a situação de irregularidade, a CAIXA efetivará o pagamento devido pelos serviços prestados, contudo, a CONTRATADA será comunicada por escrito para que regularize sua situação no prazo de 05 (cinco) dias úteis, sendo-lhe facultada a apresentação de defesa, no mesmo prazo, sob pena das sanções cabíveis e, não havendo regularização, rescisão contratual.

Parágrafo Décimo – Nenhum pagamento isentará a CONTRATADA das suas responsabilidades e obrigações, nem implicará aceitação definitiva dos serviços.

Parágrafo Décimo Primeiro – O não pagamento do documento fiscal, por culpa exclusiva da CAIXA, no prazo estabelecido neste contrato, enseja a atualização do respectivo valor pelo IGP-M – Índice Geral de Preços de Mercado, da Fundação Getúlio Vargas, utilizando-se a seguinte fórmula:

VAT = VIN x (1+IGP-M1) x (1+IGPM-2) x ... (1+IGPM-n), onde:

VAT: Valor atualizado
VIN: Valor inicial
IGPM-n: Evolução mensal do índice IGP-M/FGV, desde o mês inicial até o mês final da apuração

CLÁUSULA OITAVA – DA EXECUÇÃO DOS SERVIÇOS E VIGÊNCIA DO CONTRATO

O presente contrato terá a duração de 12 (doze) meses, a contar de 30/12/2025, podendo ser prorrogado por sucessivos períodos nos limites definidos na Lei nº. 13.303/2016.

Parágrafo Primeiro - A prorrogação dar-se-á por apostilamento, quando houver manifestação formal e expressa da CONTRATADA e não houver alteração das demais disposições contratuais, dispensando-se a assinatura da CONTRATADA. Caso a prorrogação esteja acompanhada de alterações contratuais que impliquem modificação das obrigações pactuadas, tais ajustes serão formalizados por meio de termo aditivo.

CLÁUSULA NONA – DA FISCALIZAÇÃO

No curso da execução deste contrato caberá à CAIXA, diretamente ou por quem vier a indicar, o direito de fiscalizar a fiel observância das disposições deste instrumento.

Parágrafo Primeiro – A CAIXA, sempre que entender pertinente, realizará consulta ao Registro do CEIS/CNEP/CEPIM (Cadastro Nacional de Empresas Inidôneas e Suspensas e Cadastro Nacional das Empresas Punidas/ Cadastro de Entidades Privadas sem fins Lucrativos), para verificar se existe ocorrência de sanções que restrinjam o direito de a empresa participar de licitações ou de celebrar contratos com a Administração Pública ou a existência de penalidades aplicadas pela Administração Pública com base na Lei 12.846/2013;

Parágrafo Segundo – A CAIXA poderá promover as diligências que entender necessárias para verificar a aderência da CONTRATADA à legislação anticorrupção.

CLÁUSULA DÉCIMA – DO RESSARCIMENTO

A CONTRATADA autoriza a CAIXA a descontar o valor correspondente aos danos ou prejuízos apurados diretamente dos documentos fiscais pertinentes aos pagamentos que lhe forem devidos em relação a este contrato ou da garantia contratual, independentemente de qualquer procedimento judicial, depois de assegurada a prévia defesa em processo administrativo para apuração dos fatos.

Parágrafo Primeiro – A CONTRATADA concorda, em casos de prejuízos sofridos pela CAIXA em condenações trabalhistas originadas por seus funcionários, que tais valores sejam glosados das faturas em quaisquer contratos mantidos com a CAIXA, independente de processo administrativo.

Parágrafo Segundo – A CONTRATADA concorda com o desconto de valores apurados a crédito da CAIXA em razão de ato lesivo que tenha praticado, tais como o valor de dano apurado no âmbito da Lei Anticorrupção e multa que lhe tenha sido aplicada com base na Lei 12.846/2013, e que tais valores sejam glosados das faturas em quaisquer contratos mantidos com a CAIXA, independente de processo administrativo.

Parágrafo Terceiro – O valor a ser ressarcido à CAIXA, nos casos de danos ou prejuízos em que a CONTRATADA for responsabilizada, será atualizado pelo índice de variação do IGP-M – Índice Geral de Preços de Mercado, da Fundação Getúlio Vargas, obtido no período compreendido entre a data da ocorrência do fato que deu causa ao prejuízo e a data do efetivo ressarcimento à CAIXA, utilizando-se a seguinte fórmula:

VAT = VIN x (1+IGP-M1) x (1+IGPM-2) x ... (1+IGPM-n), onde:

VAT: Valor atualizado
VIN: Valor inicial
IGPM-n: Evolução mensal do índice IGP-M/FGV, desde o mês inicial até o mês final da apuração

Parágrafo Quarto – Caso o acumulado dos índices de correção monetária seja negativo (deflação) para o período referenciado, esse não deverá ser considerado no cálculo de atualização, prevalecendo o valor nominal.

CLÁUSULA DÉCIMA PRIMEIRA – DAS INCIDÊNCIAS FISCAIS, ENCARGOS, SEGUROS, ETC.

Correrão por conta exclusiva da CONTRATADA:

I Todos os tributos que forem devidos em decorrência do objeto deste contrato, bem como as obrigações acessórias deles decorrentes;

II As contribuições devidas à Previdência Social, encargos trabalhistas, prêmios de seguro e de acidentes de trabalho, emolumentos e outras despesas que se façam necessárias à execução dos serviços.

CLÁUSULA DÉCIMA SEGUNDA – DAS SANÇÕES ADMINISTRATIVAS

Pela inexecução total ou parcial do objeto deste contrato e/ou pelo atraso injustificado na sua execução, garantida a prévia defesa, a CONTRATADA ficará sujeita às seguintes sanções, sem prejuízo das demais cominações aplicáveis:
I. Multa;
II. Suspensão temporária de participação em licitação e contratação com a CAIXA, pelo prazo de até 2 (dois) anos.

Parágrafo Primeiro – A multa será aplicada nas situações, condições e percentuais indicados a seguir:
I. Pelo descumprimento da legislação pertinente à responsabilidade social, ambiental e climática e gerenciamento do risco social, ambiental e climático:
Parâmetro de Aplicabilidade: Constatação formal pela CAIXA de violação de leis, decretos, regulamentos ou normas aplicáveis à Responsabilidade Social, Ambiental e Climática (RSAC), ou a não implementação de práticas essenciais de gerenciamento de risco social, ambiental ou climático que sejam mandatórias para o tipo de empresa e serviço. Inclui, mas não se limita a, não cumprimento das obrigações de combate ao trabalho análogo à escravidão, trabalho infantil, exploração sexual e violação de direitos e garantias fundamentais (conforme Cláusula Multa: 2% (dois por cento) sobre o valor global do contrato, por ocorrência.
II. Pelo descumprimento das obrigações de sigilo, segurança da informação e privacidade de dados:
Parâmetro de Aplicabilidade: Em caso de ocorrência de quebra de sigilo das informações de clientes da CAIXA, será imputada multa de 1% (um por cento) sobre o valor do documento fiscal do respectivo mês da ocorrência, sem prejuízo das demais sanções cabíveis.

III. Multa de 1% (um por cento) sobre o valor por dia do documento fiscal pela ocorrência de suspensão da prestação do serviço, permanecendo o problema, a multa será aplicada cumulativamente a cada período de três horas sucessivas, até o restabelecimento integral dos serviços, sem prejuízo das demais sanções cabíveis.
IV. Multa de 20% (vinte por cento) sobre o valor do documento fiscal do mês da ocorrência, por atos fraudulentos, violação de sistemas ou qualquer ato que implique em prejuízos à CAIXA ou a seus clientes, sem prejuízo das demais sanções cabíveis
V. O somatório das multas está limitado a 30% (trinta por cento) do documento fiscal dentro do mês calendário de apuração do faturamento.
VI. As multas retromencionadas são aplicáveis, simultaneamente, ao desconto sobre eventual inadimplemento previsto na cláusula das responsabilidades da contratada, sem prejuízo, ainda, de outras cominações previstas neste contrato.

Parágrafo Segundo – A CONTRATADA autoriza à CAIXA descontar o valor da multa diretamente das notas fiscais/faturas pertinentes aos pagamentos que lhe forem devidos em relação a este contrato e/ou de quaisquer outros contratos que porventura mantenha com a CAIXA, da garantia contratual e, se não for suficiente, será cobrado judicialmente, depois de assegurada a prévia defesa em processo administrativo para apuração dos fatos.

Parágrafo Terceiro – A penalidade de suspensão temporária de participação em licitação e contratação com a CAIXA poderá também ser aplicada à empresa ou ao profissional que:
I. Tenha sofrido condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
II. Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

III. Demonstre não possuir idoneidade para contratar com a CAIXA em virtude de atos ilícitos praticados;
IV. Convocado dentro do prazo de validade da sua proposta, não celebrar o contrato;
V. Deixar de entregar a documentação exigida para o certame;
VI. Apresentar documentação falsa exigida para o certame;
VII. Ensejar o retardamento da execução do objeto da licitação;
VIII. Não mantiver a proposta;
IX. Falhar ou fraudar na execução do contrato;
X. Comportar-se de modo inidôneo, incluindo a prática de atos lesivos à Administração Pública previstos na Lei 12.846/2013 e desatender e/ou violar o Código de Conduta do Fornecedor CAIXA.
XI. Descumprir a legislação pertinente à responsabilidade social, ambiental e climática e gerenciamento do risco social, ambiental e climático;

Parágrafo Quarto – As penalidades indicadas nesta cláusula, com exceção da multa de mora, aplicadas pela autoridade competente da CAIXA, após regular processo administrativo e garantida a defesa prévia, serão lançadas no Sistema de Cadastramento Unificado de Fornecedores – SICAF;

Parágrafo Quinto – As penalidades serão devidamente publicadas no DOU e lançadas no sistema CGU-PJ, mantendo, desta forma, atualizado o Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS.

Parágrafo Sexto – A penalidade de suspensão aplicada à CONTRATADA alcança a figura dos sócios, administradores e dirigentes.

CLÁUSULA DÉCIMA TERCEIRA – DOS ILÍCITOS PENAIS

As infrações penais tipificadas nos artigos 337-E a 337-P do Decreto-Lei nº 2.848/40 (Código Penal) serão objeto de processo judicial na forma legalmente prevista, sem prejuízo das demais cominações aplicáveis.

CLÁUSULA DÉCIMA QUARTA – DA INEXECUÇÃO E DA RESCISÃO DO CONTRATO

A rescisão do contrato se dá:

I De forma unilateral, assegurada a prévia defesa;

II Por acordo entre as partes, reduzida a termo no processo, desde que haja conveniência para a CAIXA e para o contratado;

III Por determinação judicial;

IV De forma antecipada pela CAIXA, mediante comunicação escrita à contratada, com antecedência mínima de 30 (trinta) dias.

Parágrafo Primeiro – Constituem motivo para a rescisão unilateral do contrato:

I O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

II A decretação de falência ou a instauração de insolvência civil da CONTRATADA;

III O descumprimento do disposto no inciso XXXIII do artigo 7º da Constituição Federal, que proíbe o trabalho noturno, perigoso ou insalubre a menores de 18 anos e qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;

IV A prática de atos lesivos à Administração Pública previstos na Lei 12.846/2013;

V Inobservância da vedação ao nepotismo;

VI Prática de atos que prejudiquem ou comprometam à imagem ou reputação da CAIXA, direta ou indiretamente.

VII Razões de interesse público, de alta relevância, amplo conhecimento e devidamente justificadas.

Parágrafo Segundo – A rescisão decorrente dos motivos elencados nos incisos acima será efetivada após o regular processo administrativo, quando for o caso.

