BANCO DA AMAZÔNIA

CONTRATO Nº 2025/135

CONTRATO DE FORNECIMENTO DE LICENÇA DE SOFTWARE, INCLUINDO SUPORTE E MANUTENÇÃO, PARA ACESSO AO PORTAL DE GOVERNANÇA CORPORATIVA, QUE ENTRE SI FAZEM O BANCO DA AMAZÔNIA S.A. E A EMPRESA ATLAS GOVERNANCE TECNOLOGIA LTDA.

Por este instrumento particular de Contrato, em que são Partes, de um lado o **BANCO DA AMAZÔNIA S.A.**, Sociedade de Economia Mista, vinculado ao Governo Federal, com sede em Belém (PA), situado na Avenida Presidente Vargas, nº 800, inscrito no CNPJ/MF sob o nº 04.902.979/0001-44, representado neste ato por sua Gerente Executiva da Gerência de Contratações e Gestão Administrativa de Contratos - GECOG, Sra. **BRUNA ELINE DA SILVA CAVALCANTE,** brasileira, solteira, bancária, portadora da Carteira de Identidade Profissional nº 25700 OAB/PA e CPF/MF nº 796.223.562-49, doravante denominado **CONTRATANTE**, e de outro lado a empresa **ATLAS GOVERNANCE TECNOLOGIA LTDA**, sociedade unipessoal de responsabilidade limitada, com registro na Junta Comercial do Estado de Minas Gerais (JUCEMG) sob o NIRE nº 31.214.357.827, com sede em Nova Lima/MG, situada na Rua Ministro Orozimbo Nonato, n.º 102, Sala 2006, Bairro Vila da Serra, CEP 34.006-053, inscrita no CNPJ sob o nº 25.462.636/0001-86, representada neste ato por seu Administrador, Sr. **EDUARDO SHAKIR CARONE,** brasileiro, casado, administrador de empresas, portador da CNH n° 01969555103 DETRAN/SP, inscrito no CPF/MF sob n° 295.344.578-17, doravante denominada **CONTRATADA**, nos termos da decisão do Comitê de Administração da GECOG do **CONTRATANTE**, datada de 24/06/2025, observado o processo de **Dispensa de Licitação**, com fundamento no Artigo 29, Inciso II da Lei n.º 13.303/2016, c/c Art. 13 do Regulamento de Licitações e Contratos do Banco da Amazônia, firmam o presente Contrato, sujeitando ainda, as partes às demais disposições da Lei n° 13.303/2016, e suas alterações e às Normas de Direito Privado:

DO OBJETO

CLÁUSULA PRIMEIRA - O presente Contrato tem por objeto a contratação de empresa especializada, para a para aquisição de Licença não exclusiva de uso de Software, com o suporte e manutenção durante toda a vigência do Contrato para acesso ao Portal de Governança Corporativa do **CONTRATANTE**.

PARÁGRAFO PRIMEIRO – A **CONTRATADA** fornecerá 30 (trinta) licenças de Software para acesso ao Portal de Governança, incluindo administradores e usuários:

Quantidade	Descrição
30 licenças	Administrador/Usuário

PARÁGRAFO SEGUNDO – A proposta comercial apresentada pela **CONTRATADA**, datada de 28/02/2025, fica fazendo parte integrante deste Contrato como se nele estivesse transcrita.

DO PRAZO DE EXECUÇÃO/ENTREGA DO OBJETO DA CONTRATAÇÃO

CLÁUSULA SEGUNDA - A **CONTRATADA** deverá entregar as Licenças no primeiro dia útil após a assinatura do Contrato.

DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO E DAS ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

CLÁUSULA TERCEIRA – O processo de aquisição de Licenças não exclusiva de uso de Softwares descrito neste termo visa suprir as necessidades da Alta Gestão do **CONTRATANTE**, com os seguintes requisitos:

PARÁGRAFO PRIMEIRO - Requisitos Técnicos:

- Possuir estrutura tecnológica compatível com ambiente Windows, MacOS, iOS e Android.
- Possuir aplicativo (“app”) para iOS e Android, que possa, preferencialmente, ser executado em contexto isolado do dispositivo.
- Possuir disponibilidade de armazenamento de conteúdo com capacidade ilimitada com Data Center localizado em território nacional (Brasil)
- Os acessos aos serviços devem ser realizados por meio de canais de comunicação seguros, protegido por criptografia, preferivelmente por meio do protocolo HTTP sobre TLS 1.2 ou TLS 1.1 (HTTPS);
- As informações processadas, armazenadas e transmitidas devem ser protegidas com uso de algoritmos públicos de criptografia, preferivelmente com a adoção de chaves criptográficas assimétricas**.**

PARÁGRAFO SEGUNDO - **Requisitos Funcionais**

- A solução a ser fornecida será utilizada por colegiados e Órgãos de governança da **CONTRATANTE** em reuniões, tais como as reuniões de Diretoria, Conselhos de Administração e Fiscal e Comitês do **CONTRATANTE**. Esta relação é não-exaustiva.
- O Portal de Governança Corporativa deverá possibilitar a convocação e a realização de reuniões, disponibilizando e organizando as informações do **CONTRATANTE** e facilitando a interação e o desempenho das funções dos membros dos colegiados e órgãos de governança e seus assessores. Deverá, ainda, permitir a aprovação de documentos e processos.
- O Portal de Governança Corporativa deverá possuir as seguintes principais funções:
- Repositório de informações: armazenamento de informações do **CONTRATANTE** e dos membros dos colegiados e órgãos de governança.
- Convocação de reuniões, disponibilização do calendário de eventos e disponibilização da pauta e material das reuniões.
- Comunicação: facilitação da interação com os membros dos colegiados e Órgãos de governança por meio de envio de alertas, e-mails e votações on-line.

PARÁGRAFO TERCEIRO - O Portal de Governança Corporativa deverá possibilitar acesso via navegador Web (“browser”) e, no caso de dispositivos móveis, por meio de aplicação (“app”) para dispositivos móveis, conforme detalhado neste documento. Deve ainda:

- Permitir acesso 24 (horas) horas por dia, 7 (sete) dias por semana;
- Permitir acesso off-line, ou seja, quando a Internet não estiver disponível, de modo que o usuário possa trabalhar em locais sem rede, como, por exemplo, dentro de aviões em viagens aéreas, sincronizando os dados com o repositório quando a ferramenta for colocada em modo online;
- Possuir ambiente personalizado (logotipo) do **CONTRATANTE**;

- Possibilitar a inclusão de organograma das empresas, estrutura societária, documentos societários, códigos, políticas, informações legais, informações financeiras e gerenciais das companhias;
- Possuir ferramenta de busca que possibilite a pesquisa de conteúdo, conforme o perfil de acesso do usuário, inclusive do conteúdo dos materiais de reunião aos quais o usuário tenha acesso;
- Possibilitar upload e download do conteúdo (textos, imagens e arquivos diversos) necessário à realização das reuniões e ao andamento dos trabalhos dos órgãos de governança;
- Possibilitar criação e atualização de calendário de reuniões e eventos dos colegiados e órgãos de governança, com integração com MS Outlook ou Calendário do Gmail.
- Possibilitar gerenciamento do conteúdo: armazenamento, localização e recuperação de informações, inserção, edição e/ou exclusão de informações;
- Possibilitar estruturação de pauta, disponibilização do material das reuniões (permitindo a inclusão de marca d´água nos documentos, contendo o nome do usuário e a data da consulta/impressão), envio de convites, convocações, boletins e informativos;
- Possibilitar acesso online via internet que permita participação remota dos membros dos Órgãos de governança em votação à distância; e
- Possuir ferramenta que disponibilize a inclusão de anotações, com possibilidade de compartilhamento dessas anotações com os demais membros dos Órgãos colegiados.
- Possuir Assinatura eletrônica em documentos (certificada com validade jurídica).
- Possuir Projetos com visualização em Lista, Kanban e Gantt.
- Possuir a utilização de Inteligência Artificial nas reuniões e monitoramento das ações no Portal.

PARÁGRAFO QUARTO - **Requisitos de Segurança:** A solução deve atender requisitos de segurança da informação, tais como:

- Funcionar em arquitetura de segurança, composto por criptografia, firewalls, sistemas de prevenção de invasões e demais práticas usualmente adotadas, para oferecer segurança e integridade do ambiente em geral, inclusive da documentação armazenada.
- As informações processadas, armazenadas e transmitidas devem ser protegidas com uso de algoritmos públicos de criptografia, preferivelmente com a adoção de chaves criptográficas assimétricas.
- Possuir atribuição de diferentes níveis de acesso de acordo com perfil de usuário e aplicável aos colegiados aos quais o usuário tenha acesso.
- Possuir trilha de auditoria e rastreamento do histórico de acesso de usuários.
- Possuir autenticação por dois fatores distintos.
- Possuir ambiente personalizado, incluindo elementos gráficos do **CONTRATANTE;**
- Possuir uma base própria de credenciais que possibilite o **CONTRATANTE** extrair de forma estruturada e automatizada a lista de usuários com acesso, com vistas a promover a revisão periódica pelo gestor do serviço.
- Ter mecanismo de proteção contra-ataques por força bruta (captcha ou delay progressivo na autenticação ou análogo).
- Possibilitar o **CONTRATANTE** acesso às trilhas de auditoria do serviço.

- Possibilitar o **CONTRATANTE** acesso a dados de reunião armazenados (pauta, itens, resultado de votação).
- Prover meios para a exportação dos dados do **CONTRATANTE, com vistas a** promover a continuidade dos processos de negócio do **CONTRATANTE,** permitindo a migração de informações para outra solução ou outro provedor de serviços.
- Somente os usuários do **CONTRATANTE** podem acessar os dados armazenados na ferramenta.

PARÁGRAFO QUINTO - Tratamento de incidentes de segurança da informação:

- Backup e recuperação de dados;
- Bloqueio de acessos
- Destruição de informação;
- Planos de contingência para garantir a continuidade do serviço em caso de incidentes;
- Execução de testes de penetração ou levantamento de vulnerabilidades na sua infraestrutura de TI.
- Disponibilizar procedimentos e os contatos (telefones e e-mails) para acionamento pelo **CONTRATANTE** em caso de incidentes de segurança.

DOS REQUISITOS DA CONTRATAÇÃO

CLÁUSULA QUARTA - Conforme a **Cláusula Terceira** e **Anexo II** deste Contrato, estão garantidos os requisitos de integração, assim como, os requisitos funcionais:

PARÁGRAFO PRIMEIRO - No valor pago pelas Licenças estão inclusos os treinamentos, suporte e manutenção da ferramenta. A solução contratada possui de armazenamento em "cloud object storages" dos principais “datacenter” de nuvem pública ou privada obrigatoriamente localizada em território nacional, conforme norma do governo federal 14/IN01/DSIC/SCS/GSIPR, como exemplos: amazon s3, microsoft azure ou google cloud, ou outro player compatível com a norma. Assim como, possui estrutura tecnológica compatível com ambiente Windows, MacOS, iOS e Android.

PARÁGRAFO SEGUNDO - A solução atende aos requisitos de segurança da informação, tais como:

- Funcionar em arquitetura de segurança, composto por criptografia, firewalls, sistemas de prevenção de invasões e demais práticas usualmente adotadas, para oferecer segurança e integridade do ambiente em geral, inclusive da documentação armazenada.
- As informações processadas, armazenadas e transmitidas devem ser protegidas com uso de algoritmos públicos de criptografia, preferivelmente com a adoção de chaves criptográficas assimétricas.
- Possuir atribuição de diferentes níveis de acesso de acordo com perfil de usuário e aplicável aos colegiados aos quais o usuário tenha acesso.
- Possuir trilha de auditoria e rastreamento do histórico de acesso de usuários.
- Possuir autenticação por dois fatores distintos.
- Possuir ambiente personalizado, incluindo elementos gráficos do **CONTRATANTE.**
- Possuir uma base própria de credenciais que possibilite o **CONTRATANTE** extrair de forma estruturada e automatizada a lista de usuários com acesso, com vistas a promover a revisão periódica pelo gestor do serviço.
- Ter mecanismo de proteção contra-ataques por força bruta (captcha ou delay progressivo na autenticação ou análogo).
- Possibilitar o **CONTRATANTE** acesso às trilhas de auditoria do serviço.

