

ANEXO I**TERMO DE REFERÊNCIA PARA ESCRITURADOR DE AÇÕES****1. OBJETO**

Prestação de serviço de escrituração das ações da Caixa Seguridade Participações S.A., a ser realizado em todo território nacional.

2. ESPECIFICAÇÃO DO OBJETO

- 2.1 A prestação dos serviços deverá ser realizada por Instituição Financeira (“CONTRATADA”), autorizada pela Comissão de Valores Mobiliários (“CVM”) para a prestação de serviço de escrituração de ações, nos termos da Resolução CVM nº 33 de 19 de maio de 2021 (“RCVM 33”) e suas respectivas alterações posteriores.
- 2.2 A CONTRATADA deverá comprovar conformidade com o artigo 38 da Lei nº 13.303 de 30 de junho de 2016 e estar ciente e observar as REGRAS DE CONDUTA previstas no Capítulo V - Art. 21 da RCVM 33.
- 2.3 A escrituração dos valores mobiliários deverá ser realizada em sistemas informatizados adequados e seguros (“SISTEMA”) que permitam o registro, processamento e controle das informações relativas à titularidade individualizada dos valores mobiliários escriturados e com todas as formalidades exigidas.
- 2.4 Para apoiar a Caixa Seguridade Participações S.A. (“CAIXA Seguridade”, “EMISSOR”, “CONTRATANTE” ou “COMPANHIA”) em sua gestão interna e no cumprimento das normas regulamentares, a CONTRATADA deverá responder às consultas do EMISSOR relacionadas aos serviços contratados e, de forma periódica, disponibilizar informações preferencialmente por meio de acesso ao sistema eletrônico.
- 2.5 Competirá à CONTRATADA a operacionalização dos processos de escrituração, registro dos livros e documentos, pagamentos devidos aos acionistas, conforme disposto na RCVM 33, sendo o rol a seguir exemplificativo e não exaustivo:

2.6 DA ESCRITURAÇÃO E REGISTRO

- 2.6.1 Operacionalizar os processos de escrituração, registro dos livros e documentos, e transferência de titularidade das ações;
- 2.6.2 Registrar eletronicamente a propriedade das ações, vínculos e averbações;
- 2.6.3 Acompanhar e atender às solicitações judiciais referentes à formação de vínculos e averbações sobre valores mobiliários de emissão do EMISSOR;
- 2.6.4 Atualizar e manter o cadastro dos acionistas; e
- 2.6.5 Inserir as informações relativas à titularidade dos valores mobiliários em contas de valores mobiliários individualizadas, abertas em nome de cada titular de valor mobiliário.

2.7 DOS PROVENTOS E DEMAIS DELIBERAÇÕES SOCIETÁRIAS

- 2.7.1 Executar as deliberações societárias, incluindo, mas não se limitando, ao pagamento de dividendos e juros sobre capital próprio (JCP), bonificações, desdobramentos, grupamentos, cancelamentos, entre outros;
- 2.7.2 Realizar o cálculo das repercussões econômicas decorrentes de eventos societários deliberados pela CAIXA Seguridade e emitir relatórios gerenciais e legais relacionados;

- 2.7.3 Disponibilizar o cálculo dos valores a serem pagos aos acionistas e o valor do imposto de renda a ser recolhido, em até 4 (quatro) dias úteis antes do pagamento do evento societário deliberado aos acionistas;
- 2.7.4 Configurar parâmetros e efetuar o pagamento de proventos, e demais eventos societários deliberados, por meio de crédito bancário, conforme o domicílio bancário informado no cadastro de acionistas;
 - 2.7.4.1 Especificamente no que se refere ao pagamento de créditos aos acionistas, a CONTRATADA deverá liquidar as operações em até 01 (um) dia útil após a disponibilização dos recursos pela CONTRATANTE;
 - 2.7.4.2 Os recursos serão disponibilizados pela CONTRATANTE em conta corrente bancária para débito pela CONTRATADA;
 - 2.7.4.3 Comunicar em até 4 (quatro) dias úteis antes do pagamento dos eventos societários deliberados aos acionistas eventuais alterações dos dados da conta corrente da CONTRATADA;
- 2.7.5 Prescrever valores não reclamados conforme Lei nº 6.404 de 15 de dezembro de 1976 e emitir relatório de valores prescritos;
- 2.7.6 Analisar documentos de isenção fiscal e emitir informes de rendimento e arquivos de IRRF;
- 2.7.7 Executar serviços de subscrição;
 - 2.7.7.1 Controlar todas as etapas do processo de subscrição de ações (cálculo, emissão de boletins, integralização) e atender os acionistas para registro do seu exercício;
 - 2.7.7.2 Realizar conversão e desmembramento de ações em Units, quando aplicável; e
- 2.7.8 Processar demais deliberações modificativas/extintivas do capital social (fusão, incorporação, cisão, grupamento etc.).

2.8 DOS RELATÓRIOS

- 2.8.1 A CONTRATADA deverá disponibilizar à CONTRATANTE, no mínimo, por meio de sistema, as seguintes informações:
 - a. Relação diária dos titulares dos valores mobiliários emitidos pela CONTRATANTE, refletindo a posição total, com abertura analítica das posições dos investidores mantidas sob a titularidade fiduciária da central depositária;
 - b. Informações por investidor: identificação, qualificação, natureza jurídica, regime tributário do titular do valor mobiliário, cadastros, saldos, averbações, movimentações (inclusive detalhamento de datas, origem/destino dos ativos) e pagamentos;
 - c. Base acionária completa com várias possibilidades de seleção (exemplos: por opção de crédito, por domicílio, por Estado, por País, por tipo de pessoa - Física ou Jurídica) e possibilidade de *download* em formato texto ou *Excel* (incluindo datas retroativas);
 - d. Relatório de cálculos dos valores de créditos a que têm direito os titulares das ações;
 - e. Relatório de pagamentos por período e por benefício;
 - f. Relatórios para conciliação financeira e contábil dos pagamentos de benefícios;

- g. Relação do total dos valores bruto, líquido e do imposto de renda retido na fonte pelo EMISSOR, relativos ao pagamento dos créditos, de acordo com a periodicidade e dados exigidos pela legislação tributária;
 - h. Relação diária dos titulares das ações e dos valores bruto, líquido e do imposto de renda retido na fonte relativos ao pagamento de operações;
 - i. Detalhamento dos atos societários e evolução de saldos pagos e a pagar por tipo de ação;
 - j. Relatório contendo as transferências de titularidade ocorridas nas contas de valores mobiliários;
 - k. Relação dos direitos reais de fruição ou de garantia, assim como outros gravames incidentes sobre os valores mobiliários, com indicação de suas causas diretas e seu prazo de vigência, assim como outros gravames incidentes sobre os valores mobiliários;
 - l. Demonstrativo de subscrições em andamento;
 - m. Mapas analítico e sintético consolidando as informações de instruções de voto à distância encaminhadas pelos acionistas conforme os prazos previstos na legislação vigente;
 - n. Relação de quem tenha exercido direitos relativos a eventos incidentes sobre os valores mobiliários;
 - o. Relatório dos cálculos e pagamentos de proventos efetuados; e
 - p. Apresentação de relatório anual que assegure o cumprimento e efetividade dos controles internos em relação a cadastro de acionistas.
 - q. Relatório com os dados necessários para viabilizar o recolhimento do imposto de renda retido na fonte pelo EMISSOR.
- 2.8.1.1 Os relatórios das alíneas b, c e g devem disponibilizados até 5 (cinco) dias úteis após o pagamento dos dividendos e/ou atualização monetária.
- 2.8.1.2 O relatório da alínea “q” deve ser disponibilizado até 4 (quatro) dias úteis antes do pagamento dos dividendos e/ou atualização monetária.
- 2.8.2 A CONTRATADA colocará à disposição dos titulares das ações extratos, informes, avisos e boletins, na periodicidade exigida pela legislação societária, legislação fiscal, e conforme tenham sido deliberados pagamentos de direitos, conforme os exemplos não exaustivos:
- a. Extrato da conta de cada titular das ações sempre que houver movimentação, até o 10º (décimo) dia do mês seguinte ao término do mês em que ocorrer movimentação;
 - b. Extrato das contas de valores mobiliários, quando solicitado, no prazo de 2 (dois) dias úteis da solicitação, desde que referentes ao ano corrente;
 - c. Informes sobre o saldo existente ao final do ano anterior, até o final do mês de fevereiro do ano subsequente;
 - d. Aviso de pagamento de direitos;
 - e. Boletins para exercício de direitos de subscrição;

- f. Informes de recebimento de créditos e posição acionária para fins de declaração de imposto de renda ("INFORMATIVO DE RENDIMENTO");
- g. Informes relativos aos eventos incidentes sobre as ações, sempre que solicitado; e
- h. Informes referentes às medidas necessárias para o pagamento de proventos deliberados e pagos pelo EMISSOR, quando o investidor não possuir as informações cadastrais atualizadas.