Parágrafo Terceiro - Os efeitos da rescisão do contrato serão operados a partir da comunicação escrita sobre o seu julgamento, ou, na impossibilidade de notificação do interessado, por meio de publicação oficial.

Parágrafo Quarto – Caso a descontinuidade do contrato traga prejuízos à CAIXA, a decisão poderá prever que os efeitos da rescisão ocorrerão em data futura.

Parágrafo Quinto - Havendo a rescisão do contrato, cessarão todas as atividades da CONTRATADA, relativamente ao serviço contratado.

CLÁUSULA DÉCIMA QUINTA – DOS RECURSOS ORÇAMENTÁRIOS

As despesas decorrentes da presente contratação correrão à conta de dotação orçamentária prevista no item de acompanhamento orçamentário 5704-03, Plano de Trabalho GETRS 9953980001, Centro de Custo 5398, Pré-comprometimento no SAP 8000047226.

CLÁUSULA DÉCIMA SEXTA – DA SUBCONTRATAÇÃO

É vedado à CONTRATADA a subcontratação de empresa para a prestação dos serviços objeto deste contrato.

CLÁUSULA DÉCIMA SÉTIMA – ALTERAÇÕES CONTRATUAIS
Este contrato poderá ser alterado, por acordo entre as partes, nos seguintes casos:

I Quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

II Quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos pela Lei nº. 13.303/2016;

III Quando necessária a modificação do regime de execução da obra ou serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

IV Quando necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de fornecimento de bens ou execução de obra ou serviço;

CLÁUSULA DÉCIMA OITAVA – DAS DISPOSIÇÕES FINAIS
As partes ficam, ainda, subordinadas às seguintes disposições:

I É facultado a alocação de empregados portadores de deficiência nos locais de prestação dos serviços, cabendo à CONTRATADA avaliar a compatibilidade entre a deficiência apresentada e a atividade a ser desempenhada.

II A CAIXA, para atender às necessidades do serviço, poderá, a seu exclusivo critério, alterar, definitiva ou provisoriamente, o horário de início da prestação dos serviços, mediante prévia comunicação à CONTRATADA;

III Em razão de eventuais alterações estruturais da CAIXA, poderá haver modificações nos locais de prestação dos serviços, caso em que a CAIXA notificará a CONTRATADA para promover as mudanças necessárias;

IV É vedado à CONTRATADA caucionar ou ceder os créditos do presente contrato, para qualquer operação financeira, sem prévia e expressa autorização da área da CAIXA responsável pela operação pretendida;

V Nos casos de utilização deste contrato como garantia para concessão de crédito ou formalização de negócio para a CONTRATADA junto à CAIXA, a autorização caberá à área negocial responsável pelas tratativas;

VI Na cessão de créditos para outras instituições financeiras, que não a CAIXA, a autorização caberá à área gestora do contrato;

VII O pagamento de salários, benefícios e demais verbas trabalhistas, previdenciárias e sociais, referentes aos empregados alocados na prestação dos serviços objeto deste contrato, bem como multas e ressarcimentos por prejuízos sofridos pela CAIXA terão preferência sobre a cessão dos créditos;

VIII A CONTRATADA está ciente de que deve guardar por si, por seus empregados, ou prepostos, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados, ou que, por qualquer forma ou modo, venham tomar conhecimento, o mais completo e absoluto sigilo, em razão dos serviços a serem confiados, ficando, portanto, por força da lei, civil e penal, responsável por sua indevida divulgação e descuidada ou incorreta utilização, sem prejuízo da responsabilidade por perdas e danos a que der causa.

IX O caso de MPE optante pelo Simples Nacional, a Declaração de Empresas Optantes do Simples Nacional, apresentada no ato da assinatura do contrato e que o integra, permite à contratada a obtenção do benefício da dispensa de retenção dos tributos federais, na forma da IN RFB 1.244/2012.

X É admitida como válida a assinatura de forma eletrônica dos documentos apresentados, bem como para assinatura do presente contrato, utilizando Certificado Digital no padrão da Infraestrutura de Chaves Públicas Brasileira –ICP Brasil ou Sistemas eletrônicos com senha pessoal e intransferível capaz de comprovar a autoria e a integridade dos documentos, na forma do § 2º do art. 10 da Medida Provisória nº 2.200-2/2001.

CLÁUSULA DÉCIMA NONA – DO FORO

Para dirimir as questões oriundas deste Contrato, será competente a Seção Judiciária da Justiça Federal do Distrito Federal.

E por estarem, assim, justas e contratadas, as partes firmam o presente, em 02(duas) vias de igual teor e forma.

Em caso de assinatura eletrônica, conforme previsão legal, o título se reveste de eficácia executiva, dispensando-se a assinatura de testemunhas.

Brasília/DF, 08 de dezembro de 2025

OSEIAS DIAS DUARTE
CPF:692.472.421-34
10-dez-2025 | 12:46 BRT

Luiz Chaves Soares
CPF:100.406.118-84
10-dez-2025 | 12:56 BRT

Ricardo Fraga Moreira Miragai
CPF:100.406.118-84
10-dez-2025 | 07:54 PST

CAIXA
CONTRATANTE

OBVIO BRASIL SOFTWARE E SERVIÇOS S/A
CONTRATADA

ANEXO I

TERMO DE REFERÊNCIA

1 OBJETO

1.1 Contratação de soluções do portal Reclame AQUI, incluindo acesso à base de dados digital do portal, para atuação da CAIXA na gestão do atendimento, monitoramento e tratamento de reclamações envolvendo seus produtos e serviços, conforme condições e exigências estabelecidas neste documento e seus anexos:

ANEXO I-A	SEGURANÇA DAS INFORMAÇÕES E PRIVACIDADE
ANEXO I-B	REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES
ANEXO I-C	REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES DE NUVEM

1.2 As soluções deverão ser prestadas diretamente pela CONTRATADA, vedada a cessão, transferência ou subcontratação, total ou parcial, exceto por consentimento expresso da CAIXA.

1.3 O prazo do contrato é de 12 (doze) meses, contado a partir do início da prestação do serviço, podendo ser prorrogado por iguais períodos até o limite permitido pela legislação vigente.

2 EXECUÇÃO DO SERVIÇO

2.1 Os serviços contratados compreendem o acesso ao portal Reclame AQUI que deverá ser disponibilizado 7 (sete) dias por semana, 24 (vinte e quatro) horas por dia, durante todo o período de vigência da contratação.

2.2 Em caso de eventual indisponibilidade do site, a CONTRATADA deverá comunicar formalmente à CAIXA e apresentar previsão para sua regularização.

2.3 A CONTRATADA deve fornecer treinamentos específicos, gratuitamente, a cada atualização ou alteração de funcionalidades.

2.4 O serviço contratado deverá permitir:

- Inclusão de logotipos, imagens de capa e vídeos institucionais, alinhados com a identidade visual da CAIXA, além fornecer Selo de Verificação, atestando se tratar de uma conta oficial.

- Customização de formulário de reclamação, podendo incluir perguntas adicionais, com vista a facilitar e agilizar o atendimento.

- Inserção de alerta na página da CAIXA, no Reclame AQUI, para informar aos clientes problemas e/ou instabilidades tecnológicas, além de emissão de alerta, para a CAIXA, caso haja aumento, acima do esperado, no volume de reclamações.

- Atender o consumidor de maneira privada, antes da publicação da uma reclamação, sendo facultado à CAIXA, conforme estratégia definida para o atendimento, a possibilidade de ativar a opção do RA Chat, RA Contato Privado e RA Fone, ou somente ativar uma das opções para realização do atendimento.

- Acesso a dados e comportamento dos clientes e consumidores sobre desempenho, público-alvo, conteúdos, posts, cliques e comparativos com concorrentes, auxiliando a CAIXA no desenvolvimento de estratégias de atendimento, marketing e branding;

- Publicação de perguntas e respostas frequentes (FAQ), para facilitar o autoatendimento de clientes, além de posts sobre campanhas, produtos, modo de uso e até informações sobre fluxos, processos e atendimento;

- Possibilidade de habilitar botões específicos que incentivam ações dos clientes, otimizando a experiência do usuário;

- Desenvolvimento de vitrine para exibição de produtos e serviços na página da CAIXA, no Reclame Aqui, em formato carrossel de maneira randômica e botão *call-to-action* direcionado para o site da Empresa.

3 DESCRIÇÃO DOS SERVIÇOS

3.1 Para atendimento das necessidades da CAIXA, referente ao atendimento de demandas oriundas do portal Reclame AQUI, deverá ser fornecido os seguintes serviços:

ITEM	SOLUÇÃO	QUANTIDADE	DESCRIÇÃO E EXECUÇÃO	
I	HUGME	Plano para até 60 mil reclamações. Licenças adicionais: 12 – PA perfil gerentes 60 – PA perfil atendente	Software SAC 3.0, que permite o gerenciamento e tratativa de demandas do site, com painéis, emissão e extração de relatórios de desempenho e gráficos com informações sobre a posição da marca da CAIXA no portal Reclame AQUI.	Durante todo o prazo do contrato, contado a partir do início da prestação dos serviços.

II	RA BRAND PAGE PREMIUM	Até 2,5 milhões de visualizações	Software para a personalização da página da CAIXA no site Reclame AQUI, sendo possível publicar conteúdos exclusivos, colocar alerta de crise, destacar redes sociais e dúvidas frequentes (FAQ), inserir uma vitrine de produto, colocar conteúdos em destaques, dentre outros.	Durante todo o prazo do contrato, contado a partir do início da prestação dos serviços.
III	RA API E SETUP DE LIBERAÇÃO	(Conector HugMe) - para até 60.000 reclamações.	Solução tecnológica para integração da plataforma Reclame AQUI aos sistemas internos da CAIXA, automatizando o atendimento e a leitura das reclamações.	Durante todo o prazo do contrato, contado a partir do início da prestação dos serviços.
IV	RA DATA HUB	Plano 05 consultas diárias, limitado a 05 empresas únicas por mês.	Ferramenta para integração e automatização todos de todos os dados reputacionais da plataforma Reclame AQUI diretamente nos *dashboards* e sistemas da empresa, permitindo o monitoramento diário da reputação da marca CAIXA e do mercado em tempo real.	Durante todo o prazo do contrato, contado a partir do início da prestação dos serviços.
V	**SOLICITAÇÃO DE AVALIAÇÃO VIA WHATSAPP**	8.000 (oito mil) solicitações.	Funcionalidade de Solicitação de pedidos de avaliação via *WhatsApp*	Serviço programado, conforme ações e necessidade da CONTRATANTE.

4 ESPECIFICAÇÕES DOS SERVIÇOS

4.1 ITEM I – *HUGME* (durante a vigência do contrato)

4.1.1 Serviço de Licenciamento por subscrição e no formato “SaaS (Software as a Service)”, do Software HugMe RA ou de algum dos módulos HugMe, abaixo descritos.

4.1.2 Plano definido de acordo com o VOLUME DE RECLAMAÇÕES nos últimos 12 (doze) meses, exibido na página principal do perfil da CONTRATANTE, no site Reclame AQUI, sem variação do plano pelo período de 12 (doze) meses sucessivamente, quando aplicável.

4.1.3 Cada plano de acesso ao *HugMe* e seus adicionais, possui condições específicas relacionadas aos itens contratados.

4.1.4 Após a criação da Conta da CONTRATANTE e a sua vinculação aos serviços conectados, o software disponibilizará de forma automatizada, os itens e as posições de atendimento, de acordo com a contratação.

4.2 ITEM II - RA *BRAND PAGE PREMIUM* (Durante a vigência do contrato)

4.2.1 Serviço de Licenciamento por subscrição e no formato “SaaS (Software as a Service)”, do Software RA Brand Page.

4.2.2 Plano definido de acordo com o VOLUME DE VISUALIZAÇÕES únicas nos últimos 12 (doze) meses, exibido na página principal da CONTRATANTE no site Reclame AQUI, sem variação no plano durante a vigência do contrato.