- Possibilitar o **CONTRATANTE** acesso a dados de reunião armazenados (pauta, itens, resultado de votação).
- Prover meios para a exportação dos dados do **CONTRATANTE**, com vistas a promover a continuidade dos processos de negócio do Banco, permitindo a migração de informações para outra solução ou outro provedor de serviços.
- Somente os usuários do **CONTRATANTE** podem acessar os dados armazenados na ferramenta.

PARÁGRAFO TERCEIRO - A solução dispõe de tratamento de incidentes de segurança da informação conforme **Parágrafo Quinto** da **Cláusula Terceira** deste Contrato:

- Backup e recuperação de dados;
- Bloqueio de acessos;
- Destruição de informação;
- Planos de contingência para garantir a continuidade do serviço em caso de incidentes;
- Execução de testes de penetração ou levantamento de vulnerabilidades na sua infraestrutura de TI.
- Disponibilizar procedimentos e os contatos (telefones e e-mails) para acionamento pelo **CONTRATANTE** em caso de incidentes de segurança

DA DEDICAÇÃO EXCLUSIVA COM OU SEM MÃO DE OBRA

CLÁUSULA QUINTA - Esta contratação não possui dedicação exclusiva de mão de Obra.

PREÇO

CLÁUSULA SEXTA - O **CONTRATANTE** pagará à **CONTRATADA**, pelo objeto da Cláusula Primeira deste Contrato, o Valor Unitário de cada Licença contratada **R$2.584,38** (dois mil, quinhentos e oitenta e quatro reais e trinta e oito centavos), resultando no Valor Total Anual **R$77.531,40** (setenta e sete mil, quinhentos e trinta e um reais e quarenta centavos), de acordo com a proposta técnica comercial – **Anexo IV** deste Contrato da **CONTRATADA** datada de 28/02/2025:

Descrição do serviço	Quantidade	Valor Unitário (R$)	Valor Anual (R$)
Plano Enterprise	30	2.584,38	77.531,40

PARÁGRAFO ÚNICO - O valor indicado no caput desta Cláusula inclui todos os impostos, taxas, fretes, etc, que incidam sobre a contratação.

DO PAGAMENTO

CLÁUSULA SÉTIMA – O pagamento será efetuado no prazo de até 30 (trinta) dias úteis, contados a partir da emissão do termo de recebimento definitivo, emitido pelo Fiscal do Contrato. O referido termo deve atestar o recebimento do serviço e/ou bem, o cumprimento do disposto nos itens abaixo, além de expressamente autorizar a emissão da nota fiscal, por meio de crédito na **Conta Corrente nº 93377-5, Agência 9337, Banco Itáu (341)**, de titularidade da **CONTRATADA**.

PARÁGRAFO PRIMEIRO - Notas Fiscais emitidas após o 25° do mês subsequente a prestação do serviço e/ou entrega do bem não serão aceitas pelo contratante, devendo o contratado emiti-las a partir do 1° dia útil do mês seguinte.

PARÁGRAFO SEGUNDO - Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na Legislação vigente.

PARÁGRAFO TERCEIRO - A **CONTRATADA** regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

PARÁGRAFO QUARTO - Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 30 (trinta) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

PARÁGRAFO QUINTO - Para fins de liquidação, o fiscal técnico deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- O prazo de validade;
- A data da emissão;
- Os dados do Contrato e do **CONTRATANTE**;
- O período respectivo de execução do Contrato.
- O valor a pagar; e eventual destaque do valor de retenções tributárias cabíveis.

PARÁGRAFO SEXTO - Caso a **CONTRATADA** opte pelo recebimento do pagamento em conta corrente mantida em outra instituição financeira, lhe será cobrado o valor da tarifa TED, correspondente ao da tabela de tarifas e serviços do banco, sendo que esse valor será de responsabilidade da **CONTRATADA** e deduzido do valor do crédito a ser enviado.

PARÁGRAFO SÉTIMO - Os pagamentos serão automaticamente transferidos para os dias úteis subsequentes, caso não haja expediente no banco nas datas previstas para tal.

PARÁGRAFO OITAVO - Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao **CONTRATANTE**.

PARÁGRAFO NONO - No caso de atraso pelo **CONTRATANTE**, os valores devidos a **CONTRATADA** serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA/IBGE de correção monetária.

PARÁGRAFO DÉCIMO - A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, social e trabalhista, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação estabelecida na contratação.

PARÁGRAFO DÉCIMO PRIMEIRO - O **CONTRATANTE** deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no termo de referência; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

PARÁGRAFO DÉCIMO SEGUNDO - Constatando-se, junto ao SICAF, a situação de irregularidade da **CONTRATADA**, será providenciada pelo Fiscal Técnico do Contrato a sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do **CONTRATANTE.**

PARÁGRAFO DÉCIMO TERCEIRO - Não havendo regularização ou sendo a defesa considerada improcedente, o **CONTRATANTE** deverá comunicar aos Órgãos responsáveis pela Fiscalização da regularidade fiscal quanto à inadimplência da **CONTRATADA**, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

PARÁGRAFO DÉCIMO QUARTO - Persistindo a irregularidade, o **CONTRATANTE** deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

PARÁGRAFO DÉCIMO QUINTO - Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso a **CONTRATADA** não regularize sua situação junto ao SICAF.

PARÁGRAFO DÉCIMO SEXTO - Para efeito de pagamento, a **CONTRATADA** deverá apresentar juntamente com as notas fiscais/faturas discriminativas os documentos a seguir relacionados, caso não estejam disponíveis no Cadastro Único de Fornecedores (SICAF):

a) Certidão negativa ou positiva com efeitos de negativa de débitos, conjunta, relativos aos tributos federais e à **Dívida Ativa da União** e INSS;

b) Certidão negativa de débitos ou positiva com efeitos de negativa das Fazendas **Estadual e Municipal** de seu domicílio ou sede;

c) Certidão de regularidade do **FGTS (CRF);**

d) Certidão Negativa de Débitos Trabalhistas – **CNDT;**

e) Declaração do **Simples Nacional**, caso seja optante.

DA RUBRICA ORÇAMENTÁRIA

CLÁUSULA OITAVA - Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto desta contratação estão previstos no orçamento do **CONTRATANTE**, na rubrica: **27.065-2 - "LICENÇA DE USO"**.

DAS CONDIÇÕES DE REAJUSTE DE PREÇOS

CLÁUSULA NONA - Os preços serão reajustados com o intervalo mínimo de 01 (um) ano, a contar da data limite para a apresentação da proposta ou da data do orçamento a que a proposta se referir, pelo índice ICTI/IPEA, apurado no período.

PARÁGRAFO ÚNICO - Os reajustes subsequentes observarão o interregno mínimo de 01 (um) ano a contar da data base de reajuste do ano anterior.

DA GARANTIA DO CONTRATO

CLÁUSULA DÉCIMA - Por tratar-se de serviço de pronta entrega não será exigida garantia contractual.

DA VIGÊNCIA

CLÁUSULA DÉCIMA PRIMEIRA – O Contrato terá o prazo de vigência de 01 (um) ano contados a partir da data de sua assinatura, sem possibilidade de prorrogação.

DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA DÉCIMA SEGUNDA - São obrigações da **CONTRATADA:**

I) Executar o objeto do Contrato de acordo com todos os termos estabelecidos neste Contrato e demais documentos que amparam a contratação;

II) Obedecer rigorosamente a todos os prazos contratados;

III) Prestar os esclarecimentos que forem solicitados pelo **CONTRATANTE** e atender prontamente a eventuais solicitações/reclamações;

IV) Dispor-se a toda e qualquer Fiscalização do **CONTRATANTE**, no tocante ao cumprimento dos serviços e prazos contratados;

V) Prover todos os meios necessários à garantia da plena operacionalidade dos bens e serviços objeto do Contrato;

VI) Manter absoluto sigilo sobre todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados que venham a ser disponibilizados pelo **CONTRATANTE** à **CONTRATADA**, em razão da execução dos serviços contratados;

VII) Exercer suas atividades em conformidade com a Legislação vigente;

VIII) Não se utilizar direta ou indiretamente, por meio de seus fornecedores de produtos e serviços, de trabalho ilegal e/ou análogo ao escravo;

IX) Não se utilizar de práticas de discriminação negativa e limitativa para o acesso e manutenção do emprego, tais como por motivo de sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar, estado gravídico, etc;

X) Proteger e preservar o meio ambiente, prevenindo práticas danosas e executando seus serviços em observância à Legislação vigente, principalmente no que se refere aos crimes ambientais;

XI) Providenciar a correção das deficiências apontadas pelo **CONTRATANTE**, quanto ao objeto do Contrato, conforme SLA da **CONTRATADA**.

XII) A **CONTRATADA** será responsável pelos danos de qualquer natureza que acarretar ao **CONTRATANTE** ou a terceiros em decorrência de negligência, imperícia ou imprudência por parte de seus empregados ou Prepostos, na administração e execução dos serviços contratados, desde que devidamente comprovado.

DAS OBRIGAÇÕES DO CONTRATANTE

CLÁUSULA DÉCIMA TERCEIRA – São obrigações do **CONTRATANTE**:

I) Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com as Cláusulas contratuais e os termos de sua proposta;

II) Exercer a Fiscalização dos serviços por empregados especialmente designados, na forma prevista na Lei nº 13.303/2016 e Art. 99 do Regulamento do **CONTRATANTE**;

III) Atestar através do Fiscal Técnico do Contrato as Notas Fiscais/ Fatura de Serviços correspondentes às etapas executadas, após a verificação da conformidade dos serviços, para efeito de pagamento**.**

IV) Rejeitar, no todo ou em parte, os serviços executados em desacordo com as respectivas especificações.

V) Efetuar o pagamento da Nota Fiscal/Fatura emitida pela **CONTRATADA**, desde que receba com antecedência mínima de 30 (trinta) dias do vencimento daquela Nota Fiscal/Fatura e que a realização dos serviços esteja devidamente comprovada pelo setor competente e de acordo com o requerido neste Contrato.

VI) Promover a infraestrutura necessária à prestação dos serviços, incluindo instalações sanitárias, vestiários com armários guarda-roupas, local para guarda dos materiais, equipamentos, ferramentas e utensílios e outras que se apresentarem necessárias.

VII) Receber o Preposto da **CONTRATADA**, devidamente identificados, devendo tomar as providências administrativas que garantam o livre desempenho de suas atividades.

VIII) Cuidar para que os empregados da **CONTRATADA** somente recebam ordens para a execução de tarefas, do Preposto da **CONTRATADA**.

IX) Notificar a **CONTRATADA**, por escrito, da aplicação de eventuais penalidades ou acerca de falhas ou irregularidades encontradas na execução dos serviços, fixando-lhe prazo para corrigi-las.