2.9 DO ATENDIMENTO

- 2.9.1 A CONTRATADA deverá disponibilizar canais para atendimento aos acionistas, quais sejam: meios digitais, central de atendimento telefônico e/ou, preferencialmente, atendimento presencial.
- 2.9.2 A CONTRATADA deverá disponibilizar os serviços aos acionistas previstos neste contrato por meio de site na internet, preferencialmente em regime 24 X 7 (vinte e quatro horas por dia, sete dias por semana), sendo aceitável a disponibilidade mínima de segunda à sexta, das 06h00 às 00h00, e sábados e domingos, das 09h00 às 18h00, além da ferramenta de atendimento pela internet.
- 2.9.3 A CONTRATADA deverá ainda:
- a. Atender acionistas dispondo de funcionários treinados e capacitados;
 - b. Atender corretoras e processar movimentações de bolsa via custódia fiduciária; e
 - c. Atender órgãos reguladores e demandas judiciais.
 - d. A CONTRATADA deverá aferir e apresentar, indicador de desempenho – SLA semestralmente, através de relatório contendo todos os chamados técnicos relacionados ao portal e aos serviços prestados aos acionistas, com informações de: número do chamado, descrição, defeito, solução aplicada, datas e horários de abertura e encerramento, existência de reabertura, criticidade, solicitante e tempo total decorrido, observando os seguintes critérios mínimos de qualidade:

Nível de Criticidade	Ocorrência	Tempo Máximo de Conclusão do Atendimento	Índice de Chamados Atendidos no Prazo
1 - Prioridade Alta	Indisponibilidade total do serviço	2 (duas) horas	95%
2 - Prioridade Média	Degradação parcial do serviço (módulos ou componentes críticos)	6 (seis) horas	95%
3 - Prioridade Baixa	Erros não críticos, divergências de funcionamento ou questionamentos/demandas dos acionistas	2 (dois) dias	95%

2.10 DAS CORRESPONDÊNCIAS E INFORMES

- 2.10.1 Expedir correspondências aos acionistas, conforme exigido pela legislação societária (a exemplo de extratos); legislação fiscal (a exemplo de informes de rendimentos); e conforme tenham sido deliberados pagamentos de direitos (a exemplo de avisos de crédito e boletins para exercício de direitos de subscrição).

2.11 DO VOTO À DISTÂNCIA

- 2.11.1 A CONTRATADA deve atender as exigências da Resolução CVM 81 de 11 de agosto de 2022 (“RCVM 81”) e suas alterações posteriores.
- 2.11.1.1 A RCVM 81 dispõe sobre informações, pedidos públicos de procuração, participação e votação à distância em assembleias de acionistas, e atribui responsabilidades à prestação de serviço de escrituração de ações, às quais devem ser integralmente atendidas.
- 2.11.1.2 A CONTRATADA, no que lhe compete a regra, deve fazer a gestão de eventos ordinários e extraordinários, presenciais ou à distância, com mecanismos que instruem e possibilitem o voto à distância por parte dos acionistas, procedam o registro de livros decorrentes e cumpram demais atribuições que garantam sua execução segundo o regramento.
- 2.11.2 Receber e tratar as instruções de preenchimento de Boletim de Voto à Distância nas assembleias gerais de acionistas em que for facultado o voto à distância.
- 2.11.3 Consolidar votos recebidos e gerar mapas analíticos e sintéticos.
- 2.11.4 Disponibilizar à CONTRATANTE os mapas analíticos e sintéticos de votos à distância conforme RCVM 81, bem como quaisquer outros relatórios, informações ou documentos exigidos pela legislação vigente e pelas normas regulamentares aplicáveis.

2.12 DO SISTEMA

- 2.12.1 Disponibilizar SISTEMA web seguro (https), com seu acesso protegido por usuário e senha pessoal, compatível com navegadores descritos no item 2.12.4.
- 2.12.2 O SISTEMA deve possuir interface web, com acesso via internet por meio de conexão criptografada (https), de forma que não sejam necessárias instalações ou configurações locais específicas;
- 2.12.3 Deve ainda permitir integração com outros sistemas através da exportação de dados estruturados e gerar relatórios customizáveis;
- 2.12.4 A solução deverá ser compatível no mínimo com os navegadores web a seguir:
- Microsoft Edge versão 140 ou superior;
 - Mozilla Firefox 128 ou superior;
 - Google Chrome 137 ou superior; ou
 - Safari 18 ou superior.
- 2.12.5 Mantê-lo com disponibilidade integral, exceto janelas de manutenção previamente comunicadas com antecedência mínima de 72 (setenta e duas) horas; e
- 2.12.6 Garantir a liberação de acesso às pessoas autorizadas pela CONTRANTE em até 24 horas das solicitações recebidas.

2.13 DA MIGRAÇÃO E ENCERRAMENTO

- 2.13.1 Realizar migração, se aplicável, do histórico da base acionária, inclusive registros incompletos, para o SISTEMA utilizado, garantindo a integridade dos dados;
- 2.13.2 A Companhia poderá determinar que essas informações sejam repassadas diretamente à CONTRATADA pelo Banco Escriturador anterior.
- 2.13.2.1 Transferir os registros ao novo prestador, em caso de encerramento do contrato, independentemente da causa; e

2.13.3 Comunicar à CVM, até o 5º dia útil do mês subsequente, a celebração e extinção do contrato de escrituração, conforme previsto no Art. 12 da RCVM 33.

3. OBRIGAÇÕES LEGAIS E NORMATIVAS

3.1 A prestação de serviço de escriturador de ações, realizado pela CONTRATADA devidamente autorizada pela CVM, deve se amparar na:

- a. Resolução CVM nº 33/2021 – Dispõe sobre a prestação de serviços de escrituração de valores mobiliários e de emissão de certificados de valores mobiliários. Estabelece que o serviço deve ser prestado por instituições financeiras autorizadas pela CVM, com sistemas informatizados adequados, capacidade técnico-operacional e canais de atendimento aos titulares dos valores mobiliários;
- b. Resolução CVM nº 81/2022 – Consolida regras sobre assembleias de acionistas, incluindo disposições sobre participação e votação à distância, boletins de voto e registro de instruções. Traz obrigações específicas para escrituradores quanto à guarda e disponibilização de documentos relacionados às assembleias, como boletins de voto a distância, por prazo mínimo de 5 anos;
- c. Resolução CVM nº 80/2022 – Dispõe sobre o registro e a prestação de informações periódicas e eventuais dos emissores de valores mobiliários admitidos à negociação em mercados regulamentados de valores mobiliários;
- d. Lei n. 13.303, de 30 de junho de 2016 – Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- e. Lei n. 6.404, de 15 de dezembro de 1976 – Dispõe sobre as Sociedades por Ações. Com destaque aos artigos 100 e 101 que tratam do registro e manutenção do cadastro dos acionistas para fins de controle da titularidade e da movimentação dos valores mobiliários emitidos pela Companhia;
- f. Regulamento de Emissores B3 – Brasil, Bolsa, Balcão – Dispõe sobre regras e procedimento a serem seguidos por emissores de valores mobiliários.
- g. Instrução Normativa nº 2.043/2021 – Dispõe sobre a obrigação acessória EFD Reinf, estabelece os prazos de envio, bem como prevê as multas em caso de descumprimento;
- h. Lei nº 15.270/2025 – Dispõe sobre a instituição da retenção de IR sobre a distribuição de lucros e dividendos que excederem o montante de R\$ 50.000,00 mensais a partir do exercício de 2026, especificamente, para Pessoas Físicas residentes no Brasil e Pessoas Físicas ou Jurídicas residentes no exterior, essas últimas independentemente do valor;
- i. Lei nº 13.709, de 14 de agosto de 2018 - conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, com o objetivo de proteger a privacidade e os direitos fundamentais dos cidadãos;
- j. Resolução CVM nº 50, de 31 de agosto de 2021 – Dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa – PLD/FTP no âmbito do mercado de valores mobiliários; e