4.3 ITEM III – RA API + SETUP DE LIBERAÇÃO (Durante a vigência do contrato)

4.3.1 Interface de programação que permite integrar os dados e funcionalidades do Reclame AQUI diretamente ao sistema interno da CAIXA, otimizando a análise e reposta das reclamações.

4.3.2 Plano definido de acordo com o VOLUME DE VISUALIZAÇÕES únicas nos últimos 12 (doze) meses, exibido na página principal da CONTRATANTE no site Reclame AQUI, sem variação no plano durante a vigência do contrato.

4.4 ITEM IV - RA DATA HUB (Durante a vigência do contrato)

4.4.1 Plataforma de inteligência que integra os dados reputacionais do Reclame AQUI aos sistemas da empresa. Permite monitorar a reputação da marca e do mercado em tempo real, para identificar riscos, entender o comportamento dos consumidores e gerar insights estratégicos para tomada de decisão.

4.4.2 Deverá ser disponibilizado os seguintes indicadores:

- Volume e frequência de reclamações;
- Tempo médio de resposta e resolução;
- Categorias mais citadas;
- Índice de reputação;
- Nota média dos consumidores;
- Reclamações respondidas e resolvidas;
- Clientes que voltariam a fazer negócio

4.4.3 Plano definido de acordo com a QUANTIDADE DE EMPRESAS MONITORADAS, sem variação no plano durante a vigência do contrato.

4.4.4 A CONTRATANTE poderá a qualquer tempo, solicitar alteração do plano via autorização por e-mail, Pedido de Compra, Formulário de Pedido e/ou Termo Aditivo.

4.5 **ITEM V - SOLICITAÇÃO DE AVALIAÇÃO VIA WHATSAPP** (Durante a vigência do contrato até atingimento do limite contratado)

4.5.1 A contratação da funcionalidade de solicitação de avaliação via *WhatsApp* com o objetivo elevar a reputação e a nota da CAIXA no portal Reclame AQUI.

4.5.1.1 A estratégia consiste em enviar mensagens aos clientes que tiveram suas reclamações resolvidas, mas ainda não avaliaram o atendimento na plataforma. Com essa ação, espera-se um aumento significativo na nota e na reputação da CAIXA, reforçando o compromisso com a qualidade no relacionamento com o cliente.

4.5.2 Plano definido de acordo com a quantidade de solicitações contratadas, sem variação no valor durante a vigência do contrato.

5 INDICADOR DE DESEMPENHO

5.1 A CONTRATADA deverá garantir a disponibilidade mínima de 99,50% das soluções contratadas, sujeito às penalidades em caso de disponibilidade inferior, conforme segue:

5.2 O Nível de Disponibilidade do Serviço (NDS) será calculado mensalmente, conforme fórmula que segue abaixo:

$$NDS = \left(\frac{A - B}{A}\right) X\ 100$$

Onde:
A = Tempo total em minutos em que o serviço deveria estar disponível durante o mês.
B = Tempo em minutos que o serviço ficou indisponível.

5.2.1 Para fins de cálculo do NDS, em minutos, será considerada a quantidade de dias do respectivo mês.

5.3 Caso a disponibilidade mínima estipulada no item acima não seja entregue, será realizada, na fatura subsequente, a seguinte dedução, conforme o caso:

- Disponibilidade entre 99,30% e 99,49%: 7% de desconto na fatura;
- Disponibilidade entre 99,10% e 99,29%: 10% de desconto na fatura;
- Disponibilidade menor que 99,10%: 15% de desconto na fatura.

6 OBRIGAÇÕES DA CONTRATADA

6.1 A CONTRATADA responderá pecuniariamente por danos e/ou prejuízos que forem causados à CAIXA, ou a terceiros, decorrentes de falha dos serviços ora contratados, inclusive os motivados por greves ou atos dolosos de seus empregados.

6.1.1 Assume a CONTRATADA, nesse caso, a obrigação de efetuar a respectiva indenização até o 5º (quinto) dia útil após a comunicação, que lhe deverá ser feita por escrito.

6.2 Conceder a Licença e executar os Serviços ofertados com elevados padrões de qualidade técnica.

6.3 Executar, dentro dos melhores padrões técnicos e sistêmicos, os serviços ofertados, observando toda a legislação e normas aplicáveis ao objeto.

6.4 Executar todos os serviços sob a sua total responsabilidade e administração, com profissionais competentes e capazes, para garantir um processo eficiente e resultados eficazes e com a melhor qualidade possível relativamente aos serviços ora ofertados.

6.5 Assumir todos e quaisquer riscos inerentes à sua atividade, inclusive todos os encargos trabalhistas, previdenciários, tributários e fiscais de sua responsabilidade, e a mão-de-obra empregada para a realização dos serviços ora ofertados.

6.6 Guardar estrita observância aos preceitos éticos e profissionais ligados às atividades por ela desenvolvidas.

6.7 Cumprir o NSD informado, quando aplicável.

6.8 Responsabilizar-se por todo e quaisquer prejuízos e danos causados e comprovados à Empresa em virtude, especificamente dos serviços prestados.

6.9 Observar as disposições legais e regulamentares que disciplinam a concessão da Licença e eventual prestação dos Serviços.

ANEXO I-A
SEGURANÇA DAS INFORMAÇÕES E PRIVACIDADE

1 SEGURANÇA DA INFORMAÇÃO – GRAU DE CRITICIDADE MÉDIO:

1.1 A CONTRATADA de conhecer e cumprir a Política de Segurança e Informação da CAIXA, disponibilizada no site da CAIXA (https://www.caixa.gov.br/Downloads/caixa-governanca/politica-seguranca-informacao.pdf), dando conhecimento aos seus funcionários no âmbito da prestação dos serviços objeto do contrato.

1.2 A CONTRATADA deve manter-se atualizada quanto a eventuais revisões da Política de Segurança da Informação da CAIXA.

1.3 A CONTRATADA deve proteger as informações corporativas da CAIXA e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.

1.4 A CONTRATADA deve garantir que seus empregados e colaboradores tratem de forma estritamente confidencial todas as informações obtidas durante a prestação dos serviços ou em função deles e somente as utilizem no âmbito dos serviços contratados.

1.5 A CONTRATADA deve garantir que seus empregados e colaboradores respeitem os ambientes físicos e demais locais sinalizados como área restrita, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como as restrições de compartilhamento desses materiais em qualquer mídia ou rede social.

1.6 A CONTRATADA deve garantir que as práticas de segurança da informação por ela executadas sejam divulgadas e exigidas de todos os componentes de sua cadeia de suprimento.

1.7 A CONTRATADA deve assegurar que os recursos e informações da CAIXA colocados à sua disposição sejam utilizados apenas para a finalidade contratada.

1.8 A CONTRATADA deve manter registros e evidências documentais da disseminação das práticas de segurança na cadeia de suprimentos.

1.9 A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA e seu mercado de atuação, tais como a LGPD (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014) e outras normas aplicáveis ao setor financeiro.

1.10 A CONTRATADA fica ciente de que deve guardar o mais completo e absoluto SIGILO em relação às informações e dados que tiver conhecimento em razão do serviço a ser prestado, observadas as solicitações de órgãos de regulação, fiscalização, supervisão e de controle, bem como as determinações judiciais que deverão ser comunicadas imediatamente, pois ambas somente poderão ser atendidas mediante prévia autorização da área jurídica da CONTRATANTE.

1.11 A CONTRATADA fica ciente que, por força da lei, é responsável civil e criminalmente pela divulgação indevida, descuidada ou incorreta utilização das informações corporativas da CAIXA e de seus clientes, sem prejuízo da responsabilidade por perdas e danos a que derem causa e das cominações contratuais impostas.

1.12 A CONTRATADA deve comunicar imediatamente à CONTRATANTE qualquer descumprimento às cláusulas acima, principalmente para os casos em que ficar comprovado o comprometimento de informação corporativa da CAIXA ou sob sua responsabilidade.

1.13 A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações da CAIXA assinem o Termo de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço (MO19607), por meio físico ou digital a ser informado pela CAIXA.

1.14 A CONTRATADA deve realizar ou contratar, treinamento para seus dirigentes, empregados e colaboradores, visando a sensibilização e conscientização em relação à segurança da informação e privacidade de dados, abordando no mínimo 80% do seguinte conteúdo:

Domínio Temático	Conteúdo	Carga Horária Anual
Política de Segurança da Informação	- Conhecimento da política de segurança da informação da empresa e da Política de Segurança e Informação da CAIXA.	**4 horas**
Tratamento da Informação	- Uso seguro de informações corporativas a que tiver acesso; - Adoção da política de “mesa limpa”, “tela limpa” e “impressora limpa”; - Descarte seguro de informação.	
Reporte de Incidentes	- Formas de reporte de incidentes de segurança da informação na empresa e na CAIXA.	
Fundamentos para Segurança Digital	- Conceitos básicos de segurança digital; - Uso da Internet;	
Segurança de Dispositivos Digitais Pessoais	- Proteção e privacidade em dispositivos digitais pessoais; - Conhecendo, configurando e usando o dispositivo; - Mantendo o dispositivo; -Vulnerabilidades e ameaças.	
Segurança em Redes	- Segurança na Internet; - Segurança em redes wi-fi públicas; - Proteção de redes pessoais; - Computação em nuvem.	
Segurança Do Usuário	- Autenticação no acesso a sistema e a serviços; - Proteção de contas pessoais; - Mídias sociais; - Segurança com e-mails; - Armazenamento e compartilhamento de dados; - Backup de arquivos pessoais importantes; - Qualidade de vida digital.	
Segurança e Comportamento em Mídias Sociais	- Netiqueta; - Construindo seu perfil na Internet; - Segurança em mídias sociais; - Administrando seu rastro digital; - Uso saudável de mídias sociais; - Fake News; - Jogos online.	
Comunidades Digitais	- Educação na Internet; - Construindo comunidades digitais cidadãs	

Direito Digital	- Conceitos jurídicos e legislação relacionada à segurança da informação; - Direitos autorais; - Fraudes; - Assédio virtual; - Crimes na Internet; - **Hacktivismo.*	
Prevenção à fraude	- Engenharia social (formas defensivas contra ***Phishing* e ****Smishing*).	

**Hacktivismo é normalmente entendido como escrever código fonte, ou até mesmo manipular bits, para promover ideologia política - promovendo expressão política, liberdade de expressão, direitos humanos, ou informação ética.*

***Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais, geralmente disparado por e-mail, usando links ou anexos maliciosos disfarçados em uma mensagem aparentemente legítima.*

****Smishing é um tipo de Phishing realizado por SMS e mensagens de texto enviadas para o celular. Geralmente, essas mensagens pedem para que você clique em um link e preencha um formulário ou responda à mensagem. Podem falar, por exemplo, sobre uma necessidade de atualização de cadastro ou a oportunidade de resgatar um prêmio imperdível.*

1.14.1 O referido treinamento será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual, com carga horária mínima anual de 04 horas.

1.14.2 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao ano base, a documentação comprobatória de cumprimento do treinamento.

1.15 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do período, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA, contendo indicadores de conformidade, incidentes registrados, ações corretivas e melhorias implementadas.

1.16 A CONTRATADA deve se adequar às normas e a legislação vigente inerentes à Segurança da Informação relacionadas às atividades da CONTRATANTE, enquanto empresa pública e instituição financeira.

1.17 A CONTRATANTE poderá exercer o direito de exigir alterações nos controles de segurança da CONTRATADA, à medida que os ambientes externos e internos se modifiquem.

1.18 A CONTRATADA deve solicitar formalmente autorização para subcontratação de serviços, cabendo a CONTRATANTE autorizar ou não.