DAS SANÇÕES ADMINISTRATIVAS

CLÁUSULA DÉCIMA QUARTA - Pela inexecução total ou parcial do objeto deste Contrato, o **CONTRATANTE** poderá, garantido o contraditório e a ampla defesa, sem prejuízo das demais cominações do Contrato, aplicar as penalidades previstas na Lei nº 13.303/16:

I. Advertência;

II. Multa de 10% (dez por cento) sobre o valor global da contratação, pela inexecução total do ajuste;

III. Multa diária de 0,2% (dois décimos por cento), calculado sobre o valor da respectiva fatura, quando houver atraso prestação dos serviços, enquanto perdurar o inadimplemento;

IV. Suspensão do direito de licitar e de contratar com o **CONTRATANTE** pelo prazo de até 02 (dois) anos.

PARÁGRAFO PRIMEIRO - O atraso na entrega do produto superior a 30 (trinta) dias consecutivos, poderá ensejar, a exclusivo critério do **CONTRATANTE**, a rescisão do Contrato.

PARÁGRAFO SEGUNDO – A rescisão do Contrato provocada pela **CONTRATADA** implicará, de pleno direito a cobrança pelo **CONTRATANTE**, de multa equivalente a 10% (dez por cento) do valor total contratado.

PARÁGRAFO TERCEIRO – Nenhuma penalidade será aplicada pelo **CONTRATANTE** sem o devido processo administrativo, assegurado o contraditório e a ampla defesa, no prazo de 10 (dez) dias úteis.

PARÁGRAFO QUARTO – A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e sua cobrança, facultada a defesa prévia, não isentará a obrigação de indenizar eventuais perdas e danos.

PARÁGRAFO QUINTO – O valor das multas apurado, após o processo administrativo, será descontado dos pagamentos eventualmente devidos pelo **CONTRANTE**.

PARÁGRAFO SEXTO - Inexistindo pagamento devido pelo **CONTRATANTE,** ou sendo este insuficiente, caberá a parte contrária efetuar o pagamento do que for devido, no prazo máximo de 10 (dez) dias consecutivos, contados da data de sua comunicação de confirmação da multa, em depósito em conta corrente própria em nome do **CONTRATANTE**.

PARÁGRAFO SÉTIMO - Em não se realizando o pagamento nos termos definidos no Parágrafo acima, far-se-á a sua cobrança judicialmente.

DA RESCISÃO

CLÁUSULA DÉCIMA QUINTA - A rescisão do Contrato poderá ocorrer nas seguintes hipóteses:

I- Mediante distrato, pela inexecução parcial ou total do Contrato;

II- Amigavelmente, por acordo entre as partes, desde que haja conveniência para a Administração, precedida de autorização escrita e fundamentada, mediante aviso prévio por escrito, de 30 (trinta) dias consecutivos;

III- Judicialmente, nos termos da Legislação.

PARÁGRAFO PRIMEIRO - Sem prejuízo de outras Sanções, constituem motivos para rescisão por justa causa deste Contrato, pelo **CONTRATANTE** as situações descritas nos subitens abaixo:

a. Paralisação injustificada dos serviços;

b. O não cumprimento de Cláusulas contratuais, especificações ou prazos;

c. A subcontratação, ainda que parcial, dos serviços objeto do Contrato;

d. A cessão ou transferência do contrato;

e. O desatendimento às determinações da FISCALIZAÇÃO designada para acompanhar e fiscalizar a execução dos serviços;

f. O cometimento reiterado de faltas na execução dos serviços;

g. A decretação de falência, o pedido de recuperação judicial ou extrajudicial;

h. A dissolução da sociedade.

i. A alteração societária que modifique a finalidade ou o controle acionário ou, ainda, a estrutura da **CONTRATADA** que, a juízo da **CONTRATANTE**, inviabilize ou prejudique a execução deste Contrato;

j. A prática de qualquer ato que vise fraudar ou burlar o fisco ou órgão/entidade arrecadador/credor dos encargos sociais e trabalhistas ou de tributos;

k. O descumprimento de quaisquer das condições ajustadas neste Contrato;

l. A utilização pela **CONTRATADA** de mão-de-obra de menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendizes, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do art. 7º da Constituição Federal (Emenda Constitucional nº 20, de 1998);

m. O conhecimento, ainda que, "a posteriori", de fato ou ato que afete a idoneidade da **CONTRATADA** ou de seus sócios/cotistas ou de seus gestores ou ainda de seus representantes;

n. Razões de interesse público;

o. Ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditivo da execução deste Contrato;

p. Deixar de comprovar sua regularidade fiscal, trabalhista, inclusive contribuições previdenciárias e depósitos de FGTS para com seus empregados;

q. Utilizar em benefício próprio ou de terceiras informações sigilosas ás quais tenha acesso por força de suas atribuições.

PARÁGRAFO SEGUNDO - O **CONTRATANTE** poderá, a qualquer tempo, mediante aviso com antecedência mínima de 90 (noventa) dias, denunciar o Contrato, para efeito de rescisão, sem que, por esse motivo, seja obrigado a suportar ônus de indenização, multa ou pagamento extra de qualquer natureza, salvo previsão em Lei.

PARÁGRAFO TERCEIRO – Na rescisão deste Contrato, o **CONTRATANTE** aplicará a multa rescisória prevista no **Parágrafo Segundo** da **Cláusula Décima Quarta** deste Contrato, reservando-se, ainda, o direito de intentar ação judicial para indenização por perdas e danos.

PARÁGRAFO QUARTO – O descumprimento total ou parcial de qualquer das obrigações ora assumidas sujeitará a **CONTRATADA** às sanções previstas na Lei nº 13.303/2016, garantida a prévia e ampla defesa em processo administrativo.

PARÁGRAFO QUINTO - Também poderá ocorrer rescisão quando:

a. Deixar de comprovar sua regularidade, trabalhista, fiscal, inclusive contribuições previdenciárias e depósitos do FGTS dos seus funcionários;

b. Vier a ser declarada inidônea por qualquer órgão da Administração Pública;

c. Vier a ser atingida por protesto de título, execução fiscal ou outros fatos que comprometam a sua capacidade econômico-financeira;

d. Utilizar em benefício próprio ou de terceiros, informações sigilosas às quais tenha acesso por força de suas atribuições contratuais.

PARÁGRAFO SEXTO - A rescisão acarretará, de imediato, retenção dos créditos decorrentes deste Contrato, até o limite dos prejuízos causados ao **CONTRATANTE.**

PARÁGRAFO SÉTIMO - Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados à **CONTRATADA** o contraditório e o direito à ampla defesa.

PARÁGRAFO OITAVO - Na rescisão do Contrato, o **CONTRATANTE** aplicará à **CONTRATADA** multa prevista neste Contrato.

PARÁGRAFO NONO - As responsabilidades imputadas à **CONTRATADA,** por danos diretos decorrentes de ações delitivas perpetradas contra o **CONTRATANTE,** não cessam com a rescisão deste Contrato**.**

DA HABILITAÇÃO

CLÁUSULA DÉCIMA SEXTA - A **CONTRATADA** também se obriga a manter, durante a vigência deste Contrato, todas as condições de habilitação exigidas na contratação, inclusive a condição de não empregar menor, exceto na condição de aprendiz, a partir de 14 (quatorze anos). Assume, ainda, a obrigação de apresentar, no término do prazo de validade de cada documento, os seguintes comprovantes atualizados:

a) Os comprovantes de regularidade de situação junto às Fazendas: **Estadual** e **Municipal** de seu domicílio ou sede;

b) A certidão emitida pela Receita Federal negativa ou positiva com efeitos de negativa de débitos relativos aos tributos federais, inclusive as contribuições previdenciárias, e à **dívida ativa da União**;

c) O certificado de regularidade perante o **FGTS -** Fundo de Garantia do Tempo de Serviço, mediante apresentação do CRF - Certificado de Regularidade de Fundo de Garantia;

d) A certidão negativa ou positiva com efeitos de negativa de débitos trabalhistas (**CNDT)**.

PARÁGRAFO ÚNICO - A não apresentação dos comprovantes citados acima poderá ensejar, a critério do **CONTRATANTE,** exceto quando os comprovantes estiverem disponíveis no Cadastro Único de Fornecedores (SICAF), a rescisão do Contrato a ser assinado, sem que caiba à outra parte qualquer direito de indenização.

DA VEDAÇÃO

CLÁUSULA DÉCIMA SÉTIMA - O presente instrumento não poderá ser, no todo ou em parte, objeto de cessão ou transferência.

PARÁGRAFO PRIMEIRO – É vedado à **CONTRATADA**, salvo se estiver expressamente autorizada pelo **CONTRATANTE:**

a) Veicular publicidade que tenha como apelo mercadológico o fato de ter prestado ou estar prestando serviços ao **CONTRATANTE**, ou qualquer outra informação acerca das atividades e programas do **CONTRATANTE**;

b) Utilizar o presente Contrato como garantia perante terceiros ou cessão dos direitos creditícios em operações de desconto bancário;

c) Usar, copiar, duplicar ou de alguma outra forma reproduzir ou reter quaisquer informações do **CONTRATANTE**.

PARÁGRAFO SEGUNDO - Nos termos do Art. 7º do Decreto nº 7.203, de 04.06.2010, que dispõe sobre a vedação de nepotismo no âmbito da Administração Pública Federal, também é vedado à **CONTRATADA** utilizar, durante toda a vigência do Contrato, mão de obra de cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o 3º (terceiro) grau, de empregado do **CONTRATANTE** que exerça cargo em comissão ou função de confiança.

PARÁGRAFO TERCEIRO - A **CONTRATADA** encaminhará a Declaração de Teor de conhecimento, do Decreto nº 7.203/2010.

DA ALTERAÇÃO DO CONTRATO

CLÁUSULA DÉCIMA OITAVA - A alteração incidente sobre o objeto do Contrato deve ser consensual e pode ser quantitativa, quando importa acréscimo ou diminuição do objeto do Contrato, ou qualitativa, quando a alteração diz respeito a características e especificações técnicas do objeto do Contrato.

PARÁGRAFO PRIMEIRO - A alteração quantitativa sujeita-se aos limites previstos nos § 1º e 2º do Artigo 81 da Lei nº 13.303/2016, devendo observar o seguinte:

a) A aplicação dos limites deve ser realizada separadamente para os acréscimos e para as supressões, sem que haja compensação entre os mesmos;

b) Deve ser mantida a diferença, em percentual, entre o valor global do Contrato e o valor orçado pelo **CONTRATANTE**.

PARÁGRAFO SEGUNDO - Excepcionalmente a alteração qualitativa não se sujeitará aos limites previstos nos § 1º e 2º do Artigo 81 da Lei n. 13.303/2016, desde que observe os seguintes pressupostos:

a) Os encargos decorrentes da continuidade do Contrato devem ser inferiores aos da rescisão contratual e aos da realização de um novo procedimento licitatório;

b) As consequências da rescisão contratual, seguida de nova licitação e contratação, devem importar prejuízo relevante ao interesse coletivo a ser atendido pela obra ou pelo serviço;

c) As mudanças devem ser necessárias ao alcance do objetivo original do Contrato, à otimização do cronograma de execução e à antecipação dos benefícios sociais e econômicos decorrentes;

d) A capacidade técnica e econômico-financeira da **CONTRATADA** deve ser compatível com a qualidade e a dimensão do objeto contratual aditado;

e) A motivação da mudança contratual deve ter decorrido de fatores supervenientes não previstos e que não configurem burla ao processo licitatório;

f) A alteração não deve ocasionar a transfiguração do objeto originalmente contratado em outro de natureza ou propósito diverso.