- k. Lei nº 13.810, de 08 de março de 2019 - Dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas;
- l. Instrução Normativa RFB nº 2.004, de 18 de janeiro de 2021 – Dispõe sobre a Escrituração Contábil Fiscal (ECF), estabelece os prazos de envio, bem como prevê as multas em caso de descumprimento, e
- m. Instrução Normativa RFB nº 698, de 20 de dezembro de 2006 - Estabelece normas para emissão de comprovantes de rendimentos pagos ou creditados a pessoas físicas e jurídicas decorrentes de aplicações financeiras, e disponibiliza o modelo de Informe de Rendimentos Financeiros.

3.2 A CONTRATADA deverá observar o disposto no Capítulo V - Art. 21 da RCVM 33, que trata sobre as REGRAS DE CONDUTA:

I – Exercer suas atividades com boa fé, diligência e lealdade em relação aos interesses dos emissores e dos titulares de valores mobiliários, sendo vedado privilegiar seus próprios interesses ou de pessoas a ele vinculadas;

II – Manter contas de valores mobiliários individualizadas em nome dos titulares do valor mobiliário;

III – Assegurar que os registros relativos às transferências e constituições de direitos, de fruição ou de garantia, assim como outros gravames sobre os valores mobiliários escriturados sejam feitos no menor prazo possível e que estejam amparados em documentos juridicamente válidos;

IV – Efetuar, no menor prazo possível e sem prejuízo da segurança necessária, as transferências, inscrições e averbações nas contas de valores mobiliários no depósito centralizado, sendo que, quando se tratar de transferência para conta de mesma titularidade, esta deve ser efetuada no prazo máximo de 7 (sete) dias úteis contados do recebimento da documentação completa do cliente;

V – Tomar todas as medidas cabíveis para o pagamento de proventos deliberados e pagos pelo EMISSOR, quando o titular do valor mobiliário não possuir informações cadastrais atualizadas;

VI – Responder pela legitimidade e pela veracidade dos registros das movimentações efetuadas e da titularidade dos valores mobiliários;

VII – Registrar nas contas de valores mobiliários as modificações dos valores mobiliários, após recebimento de instrução do CONTRATANTE que comunique os eventos sobre eles incidentes;

VIII – Praticar os atos de sua responsabilidade envolvidos com o repasse aos investidores e aos depositários centrais dos valores devidos por força de eventos incidentes sobre os valores mobiliários;

IX – Repassar ao CONTRATANTE os valores previamente recebidos dos investidores, relativos ao exercício de direitos de subscrição e conversões, entre outros;

X – Registrar os direitos de fruição ou de garantia, assim como outros gravames sobre os valores mobiliários, quando solicitado pelos respectivos titulares, diretamente ou por meio de seus representantes, nos termos da regulação pertinente, ou por determinação judicial, quando for o caso;

XI – Manter à disposição da CVM os registros que compõem a escrituração das contas de valores mobiliários, bem como os documentos que a eles se refiram;

XII – Adotar regras, procedimentos e controles internos que assegurem a fiscalização posterior das posições mantidas nas contas de valores mobiliários;

XIII – Garantir a segurança, eficiência e confiabilidade operacional dos sistemas de escrituração das contas de valores mobiliários;

XIV – Prevenir, controlar e corrigir irregularidades nos registros dos valores mobiliários;

XV – Adotar os procedimentos necessários ao cumprimento de solicitações dos custodiantes para a realização de depósito de valores mobiliários escriturais junto a depositário central;

XVI – Criar mecanismos a fim de assegurar a completa segregação de atividades e o sigilo sobre as posições detidas; e

XVII – Divulgar, na sua página na rede mundial de computadores, os documentos necessários para a realização da transferência a que se refere o inciso IV.

4. SEGURANÇA FÍSICA, CIBERNÉTICA E DA INFORMAÇÃO

- 4.1. Todos os documentos e informações que a contratada tenha acesso e que venha a produzir serão de propriedade da CONTRATANTE, não podendo ser utilizados, repassados, copiados ou alterados sem sua expressa autorização.
- 4.2. A CONTRATADA compromete-se a garantir e manter o sigilo sobre todas e quaisquer informações técnicas e institucionais a que tiver conhecimento, podendo somente divulgá-las com a prévia autorização por escrito da CONTRATANTE, condição que deverá ser observada mesmo após o término da contratação.
- 4.3. Todos os colaboradores da CONTRATADA envolvidos na prestação dos serviços deverão assinar o termo de confidencialidade anexo ao contrato.
- 4.4. A CONTRATADA deve providenciar a assinatura do Termo de Adesão de Pessoas Externas à Companhia à Política de Negociação de Valores Mobiliários da Caixa Seguridade Participações S.A., disponível no site Relações com Investidores da Companhia (<https://www.ri.caixaseguridade.com.br/governanca-corporativa/estatuto-politicas-e-codigos/>), tendo em vista o acesso durante a execução dos serviços contratados, de forma permanente e/ou eventual, à Informação Privilegiada.
- 4.5. A contratação e o acompanhamento contratual observarão os princípios da DISPONIBILIDADE, CONFIDENCIALIDADE e AUTENTICIDADE de acordo com a Política de Segurança da Informação da Caixa Seguridade Participações S.A., disponível no site: <https://www.ri.caixaseguridade.com.br/governanca-corporativa/estatuto-politicas-e-codigos/>.
- 4.6. Garantir a proteção dos dados pessoais e realizar a prestação do serviço em conformidade à Política de Segurança da Informação da Caixa Seguridade (disponibilizada no endereço <https://www.ri.caixaseguridade.com.br/governanca-corporativa/estatuto-politicas-e-codigos/>) e à Lei Geral de Proteção de Dados – LGPD.
- 4.7. Enviar, anualmente, declaração de conformidade quanto à identificação diária de acionistas potencialmente sujeitos a bloqueio de ativos, em observância às disposições da Lei nº 13.810, de 8 de março de 2019.

5. CLÁUSULAS DE PRIVACIDADE E SEGURANÇA DAS INFORMAÇÕES E CIBERNÉTICA

- 5.1 A CONTRATADA deverá observar o GUIA DE DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA incluídos no Apêndice A deste Termo de Referência.

5.2. A CONTRATADA deverá ainda observar o GUIA DE DIRETRIZES GERAIS DE SEGURANÇA DAS INFORMAÇÕES E PRIVACIDADE, incluídos no Apêndice B deste Termo de Referência.