1.18.1 Em caso de concretização de subcontratação de serviços, previamente autorizada pela CONTRATANTE, a CONTRATADA deverá enviar notificação mandatória sobre o fato à CONTRATANTE.

1.19 A CONTRATADA deverá informar à CONTRATANTE periodicamente, os resultados dos indicadores:

a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, treinados em Segurança da Informação, conforme item 1.14 no último ano dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base;

b) Quantidade de empregados que assinaram o Termo de Responsabilidade de Segurança da Informação, previsto no item 1.13, dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base.

1.20 O não atendimento pela CONTRATADA de qualquer requisito de segurança, definido no presente instrumento contratual, implicará em penalidades/sanções administrativas.

1.21 Em caso de indisponibilidade parcial ou total dos serviços, a CONTRATADA se compromete a cumprir as obrigações previstas no contrato e nos anexos que o integram e complementam, bem como executar o Plano de Continuidade de Serviços.

1.22 Quaisquer materiais ou documentos com informações confidenciais que tenham sido fornecidos à CONTRATADA pela CONTRATANTE serão devolvidos, acompanhados de todas as cópias, em até 5 (cinco) dias, a partir da formalização de solicitação de devolução das informações confidenciais pela CONTRATANTE.

1.23 No encerramento/finalização do contrato, a CONTRATADA se compromete a cumprir integralmente o Plano de Repasse de Conhecimentos e demais obrigações relacionadas a fase de encerramento do contrato, presentes no item 14 – PROCESSO DE DESMOBILIZAÇÃO, nos prazos definidos, além de:

a) Entregar a versão mais atualizada de todos os artefatos, componentes e demais produtos por ela produzidos durante a vigência do contrato;

b) Executar a exclusão e sanitização de dados e informações confidenciais após a devida cópia/transferência para a CONTRATANTE ou a quem ela indicar, observada a regulamentação vigente;

c) Devolver ou transferir a quem for designado pela CONTRATANTE todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.

2 PRIVACIDADE E PROTEÇÃO DE DADOS

2.1 A CONTRATADA deve ter conhecimento sobre os termos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais - LGPD e de suas regulamentações, bem como das orientações da ANPD – Autoridade Nacional de Proteção de Dados, reconhecendo sua responsabilidade objetiva e de seus empregados/colaboradores em observar o disposto na LGPD no exercício de suas atividades no tratamento de dados pessoais de clientes, empregados e colaboradores da CONTRATANTE.

2.2 Para fins deste contrato, a CONTRATANTE assume o papel de Controladora de dados pessoais e a CONTRATADA assume o papel de operadora de dados pessoais.

2.3 A CONTRATADA se compromete a tratar os dados pessoais a que tiver acesso em decorrência do presente Contrato, única e exclusivamente para cumprir a finalidade a que se destina seu tratamento, responsabilizando-se por qualquer acesso indevido.

2.4 A CONTRATADA deve garantir a confidencialidade no tratamento de dados pessoais, protegendo-os contra acesso, modificação, destruição ou divulgação não autorizada.

2.5 A CONTRATADA deve, quando do término das atividades de tratamento de dados pessoais ou ao final do contrato, a critério da CONTRATANTE, eliminar todos os dados, acompanhados de todas as cópias, após autorização.

2.6 A CONTRATADA deve colaborar com a CONTRATANTE no cumprimento de sua obrigação de responder às solicitações de exercício dos direitos dos titulares.

2.7 A CONTRATADA deve comunicar, imediatamente, à CONTRATANTE o recebimento de requisição do titular de dados no exercício de seus direitos.

2.8 A CONTRATADA garantirá à CONTRATANTE a disponibilização de todas as informações necessárias para que esta consiga demonstrar o cumprimento de suas obrigações nos termos da LGPD, mantendo a documentação disponível para a realização de auditorias e quaisquer inspeções.

2.9 A CONTRATADA deverá, obrigatoriamente, adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2.10 A CONTRATADA deve comunicar, imediatamente, à CONTRATANTE qualquer violação de dados pessoais imediatamente após tomar conhecimento, inclusive aplicando medidas de contenção, formalizando a ocorrência ao gestor operacional do contrato.

2.11 A CONTRATADA deverá comunicar, imediatamente, à CONTRATANTE qualquer solicitação judicial, de órgãos reguladores, de fiscalização, de supervisão e de controle para disponibilização de dados pessoais.

ANEXO I-B

REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES

1 GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS

1.1 A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.

1.2 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.

1.3 A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

1.4 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

1.5 Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.

1.6 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.

1.7 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no logon.

1.8 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.

1.9 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.

1.10 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.

1.11 Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.

1.12 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.

1.13 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.

1.14 A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.

1.15 A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.

1.16 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.

1.17 A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.

1.18 As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

1.19 A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.

1.20 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.

1.21 Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.

1.22 A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:

- O tipo de evento (inclusão, alteração, exclusão, consulta);
- O autor do evento;
- A data e hora do evento;
- IP e Porta do equipamento que originou o evento.

1.23 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

1.24 A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.

1.25 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.

1.26 A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto de forma segura e quais os controles necessários para oferecer este acesso de forma segura.

1.27 A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 9 deste ANEXO.

1.28 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

2 SEGURANÇA DE ATIVOS

2.1 A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.

2.2 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.

2.3 A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

2.4 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

2.5 Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.

2.6 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.

2.7 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no logon.

2.8 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.

2.9 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.

2.10 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.

2.11 Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada. A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.

2.12 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.

2.13 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.

2.14 A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.

2.15 A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.

2.16 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.

2.17 A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.

2.18 As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

2.19 A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.

2.20 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.

2.21 Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.

2.22 A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:

- O tipo de evento (inclusão, alteração, exclusão, consulta);
- O autor do evento;
- A data e hora do evento;
- IP e Porta do equipamento que originou o evento.

2.23 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

2.24 A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.

2.25 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo-real e deve ser possível configurar respostas automatizadas para eventos específicos.

2.26 A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.

2.27 A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 9 deste ANEXO.

2.28 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

3 SEGURANÇA DE REDES

3.1 Todo o tráfego de rede associado ao objeto do contrato deve ser mediado por uma solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações).

3.2 O conjunto de regras do firewall deve se basear na negação de todos os serviços, exceto aqueles especificamente permitidos.

3.3 O processo para instalação e adaptação de regras de firewalls deve ser feito com duplo controle.

3.4 A Contratada deve revisar as regras de firewall pelo menos semestralmente, guardando evidências dessas revisões e dos ajustes eventualmente realizados, comunicando à CAIXA sobre a realização desta revisão.

3.5 Todos os componentes de gateway de perímetro e sistemas de computadores devem ser monitorados contra tentativas de intrusão, por meio de solução de prevenção e detecção de intrusão (IPS).

3.6 O monitoramento de segurança deve ser configurado para rastrear e registrar tentativas de intrusão suspeitas ou reais.

3.7 A Contratada deve informar imediatamente à CAIXA em caso de tentativa de intrusão real, e informar à CAIXA em relatório mensal sobre as tentativas de intrusão suspeitas.

3.8 A Contratada deve implementar solução anti-DDoS, capaz de prevenir ataques de negação de serviço (Denial of Service).

3.9 As soluções de firewall, IPS e-DDoS utilizadas pela Contratada serão validadas pela CAIXA a partir de documentações do fabricante ou certificações.

3.10 A Contratada deve impedir o uso do protocolo Bluetooth para a transferência de dados.

3.11 Todas as comunicações e trocas de informações entre a Contratada e a CAIXA devem ser realizadas por meio de conexão protegida, com TLS 1.3 ou superior.

3.12 Para os casos aplicáveis, os acessos diretos de diferentes equipamentos ao serviço da Contratada devem ser gerenciados por ferramentas de gerenciamento de dispositivos e/ou aplicativos (MDM/MAM) ou controle de acesso à rede (NAC).

4 CICLO DE VIDA DE DESENVOLVIMENTO SEGURO

4.1 A Contratada deve adotar o princípio de *security by design* para garantir que as aplicações de TI por ela desenvolvidas sejam seguras desde a concepção.

4.2 A Contratada deve fazer análise de código automatizada com base nas melhores práticas de mercado, utilizando como referência os padrões do OWASP.

4.3 A Contratada deve fazer análise de código estática (SAST) e dinâmica (DAST) periodicamente e de forma integrada ao ciclo de desenvolvimento como um todo para a solução Contratada. Essas análises precisam ser executadas pelo menos uma vez por ano ou quando houver uma mudança considerada significativa nas funcionalidades do sistema/aplicação (como a inclusão de uma nova funcionalidade crítica ou manutenção em módulos que tratem informações sensíveis e confidenciais). A bateria de testes deve incluir testes de resistência, injeções de falhas, teste de penetração e teste de vulnerabilidades onde aplicável.

4.4 A Contratada deve incluir a análise e a remediação das vulnerabilidades detectadas como parte do ciclo de vida de desenvolvimento de software padrão, sem custo adicional para a CAIXA, dentro de um período razoável e de acordo com a criticidade da falha encontrada.

4.5 A Contratada deve estabelecer critérios de escala e prazo para correção das vulnerabilidades e deve definir as alçadas para aceitação de riscos. Adicionalmente, devem ser estabelecidas responsabilidades por perdas causadas por incidentes decorrentes de vulnerabilidades identificadas nos testes de segurança, que não foram tratadas ou corrigidas em tempo hábil.

4.6 A Contratada deve submeter suas políticas de desenvolvimento seguro à aprovação da CAIXA.

4.7 Os relatórios dos testes realizados e o planejamento das correções a serem feitas devem ser disponibilizados à CAIXA sempre que solicitado.

5 GESTÃO DE SERVIÇOS E MUDANÇAS

5.1 A Contratada deve ter um processo de Gestão de Mudanças para garantir a proteção contínua dos ativos de informação e dados, em particular aqueles que fazem parte do escopo do objeto do contrato.

5.2 A Contratada deve revisar periodicamente as atividades de gestão de mudanças, incluindo a acurácia da Base de Dados de Gerenciamento de Configuração (*Configuration Management Database* – CMDB).

5.3 A Contratada deve cumprir com os procedimentos de registros de informações relacionadas ao processo de gestão de mudanças, no contexto do contrato, incluindo:

- Referência da mudança;
- Data de implementação;
- Avaliação de impactos;

- Resultados do teste;
- Procedimentos de *rollback*;
- Alterações de emergência;
- Atualizações relacionadas ao inventário de ativos de informação;
- Armazenamento Seguro de mídia de backup produzidos durante a atualização;
- Atualização dos procedimentos de Documentação e de trabalho;
- Atualizações aos documentos de Plano de Continuidade dos Negócios / Recuperação de Desastres se for o caso;
- Categorização, priorização e procedimentos de emergência;
- Autorização de mudança;
- Gerenciamento de liberação;
- Link para incidentes / problemas (conforme apropriado);
- Quando o escopo do sistema é expandido para incluir novos ativos de informação com novas funcionalidades;
- Quando uma nova comunidade de usuários é introduzida; ou
- Anualmente, por se tratar de risco cibernético, nos termos do art. 8º da Resolução BACEN 4.893/2021.

5.4 A Contratada só deve promover os aplicativos e sistemas relacionados ao escopo do objeto do contrato para o ambiente de Produção após a realização com sucesso dos testes predefinidos baseados em caso de uso.

5.5 A Contratada deve conduzir uma avaliação de risco e ameaças, contemplando inclusive os testes baseados em casos de uso, quando da implantação de uma mudança.

5.6 A Contratada deve realizar uma avaliação de risco:

- Quando o escopo do sistema é expandido para incluir novos ativos de informação com novas funcionalidades;
- Quando uma nova comunidade de usuários é introduzida; ou
- Anualmente, por se tratar de risco cibernético, nos termos do art. 8º da Resolução BACEN 4.893/2021.