PARÁGRAFO TERCEIRO - As alterações incidentes sobre o objeto devem ser:

a) Instruídas com memória de cálculo e justificativas de competência do Fiscal Técnico e do Fiscal Administrativo do **CONTRATANTE**, que devem avaliar os seus pressupostos e condições e, quando for o caso, calcular os limites;

b) As justificativas devem ser ratificadas pelo gestor do Serviço **CONTRATANTE;**

c) Submetidas à área jurídica e, quando for o caso, à área financeira do **CONTRATANTE.**

PARÁGRAFO QUARTO - As alterações contratuais incidentes sobre o objeto e as decorrentes de revisão contratual devem ser formalizadas pôr termo aditivo firmado pela mesma autoridade que firmou o Contrato, devendo o extrato do termo aditivo ser publicado no sítio eletrônico do **CONTRATANTE.**

PARÁGRAFO QUINTO - Não caracterizam alteração do Contrato e podem ser registrados por termo de apostilamento, dispensando a celebração de termo aditivo:

a) A variação do valor contratual para fazer face ao reajuste de preços;

b) As atualizações, as compensações ou as penalizações financeiras decorrentes das condições de pagamento previstas no Contrato;

c) Acorreção de erro material havido no instrumento de Contrato;

d) As alterações na razão ou na denominação social da **CONTRATADA.**

DA GESTÃO E DA FISCALIZAÇÃO DO CONTRATO

CLÁUSULA DÉCIMA NONA – A Fiscalização do fornecimento das Licenças, objeto desta contratação será realizada pela Secretaria Executiva de Governança, Marketing e Comunicação – SECRE/COADI II, que designará representante do **CONTRATANTE** para o acompanhamento e Fiscalização do cumprimento das obrigações previstas neste Contrato.

PARÁGRAFO PRIMEIRO - O acompanhamento e a Fiscalização da execução do Contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o cumprimento do ajuste, e serão exercidos por um ou mais representantes do **CONTRATANTE.**

PARÁGRAFO SEGUNDO - A verificação da adequação do fornecimento das Licenças deverá ser realizada com base nos critérios previstos neste Contrato e na proposta.

PARÁGRAFO TERCEIRO - Os contatos entre o **CONTRATANTE** e a **CONTRATADA** serão mantidos por intermédio da Fiscalização do **CONTRATANTE**.

PARÁGRAFO QUARTO - A comunicação formal entre a Fiscalização e a **CONTRATADA**, e vice-versa, devem serem realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim e os documentos gerados constarão dos autos do processo.

PARÁGRAFO QUINTO - Após a assinatura do contrato ou instrumento equivalente, o **CONTRATANTE** poderá convocar o representante da **CONTRATADA** para reunião inicial para apresentação do plano de Fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

PARÁGRAFO SEXTO - Fiscalização: A execução do Contrato deverá ser acompanhada e fiscalizada pelo (s) fiscal (is) do Contrato, ou pelos respectivos substitutos.

PARÁGRAFO SÉTIMO - Fiscalização Técnica:

- O Fiscal Técnico do Contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no Contrato, de modo a assegurar os melhores resultados para a Administração;

- O Fiscal Técnico do Contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

- Identificada qualquer inexatidão ou irregularidade, o Fiscal Técnico do Contrato emitirá notificações para a correção da execução do Contrato, determinando prazo para a correção.

- O Fiscal Técnico do Contrato informará ao Gestor do serviço, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

- O Fiscal Técnico do Contrato comunicará ao Gestor do serviço, em tempo hábil, o término do Contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

PARÁGRAFO OITAVO - Fiscalização Administrativa:

- O Fiscal Administrativo do Contrato verificará a manutenção das condições de habilitação da **CONTRATADA**.

- Caso ocorra descumprimento das obrigações administrativas contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do serviço para que tome as providências cabíveis, quando ultrapassar a sua competência;

- Receber o objeto contratado, provisoriamente, no ato da entrega, para efeito de posterior verificação do funcionamento e da conformidade dos softwares com as especificações contratadas;

- Efetuar o pagamento à **CONTRATADA**, de acordo com a forma e prazos estabelecidos;

- Testar o recebimento definitivo do objeto contratado, condicionado à observância de todas as Cláusulas e condições fixadas neste instrumento, bem como ao atendimento de eventuais substituições do software, entregue fora das especificações ou no qual venham a ser detectados defeitos, irregularidades ou imperfeições;

- Atestar o recebimento definitivo do objeto contratado, condicionado à observância de todas as Cláusulas e condições fixadas neste instrumento, bem como ao atendimento de eventuais substituições do software, entregue fora das especificações ou no qual venham a ser detectados defeitos, irregularidades ou imperfeições;

- Designar fiscal ou comissão para acompanhar a execução do Contrato e responsabilizar-se pela atestação das faturas; orientar e supervisionar a observância, pela **CONTRATADA**, dos regulamentos administrativos e dos procedimentos de segurança do **CONTRATANTE**;
- Restituir a garantia após o cumprimento integral de todas as obrigações contratuais assumidas pela **CONTRATADA**.

PARÁGRAFO NONO - **Gestor do Serviço:**

a) O Gestor do serviço coordenará a atualização do processo de acompanhamento e Fiscalização do Contrato contendo todos os registros formais da execução no histórico de gerenciamento do Contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

b) O Gestor do serviço acompanhará os registros realizados pelos fiscais do Contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

c) O Gestor do serviço acompanhará a manutenção das condições de habilitação da **CONTRATADA**, para fins de pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

d) O Gestor do serviço emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e negócios quanto ao cumprimento de obrigações assumidas pela **CONTRATADA**, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

e) O Gestor do serviço tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela área competente para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

f) O Gestor do serviço deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração**.**

g) O Gestor do serviço deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela Fiscalização e gestão nos termos do Contrato

PARÁGRAFO DÉCIMO – A ausência ou omissão da Fiscalização do **CONTRATANTE** não eximirá a **CONTRATADA** das responsabilidades previstas neste Contrato.

DOS CRITÉRIOS DE SUSTENTABILIDADE

CLÁUSULA VIGÉSIMA - A **CONTRATADA** se compromete a atender às diretrizes da Política de Responsabilidade Socioambiental do Banco da Amazônia – PRSAC, disponível em https://www.bancoamazonia.com.br/component/edocman/prsac/viewdocument/5204 e a Política Geral de Contratações, disponível em: https://www.bancoamazonia.com.br/component/edocman/licitacoes-contratos/politica-geral-de-contratacoes/2022/politica-geral-de-contratacoes, considerando os requisitos a seguir:

- Não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;
- Não empregar menores de 18 anos para trabalho noturno, perigoso ou insalubre, e menores de dezesseis anos para qualquer trabalho, com exceção a categoria de Menor Aprendiz;

- Não permitir a prática ou a manutenção de discriminação limitativa ao acesso na relação de emprego, ou negativa com relação a sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar ou estado gravídico, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;
- Respeitar o direito de formar ou associar-se a sindicatos, bem como negociar coletivamente, assegurando que não haja represálias;
- Proteger e preservar o meio ambiente, bem como buscar prevenir e erradicar práticas que lhe sejam danosas, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos às áreas de meio ambiente, emanadas das esferas federal, estaduais e municipais e implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;
- Desenvolver suas atividades em cumprimento à legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como às Normas Regulamentadoras de saúde e segurança ocupacional e demais dispositivos legais relacionados a proteção dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se: a) “Condições ultrajantes”: condições que expõe o indivíduo de forma ofensiva, insultante, imoral ou que fere ou afronta os princípios ou interesses normais, de bom senso, do indivíduo. b) “Condições sub-humanas”: tudo que está abaixo da condição humana como condição de degradação, condição de degradação abaixo dos limites do que pode ser considerado humano, situação abaixo da linha da pobreza.
- Condições degradantes de trabalho”: condições que expõe o indivíduo à humilhação, degradação, privação de graus, títulos, dignidades, desonra, negação de direitos inerentes à cidadania ou que o condicione à situação de semelhante à escravidão;
- Atender à Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), observando quanto ao descarte adequado e ecologicamente correto;
- Apresentar conformidade com a legislação e regulamentos que disciplinam sobre a prevenção e combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo;
- Não ter sofrido sanções que implicam na restrição de participar de licitações ou de celebrar contratos com a Administração Pública, não constar registro da empresa e/ou sócios e representantes no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), atendendo às diretrizes anticorrupção;
- Adotar práticas e métodos voltados para a preservação da confidencialidade e integridade, atentando à Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018.
- O **CONTRATANTE** poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir imediatamente o contrato, sem qualquer custo, ônus ou penalidade, garantida a prévia defesa, caso se comprove que a **CONTRATADA**, subcontratados ou fornecedores utilizam-se de trabalho em desconformidade com as condições referidas nas Cláusulas supracitadas

DA MATRIZ DE RISCO

CLÁUSULA VIGÉSIMA PRIMEIRA - A Matriz de Riscos consiste no documento que descrimina de forma clara e objetiva os riscos assumidos por cada uma das Partes na celebração deste Contrato e está disposto no **ANEXO III,** deste Contrato.

DA INTEGRIDADE, DA CONDUTA ÉTICA E DOS PROCEDIMENTOS ANTICORRUPÇÃO

CLÁUSULA VIGÉSIMA SEGUNDA - As Partes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa - Lei nº 8.429, de 02 de junho de 1992 e a Lei Anticorrupção - Lei nº 12.846, de 01 de Agosto de 2013 e seus regulamentos e se comprometem a cumpri-las fielmente, por si e porseus sócios, administradores e colaboradores, bem como exigir o seu cumprimento pelos terceiros por elas contratados. Adicionalmente, cada uma das Partes declara que tem e manterá até o final da vigência deste Contrato um código de ética e conduta próprio, cujas regras se obriga a cumprir fielmente. Sem prejuízo da obrigação de cumprimento dasdisposições de seus respectivos códigos de ética e conduta, ambas as Partes desde já se obrigam, no exercício dos direitos e obrigações previstos neste Contrato e no cumprimento de qualquer uma de suas disposições:

(i) Não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente;

(ii) Adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados.

(iii) Respeitar e exigir que seus empregados, envolvidos na prestação dos serviços ora contratados, respeitem, no que couber, os princípios éticos e os compromissos de conduta definidos no Código de Conduta Ética do BANCO DA AMAZÔNIA S.A, cujo teor poderá ser acessado no site da Instituição.

PARÁGRAFO PRIMEIRO – A comprovada violação de quaisquer das obrigações previstas nesta Cláusula é causa para a rescisão unilateral deste Contrato, sem prejuízo da cobrança das perdas e danos causados à parte inocente.

PARÁGRAFO SEGUNDO – A aplicação das sanções previstas na Lei n° 12.846/13 não afeta os processos de responsabilização e aplicação de penalidades decorrentes de atos ilícitos.

DA PROPRIEDADE INTELECTUAL

CLÁUSULA VIGÉSIMA TERCEIRA - Direitos sobre a Propriedade Intelectual. Este instrumento não concede a nenhuma das Partes quaisquer direitos sobre Propriedade Intelectual, implícitos ou de outra forma, a qualquer conteúdo da outra Parte, em especial às Informações Exclusivas e Informações Confidenciais.

CLÁUSULA VIGÉSIMA QUARTA - Titularidade. A **CONTRATADA** é a única detentora de todos os direitos de propriedade intelectual sobre o Software.

CLÁUSULA VIGÉSIMA QUINTA - Atos de lesão à Propriedade Intelectual. A **CONTRATANTE** não realizará os atos que se seguem, nem permitirá que terceiros sob seu controle os realizem, a saber: **(i)** Copiar, modificar, criar obra derivada, fazer engenharia reversa, descompilar, traduzir, desmontar, ou de outra forma tentar extrair quaisquer ou todos os códigos de fonte do Software; **(ii)** Utilizar o Software para praticar atos ilícitos ou que afetem direitos de terceiros, principalmente aos que se referem a Dados Pessoais; **(iii)** Utilizar o Software de maneira que impeça ou limite a atuação de outros Usuários; **(iv)** Acessar diretamente APIs ou automatizar a interface do sistema para realização de ações em lote ou para controlar programaticamente o sistema e demais recursos da Plataforma; **(v)** Desenvolver extensões ou modificações que alterem o comportamento original do Software; e **(vi)** Buscar ou explorar vulnerabilidades de segurança de forma não autorizada.