5.2.1. O grau de criticidade para o tratamento da informação é o grau máximo.

6. ENTREGÁVEIS DO OBJETO/CRONOGRAMA

6.1. A prestação do serviço será realizada a partir da data de assinatura do contrato, obrigando-se a CONTRATADA a disponibilizá-la durante toda a vigência do contrato de acordo com a especificação do objeto descrita no item 2 deste Termo de Referência, nos prazos exemplificativos e não exaustivos apresentados na tabela abaixo:

Serviço	Periodicidade
Relação dos titulares dos valores mobiliários emitidos pela CONTRATANTE, refletindo a posição total, com abertura analítica das posições dos investidores mantidas sob a titularidade fiduciária da central depositária	Diariamente, até às 09h00.
Base acionária completa com várias possibilidades de seleção (exemplos: por opção de crédito, por domicílio, por Estado, por País, por tipo de pessoa - Física ou Jurídica) e possibilidade de <i>download</i> em formato texto ou <i>Excel</i> (incluindo datas retroativas)	Diariamente, até às 09h00.
Relatório de cálculos dos valores de créditos a que têm direito os titulares das ações	em até 4 (quatro) dias úteis antes do pagamento do evento societário deliberado aos acionistas
Relação do cálculo dos valores a serem pagos aos acionistas e o valor do imposto de renda a ser recolhido	em até 4 (quatro) dias úteis antes do pagamento do evento societário deliberado aos acionistas
Relação do total dos valores bruto, líquido e do imposto de renda retido na fonte pelo EMISSOR	Até 5 (cinco) dias úteis após o pagamento de dividendos e/ou atualização monetária
Informações dos dividendos pagos no ano calendário para fins de preenchimento da Escrituração Contábil Fiscal - ECF	Anualmente, até o dia 30 de maio
Apresentação de relatório anual que assegure o cumprimento e efetividade dos controles internos em relação a cadastro de acionistas.	Anualmente, até o dia 30 de novembro
Comunicar à CVM, a celebração e extinção do contrato de escrituração, conforme previsto no Art. 12 da RCVM 33	Até o 5º dia útil do mês subsequente a ocorrência
Mapa analítico das instruções de voto dos acionistas e Mapa Sintético das instruções de voto dos acionistas	Até 48 (quarenta e oito) horas antes da data de realização da assembleia

- 6.1.1. Os prazos para execução dos serviços estão definidos na tabela, aplicando-se, para os serviços não contemplados, os prazos previstos na legislação vigente e nas normas técnicas aplicáveis ou ainda, conforme solicitado pela Companhia.
- 6.1.2. A CONTRATADA é responsável pelo cumprimento desses prazos e normas, sob pena de aplicação das sanções previstas no contrato.
- 6.2. A remuneração dos serviços contratados pela COMPANHIA será realizada a saber:

Serviço	Periodicidade
Taxa de manutenção da base - valor fixo	Mensal (12 meses)

- 6.2.1. No valor a ser pago pela execução do objeto contratado estão todos os serviços prestados, inclusive taxa de implantação, emissão/extratos de informes, envio/postagem de extratos (Correios), caso aplicável, eventos de distribuição de dividendos e/ou JSCP, eventos de *follow-on* e/ou corporativos como grupamento e desdobramento e mapas de votação das assembleias, além de todos os insumos de encargos trabalhistas e tributos, inclusive contribuições fiscais e parafiscais, bem como quaisquer outras despesas necessárias à execução do Contrato, independentemente da quantidade de acionistas.

7. ETAPAS PREPARATÓRIAS

- 7.1. Não se aplica.

8. GARANTIA DOS BENS OU SERVIÇOS

- 8.1. Não se aplica.

9. SUPORTE TÉCNICO/ATENDIMENTO

- 9.1. A CONTRATADA deve disponibilizar serviço de suporte técnico à CONTRATANTE durante a vigência do contrato, em dias úteis (segunda à sexta-feira), no mínimo, em horário comercial (09h00 às 18h00), em português, (Brasil), prestado de modo remoto por telefone e/ou por meio de ferramenta de atendimento pela Internet, ambos disponibilizados pela CONTRATADA, para o esclarecimento de dúvidas e orientações de uso, bem como para tratar incidentes e investigações de problemas apresentados na execução dos serviços.
- 9.2. O atendimento do suporte técnico prestado pela CONTRATADA deve ocorrer no prazo máximo de 24 (vinte e quatro) horas úteis, sendo que no caso de acionamentos com alto grau de criticidade, o suporte deve ocorrer em até 1 (uma) hora.

10. TREINAMENTO E TRANSFERÊNCIA DE CONHECIMENTO

- 10.1. Por ocasião do início da efetiva utilização dos serviços, a CONTRATADA deverá ministrar treinamento/simulação aos colaboradores indicados pela CAIXA Seguridade, sendo permitida a sua realização de forma remota com o uso de ferramentas interativas como o Microsoft Teams® ou Zoom.

- 10.1.1. O treinamento com um especialista da CONTRATADA para capacitação da equipe da CAIXA Seguridade referente ao funcionamento da ferramenta, em dia e horário a ser ajustado após a contratação, com duração de até 02 (duas) horas.
- 10.1.2. A definição do dia, horário e o conteúdo das atividades será acordada entre o CONTRATANTE e a CONTRATADA, devendo ocorrer obrigatoriamente em dias úteis.
- 10.2. No caso de modificações substanciais do funcionamento da plataforma e rotinas aplicáveis aos serviços, a CONTRATADA se obriga a realizar atividade de treinamento com os colaboradores indicados pela CONTRATANTE em até 5 (cinco) dias úteis da ocorrência, com duração de até 01 (uma) hora.

11. EQUIPE TÉCNICA

- 11.1. A CONTRATADA deverá possuir colaboradores profissionais qualificados à prestação dos serviços.
- 11.2. A qualquer momento, a CAIXA Seguridade poderá solicitar a comprovação de vínculo entre a CONTRATADA e os referidos profissionais, bem como a comprovação de qualificação que estes possuem.

12. SUSTENTABILIDADE

- 12.1. A CONTRATADA deverá observar a Política de Responsabilidade Socioambiental da Companhia, na execução dos serviços contratados, seguindo as práticas de:
 - a. valorização do ser humano, o equilíbrio econômico-financeiro e o meio ambiente;
 - b. promoção da máxima eficiência no uso dos recursos naturais e de materiais deles derivados; e
 - c. incentivo à redução, reutilização, reciclagem e destinação adequada de resíduos, bem como à aquisição de bem cujos materiais sejam atóxicos ou biodegradáveis, que favoreçam a economia de insumos e energia, produzam menos poluentes e utilizem o conceito de tecnologia ou produção mais limpa, devolvendo os materiais em sua forma final, via eletrônica, em busca da economia e eficiência no uso de recursos naturais e de materiais deles derivados, para minimizar os potenciais impactos ambientais negativos.
- 12.2. Ainda, a CONTRATADA deverá observar os critérios definidos, especialmente no que se refere à diretriz de “adotar critérios de natureza social, ambiental e climática nos processos de compras e contratações de bens e serviços, contemplando:
 - a. Eficiência no uso de recursos naturais e tecnológicos;
 - b. Redução de geração de resíduos e emissão de documentos físicos, com incentivo à digitalização;
 - c. Adoção de práticas que promovam a segurança da informação e a proteção de dados pessoais.

13. FINALIZAÇÃO DO CONTRATO

- 13.1. Transferir os registros ao novo prestador, em caso de encerramento do contrato, independentemente da causa, mantendo os registros pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidas pela RCVM 33.
- 13.2. Comunicar à CVM, até o 5º dia útil do mês subsequente, a celebração e extinção do contrato de escrituração, conforme previsto no Art. 12 da RCVM 33.

14. LOCAL DE ENTREGA OU EXECUÇÃO/COMUNICAÇÕES

- 14.1. A CONTRATADA executará o objeto deste contrato em suas instalações.
- 14.2. Toda comunicação trocada entre as Partes, relativamente a este contrato, deverá ser feita por escrito e entregue via e-mail, copiando sempre os responsáveis indicados abaixo:

Pela **CONTRATADA**:

Nome:

Email:

Email secundário:

Endereço:

Tel.: +55 (xx) xxxx-xxxx

Pela **CONTRATANTE**:

GERÊNCIA NACIONAL DE RELAÇÕES COM INVESTIDORES

E-mail: geris@caixa.gov.br

E-mail secundário: geris02@caixa.gov.br

Endereço: Avenida Paulista, 750, 16º andar, Bela Vista, São Paulo/SP, CEP 01310-100

Tel.: (11) 3176-1340

- 14.2.1. A mudança de qualquer um dos dados para contato indicados acima deverá ser comunicado à outra Parte, em até 5 (cinco) dias úteis contados da sua ocorrência.