5.7 A Contratada deve disponibilizar os documentos de avaliação de risco à CAIXA sempre que solicitado.

6 GESTÃO DE INCIDENTES DE SEGURANÇA

6.1 A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.

6.2 A Contratada deve realizar testes independentes de penetração/invasão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para a CAIXA. O escopo dos testes será previamente combinado e aprovado pela CAIXA, dentro dos limites do contrato.

6.3 Os testes de penetração/invasão terão como escopo, rede, aplicação web, Application Programming Interface (API), serviços hospedados e; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; dentre outros.

6.4 Todos os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções necessárias, serão fornecidos à CAIXA sempre que solicitado.

6.5 A Contratada deverá possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.

Nível de severidade	Descrição do nível de severidade	Prazo Máximo
Severidade 1 (Crítica)	Eventos cujo contexto principal é a segurança cibernética, tais como: -Impacto em ativos ou serviços críticos de TI; -Violação significativa de dados sensíveis; -Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente. **Exemplos não exaustivos:** ataque de *Ransomware*, ataque de negação de serviço distribuído – DDoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.	2 horas após o início da ocorrência.
Severidade 2 (Alta)	Eventos cujo contexto principal é a segurança cibernética, tais como: -Impacto em ativos ou serviços de TI de alta criticidade; -Detecção de acesso não autorizado e/ou alterações em sistemas de informação; -Infecção persistente por código malicioso; -Intrusão persistente na rede; -Incidentes de segurança cibernética envolvendo dirigentes; -Ameaça significativa à disponibilidade e/ou integridade do ambiente; -Ameaça significativa à imagem da CAIXA. **Exemplos não exaustivos**: ataques de escalação de privilégio em servidores, ataques do tipo brute force e password spray. Dentre outros	4 horas após o início da ocorrência.

6.6 A contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.

6.7 O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou a CAIXA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA.

6.8 A Contratada deverá ter um processo de notificação de incidentes 24x7.

6.9 A Contratada deverá comunicar à CAIXA incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.

6.10 Os incidentes serão comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA, que opera 24x7, por meio do endereço de e-mail: abuse@caixa.gov.br. Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.

6.11 A Contratada deverá comunicar à CAIXA, dentro do prazo acordado, todos os incidentes detectados que envolvam os serviços prestados, conforme a classificação abaixo:

6.12 Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA.

6.13 A Contratada deverá fornecer descrição detalhada dos incidentes, incluindo informações suficientes para classificá-los por nível de severidade, conforme a definição dos eventos. As informações sobre incidentes podem ser enriquecidas utilizado o modelo do MITRE ATT&CK®.

6.14 A contratada deverá seguir preferencialmente o modelo de comunicação de ISCF – Incidente de Segurança Cibernética em Fornecedor, a ser fornecido pela CAIXA, que também contempla situações de incidentes de segurança com dados pessoais.

6.15 Vale ressaltar que em se tratando de contratos para tratamento de dados pessoais, nos termos da LGPD, a Contratada deve provar que tem capacidade de fornecer uma resposta organizada e eficaz a um incidente de privacidade. Neste sentido, a CAIXA desenvolverá e implementará juntamente com o fornecedor do serviço um plano de resposta a incidentes de privacidade, que inclua por exemplo, definição de incidente de privacidade e o escopo da resposta ao incidente, estabelecimento de equipes multifuncionais de resposta a incidente de privacidade, entre outros aspectos relevantes.

6.16 A Contratada deve documentar os casos de uso que são utilizados para realizar a configuração e o monitoramento de eventos, correlacionando tecnologias para tratar padrões / cenários de ataque comuns e avançados; e disponibilizar os casos de uso à CAIXA sempre que solicitado.

6.17 A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.

6.18 A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.

6.19 Se a Contratada precisar envolver outras partes externas para investigar e/ou resolver incidentes que afetem o escopo do objeto contratado, ela deve obter a anuência da CAIXA por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA.

7 CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

7.1 A Contratada deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

7.2 O referido plano de continuidade deverá ser informado para a CAIXA como parte das ações de acompanhamento do contrato, e deverá ser atualizado e testado anualmente, ou em qualquer mudança significativa do ambiente.

7.3 A atuação, em caráter de contingência, causada por uma eventual indisponibilidade do serviço prestado, considera as seguintes premissas:

a) Interrupção total ou parcial dos serviços;
b) Ter infraestrutura alternativa: física e lógica em local distante do ambiente central de produção, com o objetivo de minimizar o risco de perda de ambas as instâncias;
c) Manter os serviços essenciais suportados pelo contrato;
d) Manter a lista de integrantes das equipes e o Plano de Recuperação de Desastres atualizados;
e) Ter local seguro para guarda de backups fora do local atingido;
f) Assegurar a disponibilidade dos serviços essenciais dentro do tempo previsto para recuperação do serviço, de acordo com o contrato;
g) Procedimento documentado e evidenciado de testes das mídias armazenadas *offsite*;
h) Cópias de todos os procedimentos abordando backup, restauração e reconstituição de armazenamento de dados.

7.4 O plano de continuidade deve possuir os seguintes elementos em sua composição:

a) Identificação do serviço suportado pelo contrato;
b) A forma de conectividade usada e os direitos de acesso;
c) A arquitetura do ambiente de produção;
d) As interfaces de aplicações e suas dependências;
e) O SLA contratado e os limites suportados para interrupção;
f) A forma de replicação dos dados com o site alternativo;
g) Procedimentos adotados para recuperação de desastres;
h) Lista de contatos das equipes responsáveis pelo restabelecimento do serviço, divididos por tipos de atividades executadas.

7.5 A obrigatoriedade do plano de continuidade se estende para empresas que sejam subcontratadas pela Contratada.

7.6 A Contratada deve considerar, como parte do plano de continuidade, os diferentes ambientes de risco e o grau de mitigação de riscos necessários para proteger a Instituição, caso seja necessário colocar o plano em prática.

7.7 A avaliação de riscos e dos processos críticos devem levar em consideração instrumentos específicos, como um BIA – *Business Impact Analysis*.

7.8 A Contratada, visando a continuidade dos negócios, deve implantar uma política de backup, conforme exposto no item 10 deste ANEXO.

8 AUDITORIA CONTÍNUA

8.1 A Contratada deve apresentar à CAIXA, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.

8.2 A Contratada deve informar imediatamente à CAIXA sobre qualquer auditoria regulatória, sua finalidade e como ela se relaciona com os serviços prestados à CAIXA.

8.3 A Contratada deve informar à CAIXA caso sejam contatados por um órgão regulador e se o propósito desse contato pode estar relacionado com/ou afetar os serviços prestados à CAIXA.

8.4 A Contratada deve fornecer os subsídios necessários para que a CAIXA implemente os indicadores de desempenho de segurança que vierem a ser definidos durante a vigência do contrato.

8.5 A Contratada deverá disponibilizar, caso a CAIXA solicite, acesso às instalações da Contratada para realização de processo de *Due Dilligence* Presencial, para verificar o cumprimento dos requisitos de segurança.

8.6 Caso a Contratada não tenha certificação SOC Nível 2, ela deverá fazer auditoria externa independente, pelo menos uma vez por ano, em relação ao cumprimento dos requisitos de segurança estabelecidos neste documento, e apresentar os relatórios à CAIXA sempre que solicitado.

9 CONTROLES CRIPTOGRÁFICOS

9.1 A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.

9.2 A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.

9.3 A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.

9.4 A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.

9.5 Caso a Contratada hospede uma página com uma URL e um certificado gerados pela CAIXA, a Contratada deverá armazenar este certificado em dispositivo seguro com bloqueio para exportação da chave.

9.6 As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.

9.7 A Contratada deve permitir a criptografia de volume (por exemplo: a criptografia de um disco inteiro) e a criptografia de estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).

9.8 A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.

9.9 A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.

9.10 A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.

9.11 A Contratada deve permitir a auditoria da segurança de chaves criptográficas.

9.12 A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3 e superior.

10 POLÍTICA DE BACKUP

10.1 A Contratada deve possuir e implementar política de backup das informações e dos registros de log associados ao objeto do contrato, em conformidade com os dispositivos legais aplicáveis.

10.2 A política de *backup* deve assegurar a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica e os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha, ou por solicitação da CAIXA.

10.3 A Contratada deve prover pelo menos um site de armazenamento alternativo – e geograficamente distinto - como parte de sua política de *backup*, permitindo o armazenamento e a recuperação da informação sempre que necessário e de acordo com os requisitos definidos no item 7 deste ANEXO.

10.4 A Contratada deve garantir que o site de armazenamento alternativo conta com os mesmos controles de segurança do site de armazenamento primário.

11 RELATÓRIOS QUE COMPROVAM O CUMPRIMENTO DOS REQUERIMENTOS MÍNIMOS DE SEGURANÇA.

11.1 Sempre que a CAIXA julgar necessário, poderá realizar Due Diligence presencial ou remota para verificar os requisitos de segurança presente nas cláusulas, são atendidos pela Contratada. O Due Diligence presencial é facultativo e será feito a critério da CAIXA.

11.2 Os documentos exigidos devem ter a sua primeira versão entregue antes da assinatura do contrato, que comprovam o cumprimento dos requerimentos de segurança cibernética conforme estabelecido nas cláusulas e devem ser reiterados de acordo com a vigência indicada nos quadros abaixo:

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da Contratada para verificar os requisitos de segurança presente nas cláusulas	A CAIXA, por iniciativa própria, fará due diligence presencial em função de discrepâncias identificadas em relatórios de auditoria entregues ou dúvidas onde apenas a documentação não seja suficiente.	A visita poderá ser realizada por equipe própria da CAIXA ou empresa designada pela CAIXA	SOB DEMANDA

Due Diligence Remoto	Constatar que os processos determinados pela CAIXA estão sendo seguidos, conforme descrito nas cláusulas.	Documentos previstos nas cláusulas e demais comprovantes de seus requisitos. Quando não comprovados por certificação, os itens exigidos nas cláusulas devem ser certificados por empresa de auditoria independente.	Relatórios próprios da empresa para comprovação do atendimento aos itens das cláusulas, desde que ratificados por empresa de auditoria independente Relatório de empresa de auditoria independente, a ser apresentado pela Contratada	SOB DEMANDA
Certificação SOC 2 – Tipos 1 e 2	Garantir acesso a uma avaliação independente, por meio de relatório de auditoria, sobre o ambiente de controle do provedor, relevante para a segurança, disponibilidade, confidencialidade e privacidade	SOC TYPE 2 Fornece relatórios com descrição do ambiente de controles do provedor e da auditoria externa dos controles que atendem aos princípios e critérios de segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA	Disponibilizar relatório de auditoria em nome da empresa	ANUAL

12 ENCERRAMENTO DO CONTRATO

12.1 A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.

12.2 A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.

12.3 Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.

12.4 A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer aos padrões definidos no NIST SP 800-88 Guidelines for Media Sanitization, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.

12.5 Caso a Contratada tenha ativo de informação no fim do ciclo de vida, ou considerado inservível, este ativo deverá ser destruído, com o fornecimento do Certificado de Destruição de Equipamento Eletrônico (*Certificate of Electronic Equipment Destruction* – CEED), discriminando os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição.

13 **NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS**

13.1 O não cumprimento, pela Contratada, de qualquer um dos seguintes requisitos de segurança, definidos neste instrumento contratual, ensejará a aplicação das penalidades previstas neste contrato e poderá, a critério da Contratante, ensejar a rescisão imediata do contrato, sem prejuízo de outras medidas cabíveis:

a) Omitir ou deixar de comunicar à CAIXA, de forma tempestiva e adequada, qualquer ocorrência de intrusão real, tentativa de acesso indevido ou outros incidentes relacionados à segurança tecnológica;
b) Deixar de apresentar, total ou parcialmente, as informações, documentos e relatórios solicitados pela CAIXA, nos prazos e condições acordadas.