CLÁUSULA VIGÉSIMA SEXTA - Desenvolvimento a partir do Software. Caso a **CONTRATANTE** venha a desenvolver um novo módulo, função, atividade, prestação de serviço ou produto que caracterize cópia, no todo ou em parte, dos direitos de Propriedade Intelectual da **CONTRATADA**, inclusive do programa do Software, o referido módulo, função, atividade, prestação de serviço ou de produto, será considerado como sendo parte dos direitos de Propriedade Intelectual Software fornecido pela **CONTRATADA**, ficando, portanto, sua propriedade incorporada pela **CONTRATADA**, e seu uso condicionado. ao consentimento prévio por escrito da **CONTRATADA**.

CLÁUSULA VIGÉSIMA SÉTIMA - Prazo. As obrigações referentes à titularidade e aos direitos de Propriedade Intelectual da **CONTRATADA**, previstas neste Contrato, sobreviverão por tempo indeterminado ao término, extinção ou rescisão do presente instrumento e o **CONTRATANTE** indenizará a **CONTRATADA** por todas e quaisquer responsabilidades e custos, incluindo honorários de advogados, decorrentes de violação pelo **CONTRATANTE** de direitos de Propriedade Intelectual da **CONTRATADA**.

CLÁUSULA VIGÉSIMA OITAVA - Modificações. A **CONTRATADA** poderá realizar quaisquer modificações, alterações ou adaptações que se façam necessárias para o desenvolvimento do Software. Nenhuma destas modificações afetarão o desenvolvimento e funcionalidades da Plataforma.

DA LIMITAÇÃO DE RESPONSABILIDADE

CLÁUSULA VIGÉSIMA NONA - Estado do Software. O Software é fornecido pela **CONTRATADA** ao **CONTRATANTE** "no estado em que se encontra" e "conforme a disponibilidade".

CLÁUSULA TRIGÉSIMA - Atendimento integral. A **CONTRATADA** não garante que: **(i)** As funções contidas no Software atenderão às necessidades do **CONTRATANTE**; **(ii)** A operação do Software será ininterrupta ou livre de erros; e **(iii)** O Software será compatível ou funcione com qualquer outro software, aplicações ou serviços de terceiros.

CLÁUSULA TRIGÉSIMA PRIMEIRA - Limites. A **CONTRATADA** não será responsável por: **(i)** conteúdo armazenado em banco de dados pelo **CONTRATANTE** e seus Usuários; **(ii)** por danos ou prejuízos decorrentes de decisões administrativas, gerenciais ou comerciais tomadas com base nas informações fornecidas pelo Software; **(iii)** danos especiais, eventuais, imprevistos ou indiretos, pela perda de fundo de comércio ou de lucros cessantes, paralisação de trabalho, perda de dados, falha ou mau funcionamento do computador utilizado pelo **CONTRATANTE**; e **(iv)** hipóteses da **Cláusula Vigésima Quarta** deste Contrato.

CLÁUSULA TRIGÉSIMA SEGUNDA - Exclusão de Danos. Salvo quanto a danos resultantes do Uso e/ou divulgação não autorizados das Informações Exclusivas ou relacionados à Propriedade Intelectual, sob nenhuma circunstância a **CONTRATADA** ou o **CONTRATANTE** serão responsáveis entre si ou perante qualquer outra pessoa física ou jurídica por um valor de danos superiores à Remuneração anual paga.

CLÁUSULA TRIGÉSIMA TERCEIRA - Independência de Atos. Fica expressamente entendido e acordado que toda e qualquer disposição deste Contrato que trata de uma limitação de responsabilidade, exceção de garantias ou exclusão de danos será considerada pelas partes como sendo separada e independente de qualquer outra disposição e será cumprida como tal.

CLÁUSULA TRIGÉSIMA QUARTA - Alterações no Software. O **CONTRATANTE** reconhece que a **CONTRATADA** não se compromete ou se responsabiliza pela criação e estruturação de novas funcionalidades, bem como pela realização de customizações, desenvolvimentos e consultorias solicitadas pelo **CONTRATANTE**, independente do motivo que ensejou a solicitação.

CLÁUSULA TRIGÉSIMA QUINTA - Caso Fortuito ou de Força Maior. Nenhuma das Partes será responsável por falha ou atraso na execução deste Contrato, se causados por: ato de guerra, estado de sítio ou sabotagem; força maior, pandemia, falha de eletricidade, internet ou telecomunicação que não tenha sido causada pela parte obrigada; restrições governamentais (incluindo a negação ou cancelamento de qualquer exportação, importação, ou outra licença), ou outro evento fora do controle razoável da Parte obrigada.

DO FORO

CLÁUSULA TRIGÉSIMA SEXTA - Fica eleito o Foro de Belém, Capital do Estado do Pará, com renúncia a qualquer outro, por mais privilegiado que seja para dirimir as questões que porventura surgirem na execução do presente Contrato.

E por estarem de pleno acordo as Partes reconhecem e concordam expressamente que a inserção de sua senha pessoal e/ou a utilização de outras formas de assinatura eletrônica. Inclusive biométricas, em plataformas digitais, como a “DocuSign”, constitui forma legítima e suficiente para a confirmação de seus dados, comprovação de sua identidade e validade de sua declaração de vontade para assinar e celebrar o presente Contrato para que produza todos os seus efeitos de direito, conforme dispões e Legislação aplicável.

Belém-PA, data da última assinatura eletrônica.

BANCO DA AMAZÔNIA S.A.

Assinado por:
Bruna Eline da Silva Cavalcante
246C4EF61D234EA...

BRUNA ELINE DA SILVA CAVALCANTE
Gerente Executiva de Contratações e Gestão Administrativa de Contratos – GECOG

ATLAS GOVERNANCE TECNOLOGIA LTDA

Signed by:
Eduardo Shakir Carone
D5EA9DD9090F43F...

EDUARDO SHAKIR CARONE
Administrador

TESTEMUNHAS:

Nome: DocuSigned by:
Camila Sanches Mendes Lage
C45F183FCFF44F6...

Assinado por:
Alan Barros Costa
9F28051825B64F5...

ANEXO I

TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES

Este Termo de Compromisso é celebrado entre:

BANCO DA AMAZÔNIA, Endereço Avenida Presidente Vargas, nº 800, Belém/Pará, inscrito no CNPJ/MF 04.902.979/0001-44, neste ato representado pela sua Gerente Executiva de Contratações e Gestão Administrativa de Contratos - GECOG, Sra. **BRUNA ELINE DA SILVA CAVALCANTE,** brasileira, solteira, bancária, portadora da Carteira de Identidade Profissional nº 25700 OAB/PA e CPF/MF nº 796.223.562-49, abaixo assinado ("**CONTRATANTE**"), e a empresa empresa **ATLAS GOVERNANCE TECNOLOGIA LTDA**, sociedade unipessoal de responsabilidade limitada, com registro na Junta Comercial do Estado de Minas Gerais (JUCEMG) sob o NIRE nº 31.214.357.827, com sede em Nova Lima/MG, situada na Rua Ministro Orozimbo Nonato, n.º 102, Sala 2006, Bairro Vila da Serra, CEP 34006-053, inscrita no CNPJ sob o nº 25.462.636/0001-86, representada neste ato por seu Administrador, Sr. **EDUARDO SHAKIR CARONE,** brasileiro, casado, administrador de empresas, portador da CNH n° 01969555103 DETRAN/SP, inscrito no CPF/MF sob n° 295.344.578-17, abaixo assinado ("**CONTRATADA**"), **CONTRATANTE** e **CONTRATADA** em conjunto denominadas como Partes:

CONSIDERANDO QUE as Partes, por meio do Contrato nº 2025/135 estão estabelecendo uma relação jurídica para **contratação de empresa especializada, para a para aquisição de Licença não exclusiva de uso de Software, com o suporte e manutenção durante toda a vigência do Contrato para acesso ao Portal de Governança Corporativa do CONTRATANTE**, sendo que para serem executados, necessariamente incluem o acesso, o conhecimento e o tratamento de dados e informações corporativas da **CONTRATANTE** pela **CONTRATADA**, além do uso de equipamentos, de recursos computacionais e outros que envolvam a possibilidade de divulgação de informações restritas, de exclusivo interesse da **CONTRATANTE**, sob a posse, guarda e domínio da **CONTRATADA**;

CONSIDERANDO QUE as Partes podem divulgar entre si informações classificadas como restritas e/ou sigilosas, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios;

CONSIDERANDO QUE as Partes desejam ajustar as condições de revelação das Informações Restritas e/ou sigilosas, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as Partes celebrar o presente Termo de Compromisso e Sigilo de Dados e Informações ("Termo"), o qual se regerá pelas considerações acima, bem como, **pelas considerações que forem pertinentes constantes na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).**

1. OBJETO

Este Termo tem por objeto exclusivo proteger as Informações Confidenciais que venham a ser fornecidas ou reveladas pelo **CONTRATANTE** à **CONTRATADA**, bem como disciplinar a forma pela qual elas devem ser utilizadas pela **CONTRATADA**.

1.1. Todas as informações ou dados revelados ou fornecidos, direta ou indiretamente, pela **CONTRATANTE** ou por terceiros em nome desta à **CONTRATADA**, ou obtida por esta de forma lícita, independentemente de divulgação explícita, em quaisquer meios de armazenamento ou transmissão e independente do formato, rotulação ou forma de envio, devem ser tratadas como Informações Confidenciais.

1.2. A **CONTRATADA** reconhece que as Informações Confidenciais são de propriedade exclusiva do **CONTRATANTE** ou são advindas de terceiros e estão sob sua responsabilidade.
1.3. As Informações Confidenciais poderão estar contidas e serem transmitidas por quaisquer meios, incluindo, entre outros, as formas escritas, gráfica, verbal, mecânica, eletrônica, digital, magnética ou criptográfica.

2. RESTRIÇÕES QUANTO À UTILIZAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

2.1. A **CONTRATADA** reconhece a importância de se manter as Informações Confidenciais em segurança e sob sigilo, mesmo após o término de vigência do presente Termo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem prévia autorização do **CONTRATANTE**, a qualquer terceiro estranho a este Termo.

2.2. Sem prejuízo das demais obrigações previstas neste Termo, a **CONTRATADA** obriga-se a:

(i) Tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo **CONTRATANTE** e preservar o seu sigilo, de acordo com a Legislação vigente;

(ii) Preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo ou comercializar a terceiros;

(iii) Não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito;

(iv) Não copiar ou reproduzir, por qualquer meio ou modo: (a) informações classificadas em qualquer grau de sigilo; (b) informações relativas aos materiais de acesso restrito do **CONTRATANTE** salvo autorização da autoridade competente.

(v) Não utilizar, reter, duplicar modificar, adulterar, subtrair ou adicionar qualquer elemento das Informações Confidenciais que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo **CONTRATANTE** para finalidades específicas;

(vi) Não modificar ou adulterar as Informações Confidenciais fornecidas pelo **CONTRATANTE**, bem como a não subtrair ou adicionar qualquer elemento a essas Informações Confidenciais;

(vii) Armazenar e transmitir as Informações Confidenciais digitais em ambiente seguro, com controle de acesso e mediante o uso de criptografia;

(viii) Devolver ao **CONTRATANTE**, ou a exclusivo critério dessa destruir, todas as Informações Confidenciais que estejam em seu poder em até 48h (quarenta e oito horas), contados da data da solicitação; e

(ix) Informar imediatamente o **CONTRATANTE** qualquer violação a este Termo.