APÊNDICE A**1. CLAUSULAS DE REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES****1.1 GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS**

- 1.1.1 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.
- 1.1.2 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 1.1.3 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.
- 1.1.4 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 1.1.5 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.
- 1.1.6 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 1.1.7 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.
- 1.1.8 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 1.1.9 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 1.1.10 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA Seguridade tenha dado aprovação prévia por escrito para tais contas.
- 1.1.11 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.
- 1.1.12 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 1.1.13 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 1.1.14 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.
- 1.1.15 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.
- 1.1.16 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três

meses.

- 1.1.17 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 Seguridade sempre que solicitado.
- 1.1.18 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.
- 1.1.19 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.
- 1.1.20 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 1.1.21 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.
- 1.1.22 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.
- 1.1.23 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 1.1.24 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.
- 1.1.25 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 1.1.26 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 e quais os controles necessários para oferecer este acesso de forma segura.
- 1.1.27 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.
- 1.1.28 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA Seguridade, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA Seguridade, sem ônus adicionais para a CAIXA Seguridade.

1.2 SEGURANÇA DE ATIVOS

- 1.2.1 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.
- 1.2.2 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 1.2.3 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. A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 1.2.4 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 1.2.5 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.
- 1.2.6 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 1.2.7 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.
- 1.2.8 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 1.2.9 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 1.2.10 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA Seguridade tenha dado aprovação prévia por escrito para tais contas.
- 1.2.11 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.
- 1.2.12 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 1.2.13 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 1.2.14 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.
- 1.2.15 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.
- 1.2.16 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 1.2.17 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 Seguridade sempre

que solicitado.

- 1.2.18 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.
- 1.2.19 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.
- 1.2.20 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 1.2.21 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.
- 1.2.22 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.
- 1.2.23 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 1.2.24 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.
- 1.2.25 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo- real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 1.2.26 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.
- 1.2.27 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.
- 1.2.28 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA Seguridade, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA Seguridade, sem ônus adicionais para a CAIXA Seguridade.

1.3 SEGURANÇA DE REDES

- 1.3.1 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).
- 1.3.2 O conjunto de regras do firewall deve se basear na negação de todos os serviços, exceto aqueles especificamente permitidos.
- 1.3.3 O processo para instalação e adaptação de regras de firewalls deve ser feito com duplo controle.

- 1.3.4 A Contratada deve revisar as regras de firewall pelo menos semestralmente, guardando evidências dessas revisões e dos ajustes eventualmente realizados, comunicando à CAIXA Seguridade sobre a realização desta revisão.
- 1.3.5 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).
- 1.3.6 O monitoramento de segurança deve ser configurado para rastrear e registrar tentativas de intrusão suspeitas ou reais.
- 1.3.7 A Contratada deve informar imediatamente à CAIXA Seguridade em caso de tentativa de intrusão real, e informar à CAIXA Seguridade em relatório mensal sobre as tentativas de intrusão suspeitas.
- 1.3.8 A Contratada deve implementar solução anti-DDoS, capaz de prevenir ataques de negação de serviço (Denial of Service).
- 1.3.9 As soluções de firewall, IPS e-DDoS utilizadas pela Contratada serão validadas pela CAIXA Seguridade a partir de documentações do fabricante ou certificações.
- 1.3.10 A Contratada deve impedir o uso do protocolo Bluetooth para a transferência de dados.
- 1.3.11 Todas as comunicações e trocas de informações entre a Contratada e a CAIXA Seguridade devem ser realizadas por meio de conexão protegida, com TLS 1.3 ou superior.
- 1.3.12 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).
- 1.4 CICLO DE VIDA DE DESENVOLVIMENTO SEGURO**
 - 1.4.1 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.
 - 1.4.2 A Contratada deve fazer análise de código automatizada com base nas melhores práticas de mercado, utilizando como referência os padrões do OWASP.
 - 1.4.3 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.
 - 1.4.4 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 Seguridade, dentro de um período razoável e de acordo com a criticidade da falha encontrada.
 - 1.4.5 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.
 - 1.4.6 A Contratada deve submeter suas políticas de desenvolvimento seguro à aprovação da CAIXA Seguridade.

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

1.5 GESTÃO DE SERVIÇOS E MUDANÇAS

- 1.5.1 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.

- 1.5.2 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).

- 1.5.3 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).

- 1.5.4 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.

- 1.5.5 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.

- 1.5.6 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.

- 1.5.7 A Contratada deve disponibilizar os documentos de avaliação de risco à CAIXA Seguridade sempre que solicitado.

1.6 GESTÃO DE INCIDENTES DE SEGURANÇA

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

- 1.6.2 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 Seguridade. O escopo dos testes será previamente combinado e aprovado pela CAIXA Seguridade, dentro dos limites do contrato.

- 1.6.3 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.
- 1.6.4 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 Seguridade sempre que solicitado.
- 1.6.5 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.
- 1.6.6 A contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.
- 1.6.7 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 Seguridade estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA Seguridade.
- 1.6.8 A Contratada deverá ter um processo de notificação de incidentes 24x7.
- 1.6.9 A Contratada deverá comunicar à CAIXA Seguridade incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.
- 1.6.10 Os incidentes serão comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA Seguridade, que opera 24x7, por meio do endereço de e-mail: abuse@CAIXA Seguridade.gov.br. Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.
- 1.6.11 A Contratada deverá comunicar à CAIXA Seguridade, 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)	<p>Eventos cujo contexto principal é a segurança cibernética, tais como:</p> <ul style="list-style-type: none"> -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. <p>Exemplos não exaustivos: ataque de Ransomware, ataque de negação de serviço distribuído – DDoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.</p>	2 horas após o início da ocorrência.

<p>Severidade 2 (Alta)</p>	<p>Eventos cujo contexto principal é a segurança cibernética, tais como:</p> <ul style="list-style-type: none"> -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. <p>Exemplos não exaustivos: ataques de escalação de privilégio em servidores, ataques do tipo brute force e password spray. Dentre outros</p>	<p>4 horas após o início da ocorrência.</p>
--------------------------------	---	---

- 1.6.12 Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA Seguridade.
- 1.6.13 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 utilizando o modelo do MITRE ATT&CK®.
- 1.6.14 A contratada deverá seguir preferencialmente o modelo de comunicação de ISCF – Incidente de Segurança Cibernética em Fornecedor, Anexo IIA, que também contempla situações de incidentes de segurança com dados pessoais.
- 1.6.15 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 Seguridade 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.
- 1.6.16 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 Seguridade sempre que solicitado.
- 1.6.17 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.
- 1.6.18 A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA Seguridade deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.
- 1.6.19 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 Seguridade por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA Seguridade.

1.7 CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

- 1.7.1 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.

- 1.7.2 O referido plano de continuidade deverá ser informado para a CAIXA Seguridade como parte das ações de acompanhamento do contrato, e deverá ser atualizado e testado anualmente, ou em qualquer mudança significativa do ambiente.
- 1.7.3 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.
- 1.7.4 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;
- 1.7.5 A obrigatoriedade do plano de continuidade se estende para empresas que sejam subcontratadas pela Contratada.
- 1.7.6 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.
- 1.7.7 A avaliação de riscos e dos processos críticos devem levar em consideração instrumentos específicos, como um BIA – Business Impact Analysis.
- 1.7.8 A Contratada, visando a continuidade dos negócios, deve implantar uma política de backup, conforme exposto no item 10.
- 1.8 AUDITORIA CONTÍNUA**
- 1.8.1 A Contratada deve apresentar à CAIXA Seguridade, 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.
- 1.8.2 A Contratada deve informar imediatamente à CAIXA Seguridade sobre qualquer auditoria regulatória, sua finalidade e como ela se relaciona com os serviços prestados à CAIXA

Seguridade.

- 1.8.3 A Contratada deve informar à CAIXA Seguridade caso sejam contatados por um órgão regulador e se o propósito desse contato pode estar relacionado com/ou afetar os serviços prestados à CAIXA Seguridade.
- 1.8.4 A Contratada deve fornecer os subsídios necessários para que a CAIXA Seguridade implemente os indicadores de desempenho de segurança que vierem a ser definidos durante a vigência do contrato.
- 1.8.5 A Contratada deverá disponibilizar, caso a CAIXA Seguridade solicite, acesso às instalações da Contratada para realização de processo de Due Dilligence Presencial, para verificar o cumprimento dos requisitos de segurança.
- 1.8.6 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 Seguridade sempre que solicitado.