ANEXO I-C

REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES DE NUVEM

1 GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS

1.1 A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.

1.2 A Contratada deve manter rígido controle de acesso de seus colaboradores baseado nas informações de contratação, dispensa e controle de ausências (férias, licenças, atestados, admissão, demissão etc.) impedindo o acesso ao ambiente computacional, local ou remoto, quando o colaborador não estiver em pleno exercício de suas atividades.

1.3 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.

1.4 A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

1.5 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

1.6 Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.

1.7 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.

1.8 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no logon.

1.9 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.

1.10 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.

1.11 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.

1.12 Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.

1.13 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.

1.14 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.

1.15 A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.

1.16 A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.

1.17 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.

1.18 A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.

1.19 As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

1.20 A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.

1.21 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.

1.22 Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.

1.23 A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:

- O tipo de evento (inclusão, alteração, exclusão, consulta);
- O autor do evento;
- A data e hora do evento;
- O endereço lógico do equipamento de origem do tipo do evento.

1.24 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

1.25 A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.

1.26 Devem ser observadas as boas práticas de segregação e diferenciação entre ambientes de não produção e produtivo, estabelecendo-se acessos pertinentes para cada etapa do ciclo de desenvolvimento/manutenção e alinhado com o princípio do privilégio mínimo.

1.27 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo-real e deve ser possível configurar respostas automatizadas para eventos específicos.

1.28 A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.

1.29 A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 2.4.

1.30 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

2 CONTROLES CRIPTOGRÁFICOS

2.1 Os requisitos apresentados devem ser obedecidos pela Contratada ou, caso os dados estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor. Neste último caso, a Contratada deverá comprovar por relatório de auditoria (*Due Dilligence* Remoto) que o armazenamento/processamento dos dados ocorre somente em ambiente de nuvem.

2.2 A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.

2.3 A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.

2.4 A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.

2.5 A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.

2.6 A Contratada deve fazer a geração e a renovação de certificados digitais expostos na Internet junto a autoridades certificadoras reconhecidas internacionalmente, cujas raízes de cadeias utilizadas na emissão dos certificados digitais façam parte do repositório de cadeias confiáveis dos principais navegadores e versões de sistemas operacionais, como: iOS 7 e superiores; Android 4 e superiores; Microsoft Edge 12 e Safari 8 e superiores; Linux Ubuntu 14 e superiores; Linux Mint 15 e superiores; MAC OS X 10.10 e superiores; e Windows 7 e superiores.

2.7 A Autoridade Certificadora deve possuir o selo Web Trust dentro do prazo de validade e a certificação Web Trust deve estar de acordo com, no mínimo, os Princípios e Critérios para Autoridades Certificadoras – versão 2.2.1, disponível em https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wt100awebtrust-for-ca-221-110120-finalaoda.pdf?la=en&hash=0FDB6C541E7A61976625B9EAC55474D260A7E6FD para todas as raízes de cadeias utilizadas na emissão dos certificados digitais.

2.8 Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (https://www.ssllabs.com/ssltest).

2.9 As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.

2.10 Caso haja a necessidade do compartilhamento de chaves simétricas entre a CAIXA e a Contratada, essas chaves devem ser geradas pela CAIXA e levadas para o ambiente da Contratada, onde devem ser armazenadas por meio de soluções FIPS 140-2 nível 3, sem possibilidade de exportação das chaves. Nesse caso, a Contratada deve prover meios que permitam a inserção das chaves da CAIXA no seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.

2.11 No caso de utilização de um Provedor de Serviços em Nuvem, as certificações FIPS exigidas estão descritas no item 10.

2.12 A Contratada deve permitir a criptografia de dados em repouso, considerando volumes (por exemplo: a criptografia de um disco inteiro) e estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).

2.13 A Contratada deve prover a criptografia de dados em repouso utilizando, no mínimo, algoritmo AES com chaves de 128 bits.

2.14 A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.

2.15 A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.

2.16 A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.

2.17 A Contratada deve permitir a auditoria da segurança de chaves criptográficas.

2.18 A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3, ou, quando não for suportado, 1.2.

2.19 A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA, suportando, no mínimo, TLS 1.2 e as cifras a seguir:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

2.20 Os parâmetros TLS Renegotiation e TLS Ressumption devem estar desabilitados.

2.21 Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão TLS, por exemplo – a Contratada deve fazer todas as validações previstas no método X509_verify_cert, existente na estrutura do Openssl.

2.22 O certificado de cliente só deve ser aceito se o método X509_verify_cert retornar OK para todas as validações previstas.

3 CONTROLE DE ACESSO AO AMBIENTE DE NUVEM

3.1 Quando viável tecnicamente, o acesso de empregados CAIXA à nuvem deverá ser integrado com ferramenta de SSO da CAIXA, ou com o AD, para garantir o uso das credenciais internas, isso deve garantir que o usuário não acesse o ambiente do parceiro, caso seja desligado ou esteja ausente da CAIXA por qualquer motivo por período determinado.

3.2 Como apresentado no item 2.4, quando a autenticação for provida pela Contratada ou pelo Provedor de Serviços em Nuvem, deverá ser realizada autenticação por múltiplos fatores para o acesso dos empregados da CAIXA, que precisem acessar os recursos em nuvem.

3.3 O acesso aos recursos da CAIXA deverá ser realizado em tenant designado especificamente, sem que estes recursos sejam compartilhados com qualquer outra entidade, bem como a camada de dados da aplicação não pode ser compartilhada com outros clientes do Provedor de Serviços em Nuvem.

3.4 O Provedor de Serviços em Nuvem deve permitir que somente os usuários autorizados pela CAIXA tenham acesso aos recursos em conformidade aos respectivos perfis de uso.

3.5 Os acessos administrativos aos recursos do Provedor de Serviços em Nuvem, nos tenants que atendam à CAIXA, deverão ser feitos através de rede privada, tanto para empregados CAIXA quanto para representantes do Provedor.

4 REQUISITOS DE AUTORIZAÇÃO DE ACESSO AOS DADOS PELO BACEN

4.1 A Contratada deve garantir que a prestação dos serviços não causará prejuízo ao funcionamento regular da CAIXA nem embaraço à atuação da Banco Central do Brasil, assegurando que a legislação e a regulamentação nos países e nas regiões em cada CAIXA nem do Banco Central do Brasil aos dados e às informações.

4.2 A Contratada deve assegurar que os dados sujeitos a limites geográficos não serão migrados para além das fronteiras definidas em contrato, incluindo dados de backup, dados em produção, dados em repouso, contingência ou recuperação de desastre sem prévio conhecimento da CAIXA por meio comunicação formal.

4.3 Deve ainda garantir acesso à CAIXA, a qualquer tempo, aos dados e às informações processadas, armazenadas e geradas pela atividade de processamento, Log, sob responsabilidade da Contratada.

4.4 Esta mesma Contratada deve assegurar que os dados da CAIXA processados e armazenados na Contratada são de propriedade exclusiva da CAIXA.

4.5 A Contratada deve assegurar também que o acesso aos dados processados e armazenados na Contratada é de acesso exclusivo da CAIXA, não sendo autorizado acesso da Contratada ou terceiros sem autorização formal da CAIXA.

4.6 A Contratada deve assegurar a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas e/ou armazenadas em nuvem.

4.7 Também deve assegurar à CAIXA acesso aos relatórios e documentos elaborados por empresa de auditoria especializada independente, contratada pelo provedor de serviço em nuvem, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados a qualquer tempo.

4.8 A Contratada deve assegurar à CAIXA, acesso a toda documentação comprobatória, em nome do provedor, que esclareça a Região/Zona de Disponibilidade escolhidos pela CAIXA para hospedagem de seus recursos.

4.9 A Contratada deve assegurar a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.

4.10 A Contratada deve garantir, em caso de decretação de regime de resolução da CAIXA pelo Banco Central do Brasil, acesso pleno e irrestrito aos contratos e acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.

4.11 A Contratada deve garantir notificação prévia ao responsável pelo regime de resolução sobre a intenção da empresa Contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observado que:

4.11.1 A Contratada assegura o atendimento de eventual pedido de prazo adicional de (30) trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução.

4.11.2 Caso haja subcontratação do serviço em nuvem, desde que explicitamente autorizado pela CAIXA, é obrigatório a Contratada apresentar a garantia formal do atendimento das cláusulas deste item 4 por parte da Provedor de Serviços em Nuvem, seja por meio de declaração própria durante o processo de contratação, seja por meio de aditivo contratual, caso não previsto inicialmente no contrato original.

5 PROTEÇÃO DOS DADOS PROCESSADOS E ARMAZENADOS EM NUVEM

5.1 Além dos requisitos descritos no item 3, a Contratada também deve permitir trabalhar com chaves simétricas e assimétricas geradas e armazenadas pela CAIXA. Para tanto, ela deve prover meios que permitam o envio das chaves da CAIXA para o seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.

5.2 Caberá à CAIXA decidir quem fará a geração e a gestão de cada chave: se a própria CAIXA ou a Contratada.

5.3 Caso a CAIXA decida fazer a geração de chaves assimétricas, ela definirá a Autoridade Certificadora que será utilizada na emissão dos certificados digitais e fornecerá a cadeia certificadora para a Contratada sempre que necessário. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (https://www.ssllabs.com/ssltest).

5.4 O modelo Third Party Certificates pode ser oferecido para o caso de certificados digitais utilizados no estabelecimento de conexões TLS. Nesse caso específico, as chaves devem ficar armazenadas exclusivamente em repositórios de chaves da Contratada e esta deve emitir o CSR (Certificate Signing Request) e enviá-lo para a CAIXA, que providenciará a emissão dos certificados digitais correspondentes. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (https://www.ssllabs.com/ssltest).

5.5 Quando a Contratada for diferente do Provedor de Serviços em Nuvem e estiver agindo em nome deste, as chaves devem ser compartilhadas diretamente entre o Provedor e a CAIXA e a Contratada não deverá ter qualquer acesso às chaves envolvidas.

5.6 Quando se tratar de contratação no modelo IaaS, exige-se a certificação FIPS 140-2 nível 3.

5.7 Quando se tratar de contratação no modelo PaaS ou SaaS, exige-se a certificação FIPS 140-2 nível 2.

5.8 O Provedor de Serviços em Nuvem deve permitir que os usuários criptografem seus dados e objetos antes de enviá-los para o serviço de armazenamento.

5.9 A Contratada, assim como o Provedor de Serviços em Nuvem, deve tratar com rigor as informações sigilosas, não podendo ser usadas ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal da CAIXA.

5.10 A Contratada deverá assinar Termo de Confidencialidade resguardando que os recursos, dados e informações de propriedade da CAIXA, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

5.11 Os dados, metadados, informações e conhecimento tratados pela Contratada, não poderão ser fornecidos a terceiros e/ou usados por esta para fins diversos do previsto, sob nenhuma hipótese, sem autorização formal da CAIXA.

5.12 A CAIXA e a Contratada obrigam-se por seus empregados, sócios, diretores e mandatários, manter total sigilo e confidencialidade no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ela relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados.

6 MONITORAÇÃO DOS DADOS PROCESSADOS E ARMAZENADOS EM NUVEM

6.1 A Contratada deverá fornecer, sempre que solicitado pela CAIXA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de APIs para análise de segurança e auditorias.

6.2 A trilha de auditoria deve conter, minimamente, itens descritos no item 1.23 deste documento.

6.3 O Provedor de Serviço em Nuvem, deve dispor de recurso que permita o gerenciamento centralizado de eventos e envio para a CAIXA, sempre que solicitado, de logs/informações de trilha.