3. PROTEÇÃO DE DADOS PESSOAIS

3.1. A **CONTRATADA** obriga-se a, sempre que aplicável, atuar em conformidade com a Legislação vigente sobre proteção de dados relativos a uma pessoa física identificada ou identificável (“Dados Pessoais”) e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais”), bem como seguir as instruções informadas pelo **CONTRATANTE** quanto ao tratamento dos Dados Pessoais que teve acesso em função do presente Termo.

3.2. A **CONTRATADA** compromete-se a auxiliar o **CONTRATANTE**: i) com a suas obrigações judiciais ou administrativas, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e ii) no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas;
3.3. Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da relação estabelecida com o **CONTRATANTE** ou na execução das atividades ligadas a este Termo, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade da relação negocial conforme as disposições acordadas, a **CONTRATADA** concorda em notificar formalmente este fato o **CONTRATANTE**, que terá o direito de resolver a relação negocial sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.

3.4. **Agentes de Tratamento.** A **CONTRATADA** realizará o Tratamento de Dados Pessoais como Operadora, por meio da disponibilização do software, sendo o **CONTRATANT**E a responsável por estabelecer a finalidade, hipótese legal e os Dados Pessoais ("DP") que serão objeto de Tratamento, ou seja, a Controladora.

3.5. **Acesso e Processamento de Dados Pessoais:** A **CONTRATADA** declara que o presente Contrato tem por objeto o armazenamento e tratamento de informações corporativas relacionadas à estrutura de governança da Contratante, e que não possui acesso aos dados que porventura o **CONTRATANTE** venha a armazenar em banco de dados do Software, exceto aqueles necessários para o cadastro e acesso de usuários e envio de comunicações, quais sejam, **(i)** Nome; **(ii)** Correio Eletrônico – e-mail; e **(iii)** Telefone celular:

3.5.1 **Suspeita de irregularidade.** A **CONTRATADA s**e reserva ao direito de, em caso de suspeita de violação ou irregularidade da LGPD, notificar o cliente e/ou suspender a atividade de tratamento.

3.6. **Anonimização.** O **CONTRATANTE** está ciente e de acordo com o uso de Dados Anonimizados do sistema pela **CONTRATADA** para fins de suporte técnico, estatísticos, de melhoria de usabilidade, de análise e balanceamento dos servidores e outros fins voltados para a melhoria da experiência do usuário e de desempenho do Software.

3.7. **Subcontratação de operadores.** A **CONTRATADA** poderá subcontratar parte dos serviços que envolva o Tratamento de DP para Suboperadores mediante a formalização de contrato escrito que contenha Cláusulas de proteção de DP para obrigá-los às mesmas condições de segurança impostas por este Contrato em relação à **CONTRATADA**.

3.8. **Transferência Internacional.** As PARTES concordam que poderá ser realizada a transferência internacional de DP para países que proporcionem grau adequado de proteção de DP e/ou mediante a implementação de mecanismo contratual, como Cláusulas contratuais para transferências de DP.

3.9. **Incidente de Segurança da Informação.** Na ocorrência de qualquer Incidente de Segurança da Informação que possa acarretar risco ou dano relevante aos titulares que envolva os DP tratados por força do Contrato, a **CONTRATADA** comunicará o **CONTRATANTE** sobre o ocorrido no prazo de 48 (quarenta e oito) horas, a partir da ciência do Incidente de Segurança e adotará as medidas que entender necessárias para reverter e/ou mitigar os seus efeitos.

4. DISPOSIÇÕES GERAIS

4.1. A **CONTRATADA** declara estar ciente de que o manuseio inadequado das Informações Confidenciais, sua divulgação ou revelação não autorizada a quaisquer terceiros representarão, por si só, prejuízo ao patrimônio, à imagem e reputação do **CONTRATANTE**, e implicará em sua responsabilização civil ou criminal, de acordo com a violação verificada, obrigando-se ao ressarcimento das perdas e danos decorrente.

4.2. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a **CONTRATADA**, além de sanções penais cabíveis, ao pagamento o **CONTRATANTE** e a terceiros pelas perdas e danos, diretos e indiretos, decorrentes do evento de descumprimento, facultada ainda o **CONTRATANTE** a rescisão do presente Termo e demais acordos que estiverem vigentes com a **CONTRATADA**.

4.3. Este Termo não impõe obrigações à **CONTRATADA** com relação às Informações Confidenciais que (i) já sejam lícita e comprovadamente de conhecimento da **CONTRATADA** anteriormente à da sua divulgação pelo **CONTRATANTE**; (ii) sejam ou venham a se tornar de conhecimento público, sem qualquer intervenção da **CONTRATADA** e (iii) sejam divulgadas à **CONTRATADA** por qualquer terceiro que as detenham em legitima posse, sem que isto constitua violação de dever de confidencialidade previamente assumido com o **CONTRATANTE**.

4.4. Se a **CONTRATADA** vier a ser obrigada a divulgar, no todo ou em parte, as Informações Confidenciais por qualquer ordem judicial ou autoridade governamental competente, a **CONTRATADA** poderá fazê-lo desde que notifique imediatamente o **CONTRATANTE**, para permitir que esta adote as medidas legais cabíveis para resguardo de seus direitos.

4.5. Se a **CONTRATADA**, na hipótese aqui tratada, tiver que revelar as Informações Confidenciais, divulgará tão somente a informação que foi legalmente exigível e envidará seus melhores esforços para obter tratamento de segredo para quaisquer Informações Confidenciais que revelar, nos precisos dispositivos deste Termo e da Lei.

4.6. A **CONTRATADA** concorda que não deve se opor à cooperação ou empenho de esforços com o **CONTRATANTE** para auxiliar na adoção das medidas judiciais competentes, sendo certo que nada poderá ser exigido ou solicitado a **CONTRATADA** que não esteja dentro dos estritos limites legais.

4.7. O presente Termo permanecerá em vigor por prazo indeterminado, independentemente da formalização de qualquer negócio entre as Partes.

4.8. Quaisquer alterações a este Termo somente terão validade e eficácia se forem devidamente formalizadas através de termo aditivo firmado entre as Partes.

4.9. O presente Termo será interpretado pela Legislação da República Federativa do Brasil e as Partes desde já elegem o Foro da Cidade de Belém, Estado do Pará, para dirimir qualquer controvérsia oriunda deste instrumento, salvo disposição específica pela legislação aplicável.

E por estarem de pleno acordo as Partes reconhecem e concordam expressamente que a inserção de sua senha pessoal e/ou a utilização de outras formas de assinatura eletrônica. Inclusive biométricas, em plataformas digitais, como a "*DocuSign*", constitui forma legítima e suficiente para a confirmação de seus dados, comprovação de sua identidade e validade de sua declaração de vontade para assinar e celebrar o presente Contrato para que produza todos os seus efeitos de direito, conforme dispões e Legislação aplicável.

Belém-PA, data da última assinatura eletrônica.

BANCO DA AMAZÔNIA S.A.

Assinado por:
Bruna Eline da Silva Cavalcante
246C4EF61D234EA...

BRUNA ELINE DA SILVA CAVALCANTE
Gerente Executiva de Contratações e Gestão
Administrativa de Contratos – GECOG

ATLAS GOVERNANCE TECNOLOGIA LTDA

Signed by:
Eduardo Shakir Carone
D5EA9DD9090F43F...

EDUARDO SHAKIR CARONE
Administrador

TESTEMUNHAS:

Nome: DocuSigned by:
Camila Sanches Mendes Lage
C45F183FCFF44F6...

Assinado por:
Alan Barros Costa
9F28051825B64F5...

ANEXO II

REQUISITOS MÍNIMOS DE SEGURANÇA PARA SISTEMAS ADQUIRIDOS

REQUISITOS GERAIS DE SEGURANÇA PARA A CONTRATADA

A **CONTRATADA** deverá assinar, no início do Contrato, o Termo de Confidencialidade e Sigilo que terá como objetivo definir as regras relativas ao tratamento, acesso, proteção e revelação das informações corporativas do Banco da Amazônia (BASA).

Todos os empregados da empresa contratada que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato deverão assinar o Termo de Responsabilidade e Confidencialidade do Empregado Terceirizado. O referido termo deverá ser entregue ao Gestor do Contrato antes do início das atividades do profissional.
A **CONTRATADA** deverá:

- Adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do **CONTRATANTE**;
- Comunicar com antecedência mínima de 15 (quinze) dias ao **CONTRATANTE** qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do **CONTRATANTE**, porventura colocados à disposição para realização dos serviços contratados;
- Manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo **CONTRATANTE** a tais documentos;
- Não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do **CONTRATANTE**, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos;
- Manter seus empregados devidamente informados das normas disciplinares do **CONTRATANTE**, bem como das normas de utilização e de segurança das instalações e do manuseio dos documentos;
- Manter empregados devidamente identificados por meio de crachá funcional quando no ambiente do **CONTRATANTE**;
- Garantir que seus empregados conheçam a POL 304 - Política de Segurança da Informação e Comunicações e de Segurança Cibernética do Banco da Amazônia;
- Assumir inteira responsabilidade, pelos danos causados diretamente à administração ou a terceiros, incluindo prejuízos financeiros, decorrentes de sua culpa ou dolo, quando da não observância de requisitos mínimos de segurança no desenvolvimento de seus produtos e serviços;
- Assumir inteira responsabilidade por quaisquer danos ou prejuízos causados ao **CONTRATANTE** e a terceiros, incluindo prejuízos financeiros, por dolo ou culpa, de seus empregados, decorrentes dos serviços ora contratados;
- Garantir e manter total e absoluto sigilo sobre as informações manuseadas as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;
- Não repassar a terceiros, em nenhuma hipótese, qualquer informação sobre a arquitetura e/ou documentação, assim como dados e/ou metadados trafegados, produtos desenvolvidos e entregues, ficando responsável juntamente com o **CONTRATANTE** por manter a segurança da informação relativa aos dados e procedimentos durante a execução das atividades e em período posterior ao término da execução do Contrato;
- Assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do **CONTRATANTE** através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado;

- Providenciar para que os produtos e artefatos da contratação sejam entregues em perfeito estado, com a segurança necessária, garantindo o transporte, o seguro, a entrega e a implantação nos locais indicados pelo **CONTRATANTE** sem quaisquer danos, avarias ou ônus adicionais para o **CONTRATANTE**.

COMPLIANCE PARA SERVIÇOS EXECUTADOS EM NUVEM

A **CONTRATADA** deve garantir que a legislação brasileira prevaleça sobre qualquer outra, de modo que o **CONTRATANTE** tenha todas as garantias legais enquanto tomador do serviço e proprietário das informações, se hospedadas na nuvem.