1.9 CONTROLES CRIPTOGRÁFICOS

- 1.9.1 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 Seguridade.
- 1.9.2 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.
- 1.9.3 A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 1.9.4 A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 1.9.5 Caso a Contratada hospede uma página com uma URL e um certificado gerados pela CAIXA Seguridade, a Contratada deverá armazenar este certificado em dispositivo seguro com bloqueio para exportação da chave.
- 1.9.6 As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.
- 1.9.7 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).
- 1.9.8 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.
- 1.9.9 A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA Seguridade, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.
- 1.9.10 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.
- 1.9.11 A Contratada deve permitir a auditoria da segurança de chaves criptográficas.
- 1.9.12 A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de

dados por meio do TLS 1.3 e superior.

1.10 POLÍTICA DE BACKUP

- 1.10.1 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.
- 1.10.2 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 Seguridade.
- 1.10.3 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 na item 7.
- 1.10.4 A Contratada deve garantir que o site de armazenamento alternativo conta com os mesmos controles de segurança do site de armazenamento primário.

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

- 1.11.1 Sempre que a CAIXA Seguridade 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 Seguridade.
- 1.11.2 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	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 do Provedor de Nuvem	ANUAL

1.12 ENCERRAMENTO DO CONTRATO

- 1.12.1 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.
- 1.12.2 A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA Seguridade.
- 1.12.3 Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.
- 1.12.4 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 Seguridade certificando a conformidade dos processos realizados com a norma indicada.
- 1.12.5 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.

1.13 NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS

- 1.13.1 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) Não fornecer evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões de acesso realizadas;
- b) Não comunicar a revisão das regras de firewall;
- c) Não comunicar ocorrências de intrusão real;
- d) Não fornecer relatório mensal sobre as tentativas de intrusão;
- e) Não fornecer o planejamento de correção de vulnerabilidades;
- f) Não fornecer os relatórios dos testes SAST e DAST realizados e o planejamento das correções a serem feitas;
- g) Não fornecer os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções;
- h) Não fornecer os relatórios de incidentes conforme SLA;
- i) Não prestar as informações e relatórios solicitados pela CAIXA Seguridade;
- j) Não fornecer os relatórios de auditoria externa independente;
- k) Não fornecer relatório indicando conformidade com o NIST SP 800-88;
- l) Não atender a convocação da CAIXA Seguridade para Due Diligence presencial ou remoto;
- m) Não fornecer a documentação solicitada em decorrência do Due Diligence presencial ou remoto, conforme prazo acordado entre as partes;

2. CLAUSULAS DE REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA SOLUÇÃO EM NUVEM

2.1 GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS

- 2.1.1 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.
- 2.1.2 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.
- 2.1.3 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 2.1.4 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.
- 2.1.5 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 2.1.6 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.
- 2.1.7 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 2.1.8 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.

- 2.1.9 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 2.1.10 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 2.1.11 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA Seguridade tenha dado aprovação prévia por escrito para tais contas.
- 2.1.12 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.
- 2.1.13 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 2.1.14 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 2.1.15 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.
- 2.1.16 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.
- 2.1.17 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 2.1.18 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 Seguridade sempre que solicitado.
- 2.1.19 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.
- 2.1.20 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.
- 2.1.21 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 2.1.22 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.
- 2.1.23 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.
- 2.1.24 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

- 2.1.25 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.
- 2.1.26 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.
- 2.1.27 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo- real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 2.1.28 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.
- 2.1.29 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.
- 2.1.30 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA Seguridade, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA Seguridade, sem ônus adicionais para a CAIXA Seguridade.

2.2 CONTROLES CRIPTOGRÁFICOS

- 2.2.1 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 .
- 2.2.2 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 Seguridade.
- 2.2.3 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.
- 2.2.4 A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 2.2.5 A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 2.2.6 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 superiores; Mozilla Firefox 45 e superiores; Google Chrome 49 e superiores; Apple 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.

- 2.2.7 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.
- 2.2.8 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>).
- 2.2.9 As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.
- 2.2.10 Caso haja a necessidade do compartilhamento de chaves simétricas entre a CAIXA Seguridade e a Contratada, essas chaves devem ser geradas pela CAIXA Seguridade 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 Seguridade no seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.
- 2.2.11 No caso de utilização de um Provedor de Serviços em Nuvem, as certificações FIPS exigidas estão descritas no item 10.
- 2.2.12 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).
- 2.2.13 A Contratada deve prover a criptografia de dados em repouso utilizando, no mínimo, algoritmo AES com chaves de 128 bits.
- 2.2.14 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.
- 2.2.15 A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA Seguridade, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.
- 2.2.16 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.
- 2.2.17 A Contratada deve permitir a auditoria da segurança de chaves criptográficas.
- 2.2.18 A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3.
- 2.2.19 A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA Seguridade, suportando, no mínimo, TLS 1.3 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
- 2.2.20 Os parâmetros TLS Renegotiation e TLS Resumption devem estar desabilitados.

2.2.21 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.

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

2.3 CONTROLE DE ACESSO AO AMBIENTE DE NUVEM

2.3.1 O acesso de empregados da CAIXA Seguridade à solução em nuvem deverá ser integrado com ferramenta de SSO da CAIXA Seguridade, ou com o MS Azure 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 Seguridade por qualquer motivo por período determinado.

2.3.2 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 Seguridade, que precisem acessar os recursos em nuvem.

2.3.3 O acesso aos recursos da CAIXA Seguridade 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.

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

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

2.4 REQUISITOS DE AUTORIZAÇÃO DE ACESSO AOS DADOS PELO BACEN

2.4.1 A Contratada deve garantir que a prestação dos serviços não causará prejuízo ao funcionamento regular da CAIXA Seguridade nem embaraço à atuação da Banco Central do Brasil, assegurando que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços serão prestados não restringem nem impedem o acesso da CAIXA Seguridade nem do Banco Central do Brasil aos dados e às informações.

2.4.2 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 Seguridade por meio comunicação formal.

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

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

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

- 2.4.6 A Contratada deve assegurar a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas e/ou armazenadas em nuvem.
- 2.4.7 Também deve assegurar à CAIXA Seguridade 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.
- 2.4.8 A Contratada deve assegurar à CAIXA Seguridade, acesso a toda documentação comprobatória, em nome do provedor, que esclareça a Região/Zona de Disponibilidade escolhidos pela CAIXA Seguridade para hospedagem de seus recursos.
- 2.4.9 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.
- 2.4.10 A Contratada deve garantir, em caso de decretação de regime de resolução da CAIXA Seguridade 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.
- 2.4.11 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:
- a) 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.
 - b) Caso haja subcontratação do serviço em nuvem, desde que explicitamente autorizado pela CAIXA Seguridade, 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.

2.5 PROTEÇÃO DOS DADOS PROCESSADOS E ARMazenADOS EM NUVEM

- 2.5.1 Além dos requisitos descritos no item 2, a Contratada também deve permitir trabalhar com chaves simétricas e assimétricas geradas e armazenadas pela CAIXA Seguridade. Para tanto, ela deve prover meios que permitam o envio das chaves da CAIXA Seguridade para o seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.
- 2.5.2 Caberá à CAIXA Seguridade decidir quem fará a geração e a gestão de cada chave: se a própria CAIXA Seguridade ou a Contratada.
- 2.5.3 Caso a CAIXA Seguridade 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>).
- 2.5.4 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 Seguridade, 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>).

- 2.5.5 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 Seguridade e a Contratada não deverá ter qualquer acesso às chaves envolvidas.
- 2.5.6 Quando se tratar de contratação no modelo IaaS, exige-se a certificação FIPS 140-2 nível 3.
- 2.5.7 Quando se tratar de contratação no modelo PaaS ou SaaS, exige-se a certificação FIPS 140-2 nível 2.
- 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.
- 2.5.9 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 Seguridade.
- 2.5.10 A Contratada deverá assinar Termo de Confidencialidade resguardando que os recursos, dados e informações de propriedade da CAIXA Seguridade, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.
- 2.5.11 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 Seguridade.
- 2.5.12 A CAIXA Seguridade 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.