6.4 Os registros do Provedor de Serviço em Nuvem deverão incluir ainda todos os acessos, incidentes e eventos cibernéticos, no ambiente do mesmo, pelo período 5 (cinco) anos.

7 SEGURANÇA DO TRÁFEGO DE DADOS COM A NUVEM

7.1 A comunicação entre a CAIXA e a Contratada deve suportar criptografia TLS, com autenticação mútua, na versão 1.3.

7.2 Caso a aplicação não suporte TLS 1.3, será admitida a compatibilidade para TLS 1.2.

7.3 A necessidade de TLS também se aplica a qualquer comunicação entre a Contratada e o Provedor de Serviços em Nuvem ou entre a CAIXA e o Provedor de Serviços em Nuvem, para todos os casos em que a Contratada e o Provedor forem entidades distintas.

7.4 O Provedor de Serviços em Nuvem deverá prover segurança relacionada ao tráfego de dados, provendo aplicações de firewall, IPS e CASB para garantir a segurança de todos os fluxos, sejam externos ou em trânsito com a CAIXA.

7.5 O Provedor de Serviços em Nuvem não deverá ter permissão de uso ou acesso direto ao ambiente de autenticação da CAIXA.

7.6 Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, com pelo menos uma cópia atualizada de segurança também no Brasil.

8 OUTROS CONTROLES DE SEGURANÇA NO AMBIENTE DA CONTRATADA DO SERVIÇO DE NUVEM

8.1 O Provedor de Serviços em Nuvem deve habilitar o registro completo do Hypervisor que suporta os serviços da CAIXA, e deve suportar o uso de máquinas virtuais (Trusted VM) fornecidas pela CAIXA, desde que estas máquinas estejam em conformidade com as políticas e práticas de segurança de rede exigidas pelo Provedor.

9 GESTÃO DE INCIDENTES DE SEGURANÇA

9.1 A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.

9.2 A Contratada deve realizar testes independentes de penetração/invasão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para a CAIXA. O escopo dos testes deve ser previamente combinado e aprovado pela CAIXA, dentro dos limites do contrato.

9.3 Os testes de penetração/invasão devem ter como escopo, rede, aplicação web, Application Programming Interface (API), serviços hospedados e; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; dentre outros.

9.4 Todos os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções a serem feitas, devem ser fornecidos à CAIXA sempre que solicitado.

9.5 A Contratada deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.

9.6 A contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.

9.7 O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou a CAIXA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA.

9.8 A Contratada deve ter um processo de notificação de incidentes 24x7.

9.9 A Contratada deve comunicar à CAIXA incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.

9.10 Os incidentes devem ser comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA, que opera 24x7, por meio do endereço de e-mail: abuse@caixa.gov.br. Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.

9.11 A Contratada deve comunicar à CAIXA, dentro do prazo acordado, todos os incidentes detectados que envolvam os serviços prestados, conforme a classificação abaixo:

Nível de severidade	Descrição do nível de severidade	Prazo Máximo
Severidade 1 (Crítica)	Eventos cujo contexto principal é a segurança cibernética, tais como: -Impacto em ativos ou serviços críticos de TI; -Violação significativa de dados sensíveis; -Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente. **Exemplos não exaustivos:** ataque de Ransomware, ataque de negação de serviço distribuído – DdoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.	2 horas após o início da ocorrência.
Severidade 2 (Alta)	Eventos cujo contexto principal é a segurança cibernética, tais como: -Impacto em ativos ou serviços de TI de alta criticidade; -Detecção de acesso não autorizado e/ou alterações em sistemas de informação; -Infecção persistente por código malicioso;-Intrusão persistente na rede; -Incidentes de segurança cibernética envolvendo dirigentes; -Ameaça significativa à disponibilidade e/ou integridade do ambiente; -Ameaça significativa à imagem da CAIXA. **Exemplos não exaustivos**: ataques de escalação de privilégio em servidores, ataques do tipo brute force e password spray.Dentre outros	4 horas após o início da ocorrência.

9.12 Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA.

9.13 A Contratada deve fornecer descrição detalhada dos incidentes, incluindo informações suficientes para classificá-los por nível de severidade, conforme a definição dos eventos. As informações sobre incidentes podem ser enriquecidas utilizado o modelo do MITRE ATT&CK®.

9.14 A contratada deve seguir preferencialmente o modelo de comunicação de ISCF – Incidente de Segurança Cibernética em Fornecedor, Anexo III A, que também contempla situações de incidentes de segurança com dados pessoais.

9.15 Vale ressaltar que em se tratando de contratos para tratamento de dados pessoais, nos termos da LGPD, a Contratada deve provar que tem capacidade de fornecer uma resposta organizada e eficaz a um incidente de privacidade. Neste sentido, a CAIXA desenvolverá e implementará juntamente com o fornecedor do serviço um plano de resposta a incidentes de privacidade, que inclua por exemplo, definição de incidente de privacidade e o escopo da resposta ao incidente, estabelecimento de equipes multifuncionais de resposta a incidente de privacidade, entre outros aspectos relevantes.

9.16 A Contratada deve documentar os casos de uso que são utilizados para realizar a configuração e o monitoramento de eventos, correlacionando tecnologias para tratar padrões / cenários de ataque comuns e avançados; e disponibilizar os casos de uso à CAIXA sempre que solicitado.

9.17 A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.

9.18 A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA deve ser considerada, observada a regulamentação em vigor, conforme art 3º, §4º da Res. BACEN 4.893/2021.

9.19 Se a Contratada precisar envolver outras partes externas para investigar e/ou resolver incidentes que afetem o escopo do objeto contratado, ela deve obter a anuência da CAIXA por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA.

10 CERTIFICADOS E RELATÓRIOS QUE COMPROVAM O CUMPRIMENTO DOS REQUERIMENTOS MÍNIMOS DE SEGURANÇA.

10.1 Para serviços de nuvem, caso a Contratada pela CAIXA e o Provedor de Serviços em Nuvem sejam empresas diferentes, a referida Contratada terá a responsabilidade de obter as documentações exigidas do Provedor, para apresentação à CAIXA.

10.2 Os documentos exigidos devem ter a sua primeira versão entregue antes da assinatura do contrato, e devem ser reiterados de acordo com a vigência indicada nos quadros abaixo. O Due Diligence presencial é facultativo e será feito a critério da CAIXA.

10.3 Caso o prazo de validade da certificação ainda esteja vigente com relação à última apresentação, não é necessária uma nova apresentação.

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da Contratada para verificar os requisitos de segurança presente nas cláusulas	A CAIXA, por iniciativa própria, fará due diligence presencial em função de discrepâncias identificadas em relatórios de auditoria entregues ou dúvidas onde apenas a documentação não seja suficiente.	A visita poderá ser realizada por equipe própria da CAIXA ou empresa designada pela CAIXA	SOB DEMANDA
Due Diligence Remoto	Constatar que os processos determinados pela CAIXA estão sendo seguidos, conforme descrito nas cláusulas	Documentos previstos nas cláusulas e demais comprovantes de seus requisitos. Quando não comprovados por certificação, os itens exigidos nas cláusulas devem ser certificados por empresa de auditoria independente.	Relatórios próprios da empresa para comprovação do atendimento aos itens das cláusulas, desde que ratificados por empresa de auditoria independente	SOB DEMANDA

10.4. CERTIFICAÇÕES APLICÁVEIS AOS FORNECEDORES DE SERVIÇOS EM NUVEM:

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
FIPS 140-2 Nível 2 para SaaS e PaaS e FIPS 140-2 nível 3 para IaaS	Garantir que o provedor tenha mecanismo seguro para proteção de chaves criptográficas que sustentem os seus processos	Certificação do NIST que atesta um nível elevado de segurança para o HSM	Apresentar certificado FIPS 140-2 para equipamento utilizado no Provedor de Serviços em Nuvem	ANUAL

Certificação SOC 2 – Tipos 1 e 2	Garantir acesso a uma avaliação independente, por meio de relatório de auditoria, sobre o ambiente de controle do provedor, relevante para a segurança, disponibilidade, confidencialidade e privacidade	SOC TYPE 2 Fornece relatórios com descrição do ambiente de controles do provedor e da auditoria externa dos controles que atendem aos princípios e critérios de segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA	Disponibilizar relatório de auditoria em nome do Provedor de Nuvem	ANUAL

11 ENCERRAMENTO DO CONTRATO

11.1 A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.

11.2 A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.

11.3 A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.

11.4 A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.

11.5 Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.

11.6 A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer aos padrões definidos no NIST SP 800-88 Guidelines for Media Sanitization, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.

11.7 Caso a Contratada tenha ativo de informação no fim do ciclo de vida, ou considerado inservível, este ativo deverá ser destruído, com o fornecimento do Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction – CEED), discriminando os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição.

12 NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS

12.1 O não cumprimento, pela Contratada, de qualquer um dos seguintes requisitos de segurança, definidos neste instrumento contratual, ensejará a aplicação das penalidades previstas neste contrato e poderá, a critério da Contratante, ensejar a rescisão imediata do contrato, sem prejuízo de outras medidas cabíveis:

a) Não fornecer evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões de acesso realizadas;
b) Não comunicar ocorrências de intrusão real;
c) Não fornecer relatório mensal sobre as tentativas de intrusão;
d) Não fornecer o planejamento de correção de vulnerabilidades;
e) Não fornecer os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções;
f) Não fornecer os relatórios de incidentes conforme SLA;
g) Não prestar as informações e relatórios solicitados pela CAIXA;
h) Não fornecer relatório indicando conformidade com o NIST SP 800-88.
i) Não atender a convocação da CAIXA para Due Diligence presencial ou remoto;
j) Não fornecer a documentação solicitada em decorrência do Due Diligence presencial ou remoto, conforme prazo acordado entre as partes;
k) Não fornecer os relatórios de auditoria externa independente, para as empresas que não possuem a certificação SOC2;
l) Não fornecer certificação SOC2;
m) Não fornecer certificação FIPS 140-2 Nível 3 ou FIPS 140-2 nível 2.

ANEXO II

DECLARAÇÃO DE VEDAÇÃO AO NEPOTISMO E IMPEDIMENTOS

A Contratada DECLARA, sob as penas da Lei, que:

1. Não está com o direito de licitar e contratar com a CAIXA suspenso, ou impedida de licitar e contratar com a União, ou que não tenha sido declarada inidônea para licitar ou contratar com a União, enquanto perdurarem os efeitos da sanção;
2. Não é constituída por administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social que seja dirigente ou empregado da CAIXA;
3. Não é constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;
4. Não tem administrador que seja sócio de empresa suspensa, impedida ou declarada inidônea;
5. Não é constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
6. Não tenha administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
7. Não há nos seus quadros de diretoria pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea;
8. Não é empregado ou dirigente CAIXA na condição de licitante;
9. Não possui relação de parentesco, até o terceiro grau civil, com:
   a) Dirigente da CAIXA;
   b) Empregado da CAIXA cujas atribuições envolvam a atuação na área responsável pela licitação, contratação ou pela gestão operacional do contrato e pela autoridade da CAIXA hierarquicamente superior as áreas mencionadas;
   c) Autoridade do ente público a que a CAIXA esteja vinculada.
10. Não é proprietário, mesmo na condição de sócio, de empresa que tenha terminado seu prazo de gestão ou rompido seu vínculo com a CAIXA há menos de 6 (seis) meses.