A **CONTRATADA** deverá:

- Cumprir integralmente as diretrizes da Resolução CMN 4.893/21;
- Fornecer backup ao **CONTRATANTE** aos dados e às informações a serem processados ou armazenados pela empresa contratada;
- Assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador;
- Apresentar conformidade com a norma ABNT NBR ISO/IEC 27001:2013 referente aos serviços de computação em nuvem e aos data centers que hospedem esses serviços ou, alternativamente, demonstrar atender os objetivos e controles da referida norma, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao **CONTRATANTE** promover diligência destinada a esclarecer ou complementar informações;
- Fornecer ao **CONTRATANTE** acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador, relativos aos procedimentos e aos controles utilizados na execução dos serviços a serem contratados;
- Assegurar, enquanto o C ontrato estiver vigente, a identificação e a segregação dos dados dos clientes do **CONTRATANTE** por meio de controles físicos ou lógicos e forneça ao **CONTRATANTE** documentos e/ou relatórios que evidenciem o cumprimento desta exigência;
- Assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do **CONTRATANTE**;
- Adotar um padrão de identidade federada para permitir o uso de tecnologia **single sign-on** no processo de autenticação dos usuários do serviço de nuvem, o qual deve ser acompanhado de autenticação multifator (MFA).
- Registrar e armazenar, pelo período de um ano, todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações.
- Apoiar o **CONTRATANTE**, quando necessário, nas atividades de investigação de incidentes de cibersegurança. Isso inclui fornecer prontamente informações e recursos necessários para a investigação, como logs, registros de eventos e relatórios de auditoria.
- Adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, caso o serviço a ser contratado seja relativo ao serviço de execução de aplicação por meio da internet;
- Garantir que o ambiente seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados por outros usuários do serviço em nuvem;
- Assegurar que toda atualização do sistema seja previamente analisada e homologada antes que possa ser instalada/configurada, além de dispor de documentação de todas as alterações realizadas no serviço e/ou sistema mediante processos formalizados de Gestão e Mudanças;
- Assegurar a adoção de medidas de segurança para a transmissão e armazenamento dos dados e das informações processados ou armazenados pelo prestador, e fornecer ao **CONTRATANTE** evidências da adoção das referidas medidas;
- Comunicar previamente ao **CONTRATANTE** sobre a subcontratação de serviços relevantes para a prestação do serviço contratado;

- Notificar ao **CONTRATANTE** sobre a intenção de interromper a prestação de serviços com pelo menos trinta dias de antecedência da data prevista para a interrupção;

- Conceder o 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;

- Manter o **CONTRATANTE** permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

- Se adicionalmente contratado o serviço, dispor de Plano de Comunicação de Incidentes e/ou dashboards com informações referentes a saúde dos serviços oferecidos de incidentes que possam ocorrer, informando o **CONTRATANTE** os casos de incidentes de segurança da informação, assim considerados os eventos não previstos ou não desejados que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do **CONTRATANTE**;

- Dealizar a análise e gestão de riscos de segurança de informação, conforme procedimentos internos da **CONTRATADA**;

- 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;

- Desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços ou envolvendo dados pessoais de empregados e/ou clientes do **CONTRATANTE**;

- Realizar anualmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) e auditorias por terceira parte reconhecidamente confiável, disponibilizando relatório comprobatório, sempre que solicitado pelo **CONTRATANTE**;

- Prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso;

- Deverá fornecer, sempre que solicitado pelo **CONTRATANTE**, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de Application Programming Interface (API), caso haja, para análise de segurança e auditorias;

- Dispor de recursos e soluções técnicas que garantam a segurança da informação dos dados do **CONTRATANTE**, incluindo os seguintes itens: solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações), solução de prevenção e detecção de intrusão (IDS/IPS), antivírus, anti-malware, solução anti-DDoS, solução de gestão de logs, solução de gestão integrada de pacotes de correção (patches), solução de correlação de eventos de segurança (SIEM);

- Realizar backups e salvaguardas dos conteúdos das comunicações realizadas por meio da solução e permitir a consulta desses dados;

- Garantir a exclusividade de direitos, por parte do BASA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como **backups** de segurança.

- Comprometer-se a preservar os dados do **CONTRATANTE** contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente ao **CONTRATANTE** qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados;

- operar o serviço dentro do uso proposto, com desempenho razoável e exigindo o mínimo possível de permissões dos demais sistemas do **CONTRATANTE**, além de proteger os dados transmitidos por meio dele, quando necessário;

- atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar:
- as diretrizes de tratamento;
- o modo de atendimento a solicitações de titulares de dados pessoais;
- as medidas protetivas para garantia da confidencialidade dos dados pessoais;
- as medidas protetivas durante as comunicações com o BASA;
- o registro de atividades de tratamento de dados pessoais;
- a solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;
- a medidas de devolução / descarte dos dados.
- A partir do ponto de entrada/saída da internet nos datacenters do provedor de nuvem ofertados, a contratada deverá observar:
- inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei;
- inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
- não fornecimento a terceiros de dados do **CONTRATANTE**, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
- fornecer ao **CONTRATANTE**, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do **CONTRATANTE**.
- Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo **CONTRATANTE**, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se que:
- pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;
- a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, desde que em conformidade com a Resolução CMN 4.893/21.
- A empresa deve garantir a adequação e a adoção de medidas pelo BASA, em decorrência de qualquer determinação do Órgãos Governamentais aos quais o **CONTRATANTE** é subordinado que impacte sobre o Contrato vigente.
- A **CONTRATADA** deve manter o **CONTRATANTE** permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.
- É vedado o uso de informações do **CONTRATANTE** pela **CONTRATADA** para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;
- Em caso de extinção do Contrato, a contratada deverá transferir os dados e as informações processados ou armazenados por ele ao novo prestador de serviços ou ao **CONTRATANTE** e, após a confirmação da integridade e da disponibilidade dos dados e informações recebidos, os excluir.
- Em caso da decretação de regime de resolução do **CONTRATANTE** pelo Banco Central do Brasil, a **CONTRATADA** deverá:
- Conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, 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 que estejam em poder da **CONTRATADA**; e
- Notificar previamente o responsável pelo regime de resolução sobre sua a intenção de interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção. A **CONTRATADA** obriga-se a aceitar eventual pedido de prazo

adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução. A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência do **CONTRATANTE**.

REQUISITOS DE ARQUITETURA, DESIGN E MODELAGEM DE AMEAÇAS

O sistema, com recursos web, deverá incorporar, no mínimo, proteção contra:

- **Controle de acesso falho:** as restrições sobre o que os usuários autenticados têm permissão para fazer muitas vezes não são aplicadas de forma adequada. Os invasores podem explorar essas falhas para acessar funcionalidades e/ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

- **Falhas criptográficas:** Muitos aplicativos da web e APIs não protegem adequadamente os dados sigilosos, como dados pessoais e financeiros. Os invasores podem roubar ou modificar esses dados fracamente protegidos para conduzir fraude de cartão de crédito, roubo de identidade ou outros crimes. Os dados sigilosos podem ser comprometidos sem proteção extra, como criptografia em repouso ou em trânsito, e requerem precauções especiais quando trocados com o navegador.

- **Injeção:** Injeções ocorrem quando dados informados pelo usuário são enviados para um interpretador como parte de um comando ou uma query. O dado malicioso do atacante faz o interpretador executar comandos que não deveria ou modificar dados. Algumas das injeções mais comuns são SQL, NoSQL, OS command, Mapeamento Relacional de Objeto (ORM), LDAP e Expression Language (EL) ou Object Graph Navigation Library (OGNL). O conceito é idêntico entre todos. A revisão do código-fonte é o melhor método para detectar se os aplicativos são vulneráveis a injeções.

- **Design inseguro:** O design seguro é uma cultura e metodologia que avalia constantemente as ameaças e garante que o código seja desenvolvido e testado de forma robusta para evitar métodos de ataque conhecidos. O design seguro requer um ciclo de vida de desenvolvimento seguro, alguma forma de padrão de design seguro ou biblioteca ou ferramenta de componentes de estradas pavimentadas e modelagem de ameaças.

- **Configuração incorreta de segurança:** geralmente é o resultado de configurações padrão inseguras, configurações incompletas ou ad hoc, armazenamento em nuvem aberta, cabeçalhos HTTP configurados incorretamente e mensagens de erro detalhadas contendo informações confidenciais. Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas também devem ser corrigidos / atualizados em tempo hábil.

- **Componentes vulneráveis e desatualizados:** componentes, como bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios do aplicativo. Se um componente vulnerável for explorado, esse tipo de ataque pode facilitar a perda séria de dados ou o controle do servidor. Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas do aplicativo e permitir vários ataques e impactos.
- **Falhas de identificação e autenticação:** as funções do aplicativo relacionadas à autenticação e gerenciamento de sessão são frequentemente implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir as identidades de outros usuários temporária ou permanentemente.

- **Falhas de software e integridade de dados:** As falhas de software e integridade de dados estão relacionadas ao código e à infraestrutura que não protegem contra violações de integridade. Por exemplo, quando objetos ou dados são codificados ou serializados em uma estrutura que um invasor pode ver e modificar, logo é vulnerável à desserialização insegura. Outro exemplo é quando um aplicativo depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs).

- **Registro (logging) e monitoramento insuficientes:** registro (logging) e monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes,

permite que os invasores ataquem ainda mais os sistemas, mantenham a persistência, ganhem acesso em mais sistemas e adulterem, extraiam ou destruam dados.

- **Server-Side Request Forgery (SSRF):** As falhas de SSRF ocorrem sempre que um aplicativo web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de ACL de rede.

- **Validação de entrada inadequada:** o produto recebe entradas ou dados, mas não valida ou valida incorretamente se a entrada possui as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado pela aplicação.

- **Caracteres Especiais ou maliciosos:** caracteres especiais são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros. Garanta que apenas entradas válidas, esperadas e apropriadas sejam processadas pelo Sistema.

- A solução deverá possuir conformidade com o OWASP TOP 10 vigente visando assegurar a segurança dos dados, gerar confiança entre os usuários, prevenir perdas financeiras e cumprir regulamentações de segurança, proporcionando a integridade e a credibilidade necessárias para um site ou aplicativo.

A solução não deve ser baseada nos frameworks Wordpress ou Joomla.
Deverá ser imposto o menor privilégio em conexões com o banco de dados ou outros sistemas de back-end.

A **CONTRATADA** deverá realizar configuração segura (hardening) do servidor web no qual a aplicação está hospedada e deverá assegurar que servidores web da aplicação estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmark mais atual.

As seguintes flags e procedimentos relacionados deverão ser adotados em relação às configurações do cabeçalho para a comunicação entre o servidor e o cliente:

- A aplicação deverá instruir o browser a só permitir acesso via HTTPS. Deverá ser ativado o HTTP Strict Transport Security (HSTS) adicionando um cabeçalho de resposta com o nome 'Strict-Transport-Security' e o valor 'max-age = expireTime', em que expireTime é o tempo em segundos que os navegadores devem lembrar que o site só deve ser acessado usando HTTPS. O max-age deve ser de pelo menos 31536000 segundos (1 ano);

- O cabeçalho X-Content-Type-Options deverá estar configurado como 'nosniff' para todas as páginas da web;

- A aplicação deverá retornar o cabeçalho X-Frame-Options com o valor DENY ou SAMEORIGIN, que permitirá “framing” das páginas conforme SAME ORIGIN;
- A aplicação deverá ter o CSP habilitado enviando os cabeçalhos de resposta Content-Security-Policy, conforme políticas que atenda critérios de segurança na implementação dessa diretiva;
- A aplicação deverá ter o cabeçalho X-XSS-Protection desabilitado, por meio da configuração do seu valor como 0 (zero);
- A aplicação não deverá possuir os cabeçalhos “fingerprinting”: X-Powered-By, Server, X-AspNet-Version;
- A aplicação deverá forçar content-type para as respostas. Se a aplicação retorna json, a resposta content-type da aplicação deverá ser application/json;
- Os tipos de conteúdo text/ *, / + xml e application/xml também devem especificar um conjunto de caracteres seguro (por exemplo, UTF-8, ISO-8859-1);
- O conteúdo da aplicação não poderá ser incorporado a um site de terceiro por padrão;
- O Cross-Origin Resource Sharing (CORS) e cabeçalho Access-Control-Allow-Origin deverão utilizar uma lista de permissão restrita de domínios e subdomínios confiáveis para correspondência e não oferecer suporte à origem "null", e validar os dados inseridos pelo usuário;

- O cookie emitido pela aplicação deverá possuir os atributos SameSite, SECURE e HttpOnly;

A aplicação deverá utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações

Antes da entrada em produção, a solução passará por homologação quanto a sua segurança. Quaisquer eventuais vulnerabilidades identificadas pela equipe do BASA serão tratadas como defeito de software e deverão obrigatoriamente ser corrigidas pela **CONTRATADA**.