2.6 MONITORAÇÃO DOS DADOS PROCESSADOS E ARMAZENADOS EM NUVEM

- 2.6.1 A Contratada deverá fornecer, sempre que solicitado pela CAIXA Seguridade, 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.
- 2.6.2 A trilha de auditoria deve conter, minimamente, itens descritos no item 1.23 deste documento.
- 2.6.3 O Provedor de Serviço em Nuvem, deve dispor de recurso que permita o gerenciamento centralizado de eventos e envio para a CAIXA Seguridade, sempre que solicitado, de logs/informações de trilha.
- 2.6.4 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.

2.7 SEGURANÇA DO TRÁFEGO DE DADOS COM A NUVEM

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

- 2.7.2 Caso a aplicação não suporte TLS 1.3, será admitida a compatibilidade para TLS 1.3.
- 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 Seguridade e o Provedor de Serviços em Nuvem, para todos os casos em que a Contratada e o Provedor forem entidades distintas.
- 2.7.4 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 Seguridade.
- 2.7.5 O Provedor de Serviços em Nuvem não deverá ter permissão de uso ou acesso direto ao ambiente de autenticação da CAIXA Seguridade.
- 2.7.6 Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA Seguridade, 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.

2.8 ALTA DISPONIBILIDADE DOS SERVIÇOS EM NUVEM

- 2.8.1 Para assegurar a continuidade dos serviços e a resiliência das operações críticas da CAIXA Seguridade, as soluções em nuvem fornecidas pela CONTRATADA deverão ser projetadas com foco em alta disponibilidade.
- 2.8.2 Para tanto, é obrigatória a adoção de arquiteturas que contemplem a distribuição geográfica das cargas de trabalho (workloads) em múltiplas zonas de disponibilidade, de forma a mitigar riscos de indisponibilidade, de integridade e de continuidade, garantindo a operação ininterrupta dos serviços essenciais.
- 2.8.3 Além disso, a CONTRATADA deve assegurar que:
- i. Os dados e serviços estejam replicados de forma síncrona ou assíncrona entre as zonas, conforme a criticidade da aplicação;
 - ii. Os mecanismos de balanceamento de carga e failover estejam devidamente configurados e testados periodicamente;
 - iii. Toda a infraestrutura esteja em conformidade com os requisitos regulatórios e legais aplicáveis no Brasil, incluindo a residência dos dados em território nacional;
 - iv. Haja documentação clara sobre os procedimentos de recuperação e continuidade em caso de falhas regionais.

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

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

2.10 GESTÃO DE INCIDENTES DE SEGURANÇA

- 2.10.1 A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.
- 2.10.2 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 Seguridade. O escopo dos testes deve ser previamente combinado e aprovado pela CAIXA Seguridade, dentro dos limites do contrato.

- 2.10.3 Os teste 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.
- 2.10.4 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 Seguridade sempre que solicitado.
- 2.10.5 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.
- 2.10.6 A contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.
- 2.10.7 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 Seguridade estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA Seguridade.
- 2.10.8 A Contratada deve ter um processo de notificação de incidentes 24x7.
- 2.10.9 A Contratada deve comunicar à CAIXA Seguridade incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.
- 2.10.10 Os incidentes devem ser comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA Seguridade, que opera 24x7, por meio do endereço de e-mail: abuse@CAIXA Seguridade.gov.br. Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.
- 2.10.11 A Contratada deve comunicar à CAIXA Seguridade, 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)	<p>Eventos cujo contexto principal é a segurança cibernética, tais como:</p> <ul style="list-style-type: none"> -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. <p>Exemplos não exaustivos: ataque de Ransomware, ataque de negação de serviço distribuído – DDoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.</p>	2 horas após o início da ocorrência.

Severidade 2 (Alta)	<p>Eventos cujo contexto principal é a segurança cibernética, tais como:</p> <ul style="list-style-type: none"> -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. <p>Exemplos não exaustivos: ataques de escalção de privilégio em servidores, ataques do tipo brute force e password spray. Dentre outros</p>	4 horas após o início da ocorrência.
------------------------	--	--------------------------------------

- 2.10.12 Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA Seguridade.
- 2.10.13 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 utilizando o modelo do MITRE ATT&CK®.
- 2.10.14 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.
- 2.10.15 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 Seguridade 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.
- 2.10.16 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 Seguridade sempre que solicitado.
- 2.10.17 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.
- 2.10.18 A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA Seguridade deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.
- 2.10.19 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 Seguridade por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA Seguridade.
- 2.11 CERTIFICADOS E RELATÓRIOS QUE COMPROVAM O CUMPRIMENTO DOS**

REQUERIMENTOS MÍNIMOS DE SEGURANÇA.

- 2.11.1 Para serviços de nuvem, caso a Contratada pela CAIXA Seguridade 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 Seguridade.
- 2.11.2 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 Seguridade.
- 2.11.3 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

2.11.4 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
----------------------------------	--	--	--	-------

2.12 ENCERRAMENTO DO CONTRATO

- 2.12.1 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.
- 2.12.2 A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA Seguridade.
- 2.12.3 Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.
- 2.12.4 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 Seguridade certificando a conformidade dos processos realizados com a norma indicada.
- 2.12.5 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.

2.13 NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS

- 2.13.1 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:
- Não fornecer evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões de acesso realizadas;
 - Não comunicar ocorrências de intrusão real;
 - Não fornecer relatório mensal sobre as tentativas de intrusão;
 - Não fornecer o planejamento de correção de vulnerabilidades;
 - Não fornecer os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções;
 - Não fornecer os relatórios de incidentes conforme SLA;
 - Não prestar as informações e relatórios solicitados pela CAIXA Seguridade;
 - Não fornecer relatório indicando conformidade com o NIST SP 800-88.

- i) Não atender a convocação da CAIXA Seguridade 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.

APÊNDICE B**1 CLÁUSULAS DE SEGURANÇA DA INFORMAÇÃO**

- 1.1 A CONTRATADA deve conhecer e cumprir a Política de Segurança e Informação da Caixa Seguridade, disponibilizada no site de relações com investidores da CAIXA Seguridade (<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 proteger as informações corporativas da CAIXA Seguridade e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.
- 1.3 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.
- 1.4 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.
- 1.5 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.
- 1.6 A CONTRATADA deve assegurar que os recursos e informações da CAIXA Seguridade colocados à sua disposição sejam utilizados apenas para a finalidade contratada.
- 1.7 A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA Seguridade e seu mercado de atuação.
- 1.8 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.
- 1.9 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 Seguridade e de seus clientes, sem prejuízo da responsabilidade por perdas e danos a que derem causa e das cominações contratuais impostas.
- 1.10 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 Seguridade ou sob sua responsabilidade.
- 1.11 A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações da CAIXA Seguridade assinem o Termo de Confidencialidade.
- 1.12 A CONTRATADA deve enviar, anualmente, à CONTRATANTE a versão vigente do Termo de Confidencialidade, a ser disponibilizado pela área gestora do contrato, devidamente assinado(s) por seu(s) dirigente(s), empregados(s) e colaborador(es).
- 1.13 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	8 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	
<i>Privacy by Design e Secure by Design</i>	- Metodologia e princípios	
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 <i>wi-fi</i> 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; - Qualidade de vida digital; - Segurança de dados do usuário em viagens	
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; - Empreendedorismo na Internet	
Criptografia	- Criptografia; - Certificação Digital; - Assinatura Digital	

Direito Digital	<ul style="list-style-type: none"> - Conceitos jurídicos e legislação relacionada à segurança da informação; - Direitos autorais; - Fraudes; - Assédio virtual; - Crimes cibernéticos; - Crimes na Internet; - *Hacktivismo
Prevenção à fraude	<ul style="list-style-type: none"> - 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.