Brasília, 08 de dezembro de 2025

Luiz Chaves Soares
CPF:100.406.118-84
10-dez-2025 | 12:56 BRT

Ricardo Fraga Moreira Miragaia
CPF:100.406.118-84
10-dez-2025 | 07:54 PST

OBVIO BRASIL SOFTWARE E SERVIÇOS S/A

ANEXO III

CÓDIGO DE CONDUTA DO FORNECEDOR CAIXA

1 OBJETIVO

1.1 Este Código estabelece premissas norteadoras de comportamento que devem ser observadas pelo fornecedor, com o objetivo de orientá-lo para uma conduta pautada por elevados padrões de ética e integridade, capaz de assegurar relações sustentáveis, compatíveis com a legislação, o interesse público e as aspirações da sociedade.

1.2 Deverá o fornecedor influenciar positiva e proativamente os demais envolvidos na cadeia produtiva, estendendo essa mesma conduta para as partes com quem se relaciona comercial e contratualmente, em especial, fornecedores e prestadores de serviços.

1.3 As condutas levam em consideração não somente o legal e o ilegal, o justo e o injusto, o conveniente e o inconveniente, o oportuno e o inoportuno, mas principalmente o honesto e o desonesto, bem como o sustentável, tendo como fim o bem comum.

1.4 Este Código de Conduta poderá ser alterado pela CAIXA dentro dos parâmetros legais e, consequentemente, as alterações terão de ser acompanhadas e seguidas pelo Fornecedor.

2 PADRÕES GERAIS DE CONDUTA

2.1 Este Código de Conduta vincula o Fornecedor da CAIXA a assumir os seguintes compromissos:

2.1.1 Adotar medidas necessárias e efetivas para combater a corrupção e a fraude em todas as instâncias, prevenindo a ocorrência de qualquer tipo de comportamento ilegal.

2.1.2 Adotar as melhores práticas e comportamento ético no exercício das atribuições profissionais ou fora dele, atuando com dignidade, decoro, zelo, eficácia e consciência dos princípios morais, condutas que também devem ser repassadas para toda a sua cadeia de fornecedores.

2.1.3 Tomar conhecimento dos termos da Lei nº 12.846/2013 e de suas regulamentações, reconhecendo sua responsabilidade objetiva pelos atos praticados em seu interesse ou benefício, por qualquer pessoa que o represente.

2.1.4 Adotar mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica, nos termos do § 2º do art. 8º, do Decreto nº 11.129/2022, que regulamentou a Lei 12.846/2013.

2.1.5 Adotar mecanismos, procedimentos internos, capacitação e sensibilização para a adoção e incorporação de critérios e práticas de sustentabilidade na oferta de produtos e serviços, nos termos do Decreto nº 7.746/2012, que regulamenta o artigo 3º da Lei nº 8.666/1993.

2.1.6 Cumprir e fazer cumprir as determinações da legislação ambiental e climática vigente, bem como atuar na prevenção de impactos ambientais e climáticos gerados por seus processos, produtos e serviços e na mitigação, correção ou compensação, quando identificados.

2.1.7 Adotar e estimular a ecoeficiência em seus processos, produtos e serviços, realizando continuamente revisão e aplicação de melhorias, de forma a contribuir para processos eficientes e que gerem menor impacto ao meio ambiente, tais como a redução, reutilização, reciclagem, destinação adequada de resíduos, a implementação de uma política de aquisição de bens cujos materiais sejam atóxicos ou biodegradáveis e a adoção, sempre que possível, de sistemas de logística inversa e reversa, mediante retorno dos produtos após o uso pelo consumidor.

2.1.8 Participar de iniciativas de engajamento em mudanças climáticas e/ou segurança hídrica, quando convidado pela CAIXA.

2.1.9 Adotar a legislação trabalhista vigente, bem como medidas que visem à observância de direitos humanos, tais como a equidade de gênero, o combate ao racismo e a acessibilidade, conforme legislações pertinentes.

2.1.10 Promover ações de sensibilização de seus colaboradores sobre a temática combate à discriminação no trabalho (sexo, raça, cor, deficiência, orientação sexual, partido político, religião, credo, nacionalidade e quaisquer outras formas de discriminação) e a não utilização de práticas de assédio moral ou sexual e os mecanismos para evitá-la com a construção de uma cultura institucional de enfrentamento à discriminação.

2.1.11 Adotar medidas e ações para mitigar, corrigir, prevenir ou compensar danos/impactos relacionados à saúde e segurança de seus funcionários em decorrência das atividades da empresa.

2.1.12 Não utilizar ou contratar fornecedor que utilize mão-de-obra infantil ou trabalho degradante ou análogo ao escravo, conforme previsão em legislação.

2.1.13 Realizar o engajamento e o incentivo a boas práticas socioambientais de seus funcionários, clientes, fornecedores e demais stakeholders.

2.1.14 Adotar em seu processo produtivo ações que contribuam para a redução da geração de resíduos tóxicos e gases de efeito estufa bem como, aquelas que privilegiem a produção local, incentivando o desenvolvimento local e contribuindo para a redução dos custos de transporte, uso de combustíveis fósseis, emissão de gases de efeito estufa.

2.1.15 Quando solicitado pela CAIXA, responder a pesquisa implementada pelo CDP – *CARBON DISCLOSURE PROJECT*, que trata sobre mudanças climáticas e segurança hídrica ou outra que vier a substitui-la futuramente.

2.1.16 Promover a disseminação da política do Jogo Responsável, que consiste na adoção de diretrizes e práticas voltadas para a prevenção do jogo compulsivo e proteção de pessoas vulneráveis — como menores de idade —, assim como de potenciais transtornos de jogo eventualmente associados a apostas.

2.1.17 De maneira a disseminar o conhecimento sobre o tema Jogo Responsável, divulgar o site www.jogoresponsavel.com.br e incentivar o acesso por seus colaboradores, clientes, fornecedores e demais partes interessadas — *stakeholders* —, contribuindo para a expansão da educação dos apostadores das Loterias Federais considerando as melhores práticas mundiais do Jogo Responsável.

2.2 As violações a este Código de Conduta serão submetidas à avaliação da área responsável na CAIXA, que deliberará sobre o encaminhamento da ocorrência para abertura de Processo Administrativo de Responsabilização - PAR.

3 PADRÕES ESPECÍFICOS DE CONDUTA

3.1 A Pessoa Jurídica, na pessoa dos seus representantes, e todo o seu corpo funcional se comprometem a combater quaisquer práticas lesivas à Administração Pública, tais como:

3.1.1 Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada.

3.1.2 Financiar, custear, patrocinar ou de qualquer modo subvencionar a prática de atos de corrupção e+ fraudes.

3.1.3 Utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados.

3.1.4 Frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público.

3.1.5 Impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público.

3.1.6 Afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo.

3.1.7 Fraudar licitação pública ou contrato dela decorrente.

3.1.8 Criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo.

3.1.9 Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais.

3.1.10 Manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

3.1.11 Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação.

3.2 Se comprometem, ainda, em observância à Lei nº 12.846/13 e regulamentações a adotar as seguintes ações:

3.2.1 Diligenciar para que todos os seus colaboradores e representantes conheçam e cumpram este Código.

3.2.2 Informar imediatamente à CAIXA, caso venha a tomar conhecimento de qualquer indício de violação a este Código ou às leis pertinentes.

3.2.3 Caso tenha conhecimento, identificar e discriminar pessoas que estejam agindo em seu nome, ou por sua conta e ordem, que prometeu, deu ou ofereceu, direta ou indiretamente, vantagem ou promessa de vantagem a qualquer agente público, ou esteve envolvido na prática de atos ilícitos referentes a crimes contra a administração pública.

3.2.4 Adotar mecanismos e procedimentos para a prevenção dos crimes de lavagem de dinheiro em sintonia com a pertinente legislação, em especial, a Lei 9.613/98, bem como, dar conhecimento tempestivo à CAIXA de delitos da espécie consumados ou tentados que a ela se relacionem.

3.2.5 Combater qualquer iniciativa que vá de encontro à livre concorrência, inclusive as indutoras à formação de cartel.

3.2.6 Proteger a reputação da CAIXA, resguardando-a de ações e atitudes inadequadas que comprometam a sua imagem, praticadas direta ou indiretamente por pessoas que estejam agindo em nome da Pessoa Jurídica ou por sua conta.

3.3 A Pessoa Jurídica buscará adotar Código de Ética próprio, a fim de priorizar e sistematizar os seguintes Valores em sua governança corporativa:

3.3.1 Respeito - As pessoas são tratadas com ética, justiça, respeito, cortesia, igualdade e dignidade, sendo exigido de dirigentes, empregados e parceiros absoluto respeito pelo ser humano, pelo bem público, pela sociedade e pelo meio ambiente.

3.3.2 Honestidade – Os negócios são geridos com honestidade, estando o interesse público em 1º lugar, em detrimento de interesses pessoais, de grupos ou de terceiros.

3.3.3 Compromisso - Os dirigentes, empregados e parceiros estão comprometidos com o mais elevado padrão ético no exercício de suas atribuições profissionais, com o cumprimento das leis, das normas e dos regulamentos internos e externos que regem a empresa.

3.3.4 Transparência - Aos clientes, parceiros comerciais, fornecedores e à mídia é dispensado tratamento equânime na disponibilidade de informações claras e tempestivas, por meio de fontes autorizadas e no estrito cumprimento da legislação aplicável.

3.3.5 Responsabilidade – as ações são pautadas nos preceitos e valores éticos deste Código, de forma a eliminar ações e atitudes corruptivas, bem como proteger o patrimônio público, com a adequada utilização das informações, dos bens e demais recursos colocados à disposição para a gestão eficaz dos negócios, garantindo proteção a quem denunciar as violações a este Código.

3.3.6 Responsabilidade social, ambiental e climática – forma de gestão e realização de negócios de uma empresa, que incorpora considerações sociais (respeito, proteção, promoção de direitos e garantias fundamentais e de interesse comum), ambientais (preservação e reparação do meio ambiente, incluindo sua recuperação) e climáticas (contribuições institucionais para uma economia de baixo carbono - redução/compensação - e redução dos impactos ocasionados por intempéries e alterações ambientais de longo prazo) em seus processos decisórios, bem como a responsabilidade pelos impactos de suas decisões e atividades na sociedade e no meio ambiente;

TERMO DE RECEBIMENTO, CIÊNCIA E ADESÃO AO CÓDIGO DE CONDUTA DO FORNECEDOR CAIXA

OBVIO BRASIL SOFTWARE E SERVIÇOS S/A, inscrita no CNPJ(MF) sob o nº 13.114.403/0001-03, com sede na Praça General Gentil Falcão, 108, 16°andar, Cidade Monções, 04571-150 - São Paulo – SP, DECLARA, sob as penas da lei, para fins de formalização de contratação com a CAIXA, que:

1. Recebeu / foi disponibilizada cópia integral do Código de Conduta do Fornecedor CAIXA;

2. Tomou conhecimento de todos os seus termos e se compromete a cumpri-los integralmente;

3. Compartilhará as condutas contidas neste Código com seus empregados, sua respectiva cadeia produtiva e seus subcontratados, quando for o caso;

4. Não tem conhecimento de qualquer violação ou indício de violação a este Código ou à legislação anticorrupção;

5. Se compromete a informar à CAIXA caso venha a tomar conhecimento de qualquer violação ou indício de violação a este Código ou à legislação anticorrupção;

6. Tem conhecimento de que a manutenção da relação contratual com a CAIXA implica na concordância em seguir este Código e suas eventuais alterações, aditamentos ou revisões futuras;

7. Se compromete em acessar o endereço eletrônico www.licitacoes.caixa.gov.br, para manter-se atualizado em razão de possíveis alterações neste Código de Conduta.

Brasília, 08 de dezembro de 2025

Luiz Chaves Soares
CPF:100.406.118-84
10-dez-2025 | 12:56 BRT

Ricardo Fraga Moreira Miragaia
CPF:100.406.118-84
10-dez-2025 | 07:54 PST

OBVIO BRASIL SOFTWARE E SERVIÇOS S/A