1.13.1 O treinamento referido no item 1.13 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 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao ano base, a documentação comprobatória de cumprimento do treinamento referido no item 1.13.

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.

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.

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

1.20 A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores:

a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, treinados em SI, conforme item 1.13 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; e

b) Quantidade de empregados que assinaram o Termo de Confidencialidade, previsto no item 1.11, 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.

1.21 O não atendimento pela CONTRATADA de qualquer requisito de segurança definido no presente

instrumento contratual, implicará na sujeição à aplicação de multa e às demais sanções previstas no instrumento contratual, sem prejuízo de rescisão.

- 1.22 Em caso de indisponibilidade parcial ou total do serviço contratado, a CONTRATADA se compromete a comunicar imediatamente a CONTRATANTE e atuar de forma tempestiva para regularização do serviço.
- 1.23 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.
- 1.24 No encerramento/extinção do contrato a CONTRATADA se compromete a 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.
- 1.25 A CONTRATADA é responsável por realizar o tratamento das informações da CAIXA Seguridade e as sob sua responsabilidade, observando sua classificação de sigilo, bem como as demais regras internas da CAIXA estipuladas na versão vigente do manual normativo OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.
- 1.26 A CONTRATADA, durante a execução dos serviços contratados, deve adotar a mesma classificação da informação adotada pela CONTRATANTE, observar e cumprir as regras internas da CONTRATANTE quanto ao tratamento de informações sensíveis e confidenciais da CAIXA Seguridade.
- 1.27 A CONTRATADA é responsável pelas informações que obtiver, em razão de acesso aos recursos computacionais da CAIXA e se compromete a tomar conhecimento e cumprir as regras de uso aceitável e não aceitável da informação.
- 1.28 O treinamento de segurança da informação e proteção de dados referido no item 1.13 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 08 horas.
- 1.29 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do ano base, a documentação comprobatória de cumprimento do treinamento referido no item 1.28 e, caso estabelecido pela CONTRATANTE.
- 1.30 A CONTRATADA deve emitir relatório, anualmente, até o último dia útil do mês subsequente ao término do ano base, relacionados aos seus riscos de segurança da informação e cibernéticos identificados, medidos, mitigados e monitorados e que possam trazer algum impacto à CONTRATANTE.
- 1.31 O relatório referidos no item anterior deve proporcionar à CAIXA identificar até que ponto os riscos de segurança da informação e cibernéticos aos quais a CONTRATADA está submetida pode impactar os negócios da CAIXA.
- 1.32 A CONTRATADA garantirá que a CONTRATANTE, ou a auditoria independente indicada pela CONTRATANTE, ou os órgãos de regulação/fiscalização das atividades de atuação da CAIXA tenham acesso físico e lógico ao seu ambiente e às informações relacionadas ao objeto do contrato, para realizar verificações relativas aos padrões de segurança da informação.
- 1.33 A CONTRATADA deve manter processo de monitoramento e resposta a incidentes de segurança da informação adequado ao objeto contratual.
- 1.34 A CONTRATADA deve reportar imediatamente à CONTRATANTE os incidentes de segurança da informação identificados em seu ambiente ou operação e em toda sua cadeia produtiva.

- 1.35 A CONTRATADA deve enviar à CONTRATANTE, em até 05 dias úteis da detecção da ocorrência, relatório detalhado sobre o incidente de segurança da informação identificado, seus impactos, medidas corretivas implantadas e a implantar.
- 1.36 A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores mencionados no item 1.20 e dos demais a seguir:
- a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, que obtiveram nota mínima de aprovação no treinamento relacionado a Segurança da Informação mencionado no item 1.13 / Quantidade total de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
 - b) Quantidade de relatórios, referidos no item 1.30, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
 - c) Quantidade de relatórios, referidos no item 1.35, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base.
- 1.37 A CONTRATADA deve garantir a continuidade do processamento das informações críticas de negócios, no caso de contratação de bem ou serviço de suporte às atividades críticas da CAIXA Seguridade.
- 1.38 A CONTRATADA deve garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos.
- 1.39 A CONTRATADA deve cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais.
- 1.40 A CONTRATADA deve apresentar, sempre que requerido pela CONTRATANTE, relatórios emitidos por empresas de auditoria especializada independente que tenha realizado trabalho de auditoria em segurança da informação na CONTRATADA e certificações que atestem o nível de confiança nos princípios de segurança da informação.
- 1.41 A CONTRATADA se responsabiliza pelos incidentes de segurança detectados em sua infraestrutura ou na infraestrutura de empresa subcontratada.

2 CLÁUSULAS DE PRIVACIDADE

- 2.1 A CONTRATADA deve tomar conhecimento dos 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 CAIXA Seguridade, doravante denominada de “CONTRATANTE”, assume o papel de Controladora de dados pessoais, e a “CONTRATADA”, assume o papel de operadora de dados pessoais.
- 2.3 Para a execução da finalidade prevista no presente contrato, a CONTRATANTE colocará à disposição da CONTRATADA:

- a) os dados dos acionistas da Companhia;
- b) na categoria de dados pessoais; e
- c) para fins de tratamento nos termos descritos no item 2 do Termo de Referência e em consonância com a RCVM 33.

- 2.4 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.
- 2.5 A CONTRATADA deve garantir a confidencialidade no tratamento de dados pessoais, protegendo-os contra acesso, modificação, destruição ou divulgação não autorizada.
- 2.6 A CONTRATADA está autorizada a tratar, em nome da CONTRATANTE, os dados pessoais a que tiver acesso em decorrência do presente Contrato para a finalidade pertinente ao serviço de escriturador de ações.
- 2.7 A CONTRATADA deverá, quando do término das atividades de tratamento de dados pessoais ou ao final do contrato, a critério da CONTRATANTE, eliminar todos os dados pessoais.
- 2.8 A CONTRATADA deve manter, por escrito, o registro das operações de tratamento realizadas em nome da CONTRATANTE.
- 2.9 A CONTRATADA deve colaborar com a CONTRATANTE no cumprimento de sua obrigação de responder às solicitações de exercício dos direitos dos titulares.
- 2.10 A CONTRATADA deve comunicar imediatamente a CONTRATANTE o recebimento de requisição do titular de dados no exercício de seus direitos.
- 2.11 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.
- 2.12 A CONTRATADA deve 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.
- 2.13 A CONTRATADA notificará a CONTRATANTE de qualquer violação de dados pessoais imediatamente após tomar conhecimento, inclusive aplicando medidas de contenção, formalizando a ocorrência ao gestor operacional do contrato. Essa notificação deve ser acompanhada de todos os dados necessários para eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao(s) titular(es) de dados pessoais.
- 2.14 A CONTRATADA auxiliará a CONTRATANTE com as informações necessárias para cumprimento de suas obrigações junto à Autoridade Nacional de Proteção de Dados (ANPD) e quaisquer órgãos reguladores, de fiscalização, de supervisão e de controle, inclusive na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).
- 2.15 A CONTRATADA deverá notificar imediatamente a CONTRATANTE em caso de solicitações judiciais e de órgãos reguladores, de fiscalização, de supervisão e de controle para disponibilização de dados pessoais.
- 2.16 A CONTRATADA deverá solicitar autorização prévia da CONTRATANTE para subcontratação de outra empresa para quaisquer atividades que envolvam o tratamento de dados pessoais relativos ao presente contrato.

- 2.17 Em caso de concretização de subcontratação ou de sua rescisão, a CONTRATADA deverá enviar notificação mandatória sobre o fato à CONTRATANTE.
- 2.18 A CONTRATADA é responsável por quaisquer descumprimentos deste contrato pela empresa SUBCONTRATADA, inclusive em relação a incidentes de segurança com dados pessoais.
- 2.19 A CONTRATADA deverá observar os requisitos de privacidade desde a concepção em seus produtos, processos, serviços e soluções tecnológicas relacionadas ao tratamento de dados pessoais referentes a este contrato.
- 2.20 A CONTRATADA somente poderá realizar transferência de dados pessoais para terceiros seguindo as instruções da CONTRATANTE ou mediante prévia autorização.