Realizar configuração segura do servidor web, também conhecido como hardening. Assegurar que servidores WEB estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmarks.

Utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações.

REQUISITOS DE ARMAZENAMENTO DE DADOS E PRIVACIDADE

Os recursos de armazenamento de credenciais do sistema deverão ser utilizados para armazenar dados restritos e sigilosos, como dados pessoais, credenciais de usuário ou chaves criptográficas

Dados restritos e sigilosos não deverão:

ser exibidos em mensagens de erro;

- Ser armazenados fora do contêiner da aplicação ou de recursos de armazenamento de credenciais do sistema;
- Ser armazenados em texto claro, como um banco de dados não criptografado;
- Aparecer nos logs de aplicação;
- Ser compartilhados com terceiros, exceto se for uma parte necessária da arquitetura;
- Ser expostos através de mecanismos IPC (Inter-process Communication);
- Ser armazenados localmente ou em arquivos temporários no dispositivo. Em vez disso, os dados deverão ser recuperados de um terminal remoto quando necessário e mantidos apenas em memória.

A aplicação não deverá exibir mensagens de erro detalhadas que possa expor informações privilegiadas.

Senhas ou PINs de acesso não deverão ser expostos através da interface de usuário.

Credenciais de acesso não deverão ser armazenadas dentro do código-fonte do sistema.

Será obrigatória a validação, a filtragem e o tratamento de todos os dados inseridos pelo usuário.

Toda requisição de acesso ao banco de dados deverá passar por processo de validação de autorização.

Será vedada a filtragem de dados no cliente.

Não deverá ser utilizado o método GET (URLs) para o envio de dados restritos ou sigilosos ou para a realização transações financeiras.

O método HTTP deverá ser utilizado de acordo com a operação: GET (read), POST (create), PUT/PATCH (replace/update), e DELETE (delete).

Será proibida a utilização de dados sensíveis (credenciais de acesso, senhas, tokens ou API keys) na URL, deverá ser utilizado cabeçalho Authorization.

Toda requisição de acesso à API deverá passar por processo de validação de autorização.

Um mecanismo de validação de entrada padrão deverá ser utilizado para validar todos os dados em tamanho, tipo, sintaxe e regras de negócio antes de exibi-los ou armazená-los.

Deverá ser utilizada a estratégia de validação do tipo Whitelist.

Será obrigatória a validação content-type de dados publicados (POST) aceitáveis (por exemplo

application/x-www-form-urlencoded, multipart/form-data, application/json etc.).

Entradas inválidas deverão ser sanitizadas..

REQUISITOS DE AUTENTICAÇÃO

O sistema deve possuir controle de acesso dos usuários baseado em papéis, usuários e funções.

O sistema deve possuir mecanismo de múltiplo fator de autenticação (MFA);

O sistema deve ser capaz de admitir integração com Microsoft do **CONTRATANTE** para login único de usuário (Single Sign On = SSO).

As senhas deverão ser gravadas em banco de dados de forma criptografada.

A tela de log-on não deverá exibir a senha que está sendo informada.

O sistema não deverá armazenar ou transmitir senhas em texto plano.

A tela de entrada dos sistemas deverá validar as informações fornecidas pelo usuário somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deverá indicar qual parte do dado de entrada está correta ou incorreta.

Em caso de tentativa de log-on inválida, o sistema deverá exibir uma mensagem genérica e nunca exibir as mensagens "usuário inexistente" ou "senha incorreta", de modo a não fornecer mensagens que permitam a um usuário não autorizado deduzir informações de acesso.

Todo acesso administrativo deverá ser restrito e deverá ser garantido o acesso apenas aos usuários autorizados.

Deverá ser utilizado HTTPS para envio de credenciais.

Os sistemas não deverão passar ID de sessão por método HTTP GET.

Deverá ser utilizado sempre o método HTTP POST para a requisição de autenticação.

Será obrigatória a utilização do parâmetro “state” com hash aleatório no processo de autenticação do OAuth.

Será proibido o uso de Basic Authentication.

As autorizações de acesso deverão ser validadas, garantindo que nenhum usuário acessará o que não foi previamente definido em seu perfil.

O processo de login deve ser iniciado através de uma página com um novo cookie de sessão.

Todos os endpoints do sistema deverão ser protegidos por autenticação.
Será proibido o incremento de IDs automaticamente. No lugar, deverá ser utilizado UUID.

REQUISITOS DE GERENCIAMENTO DE SESSÃO DO USUÁRIO

As sessões deverão ser invalidadas pelo terminal remoto após um período de, no máximo, 15 minutos de inatividade e os tokens de acessos devem expirar.

O controle de sessão deverá ser tratado pelo servidor e apenas a persistência dele no cliente.

Os sistemas deverão implementar token de sessão por requisição com alta aleatoriedade, devendo ser utilizados tokens personalizados e aleatórios em todos os formulários e URLs que não serão automaticamente enviadas pelo navegador.

Toda as páginas deverão ter um link para o logout o qual, ao clicar, o sistema deverá realizar o logout sem antes questionar o usuário. O logout deve destruir todo o estado da sessão no lado servidor e os cookies no lado cliente.

Será proibido o uso de “response_type=token”.

Dados de usuários, atributos e políticas utilizados pelos controles de acesso, não podem ser manipulados pelos usuários finais, a menos que especificamente autorizado na arquitetura do projeto.

O sistema deverá utilizar o princípio do menor privilégio, os usuários só devem ser capazes de acessar funções, arquivos de dados, URLs, controladores, serviços e outrosoken recursos, para os quais possuam autorização específica.

Em caso de sistemas que utilizam JWT (JSON Web Token):t

- Será obrigatório o uso de chaves randômicas (JWT Secret);
- Será proibido armazenar dados confidenciais em tokens JWT.
- Será proibida a extração do algoritmo do cabeçalho (deverá ser validado no back-end);
- Deverá ser utilizado no back-end o algoritmo RS256;
- Será obrigatório regras de time-out de sessão do usuário de 15 minutos, access token de 3 minutos e refresh token de 8 horas.

REQUISITOS DE COMUNICAÇÃO DE REDE

O sistema deverá ser capaz de suportar a pilha dupla IPV4 e IPv6.

Todas as comunicações externas entre os servidores do sistema e os clientes deverão ser encriptadas.

O sistema deverá utilizar criptografia para as comunicações externas entre os servidores do sistema e os clientes. Os dados deverão ser criptografados na rede utilizando somente TLS 1.2 ou superior.

O sistema não deverá permitir o uso do SSL, TLS 1.0 e TLS 1.1.

Deve-se usar os seguintes algoritmos: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256), SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 e SHAKE256.

Será vedada a utilização de cifras com vulnerabilidades divulgadas e/ou conhecidas.

As requisições deverão ser limitadas (através de rate limit ou outra solução semelhante), a fim de se evitar ataques de DoS (negação de serviço) ou força bruta.

Deverá ser utilizada a validação de “redirect_url” no servidor para permitir apenas URL’s da *whitelist*.

Tráfegos HTTP deverão ser redirecionados para HTTPS.

A propriedade “readOnly” deverá ser configurada como “true” em esquemas de objeto para todas as propriedades que podem ser recuperadas por meio de APIs, mas nunca deverão ser modificadas.

Os modos de depuração do servidor da Web ou de aplicativos e da estrutura de aplicativos deverão ser desativados em produção para eliminar recursos de depuração, consoles de desenvolvedor e divulgações de segurança não intencionais.

REQUISITOS DE RESPOSTAS HTTP

Os cabeçalhos HTTP ou qualquer parte da resposta HTTP não deverão expor informações detalhadas da versão dos componentes do sistema.

A aplicação deverá retornar os seguintes códigos:

- 405 Method Not Allowed: sempre que um método solicitado não for apropriado para o recurso solicitado
- 406 Not Acceptable: sempre que o formato suportado não for correspondido. Requisições content-type deverão ser validadas para permitir apenas o formato suportado (por exemplo application/xml, application/json etc.)
- HTTP 200: código de resposta do status de sucesso do HTTP, indica que a solicitação foi bem-sucedida;
- HTTP 302: indica que o recurso solicitado foi movido temporariamente para a URL fornecida pelo cabeçalho Location.
- HTTP 401: para qualquer ação não autorizada no sistema.

- HTTP 429: para solicitações que excedam o limite de requisição permitido.
- HTTP 415: para solicitações contendo cabeçalhos de tipo de conteúdo ausentes ou inesperados

A aplicação deverá ter defesas contra ataques de poluição de parâmetro HTTP, especialmente se a estrutura do aplicativo não faz distinção sobre a origem dos parâmetros de solicitação (GET, POST, cookies, cabeçalhos ou variáveis de ambiente).

Redirecionamentos e encaminhamentos de URL deverão permitir apenas destinos que aparecem em uma lista de permissões ou deverão mostrar um aviso ao redirecionar para conteúdo potencialmente não confiável.

A aplicação deverá ter proteção contra ataques do tipo SSRF, validando ou higienizando dados não confiáveis ou metadados de arquivos HTTP, como nomes de arquivos, campos de entrada de URL, listas de protocolos, domínios, caminhos e portas.

REQUISITOS DE AUDITORIA

A solução deve dispor de logs de eventos para fins de auditoria, incluindo todas as ações administrativas e ações envolvendo os itens arquivados e pesquisados no que tange o arquivamento, visualização, recuperação e remoção de itens.

A solução deve dispor de logs com registro de informações a serem utilizadas na depuração e verificação de falhas da solução, mantendo o registro de toda atividade de arquivamento e recuperação realizada, inclusive para os processos de auditoria realizados.
A solução deve permitir a configuração de usuários (auditores), com permissão de monitorar (auditar) e acessar grupos específicos de caixas postais e/ou todas as mensagens arquivadas.

A solução deve suportar a geração e armazenamento de logs no formato IPV4 e IPv6.

As aplicações deverão implementar um sistema de *logging* que permita auditorias e investigações de incidentes de segurança, fraudes e casos de abuso.

A identificação do usuário, ou ID, deverá ser única, isto é, cada usuário deverá ter uma identificação própria.

Os sistemas de informação e suas respectivas infraestruturas deverão ser configurados de modo a registrar um critério mínimo de informações de logging e auditoria, contendo, no mínimo:

- Operações de login e logout;
- Tentativas de login malsucedidas;
- Acesso a telas cujo conteúdo é sigiloso, em segredo de justiça, possua dados pessoais ou bancários;
- Operações de inclusão, alteração ou exclusão de registros no banco de dados;
- Execução de jobs e tarefas automatizadas;
- Criação, leitura, atualização ou exclusão de informações sigilosas;
- Mudanças de configurações no sistema, na rede ou em serviços (inicialização, suspensão e reinicialização de serviços), inclusive a instalação de patches e atualizações de softwares;
- Acesso aos bancos de dados de fonte interna e externa;
- Falhas que resultem no fechamento anormal da aplicação, especialmente devido à exaustão de recurso ou atingimento do limite de um recurso (como memória do CPU, conexões de rede, espaço no disco etc.);
- Acesso e alteração de trilhas de auditoria;
- Registros de tráfego de dados de fontes internas e externas; e
- Registros de processos internos relacionados às atividades do negócio.

Os registros dos eventos deverão incluir, no mínimo, as seguintes informações:

- Identificação inequívoca do autor/ativo que realizou a atividade;
- Sistema onde ocorreu ou foi observada a atividade (logger/observador do evento);
- Tela (página) do sistema de onde a operação foi realizada;
- Tipo de atividade ocorrida (tipo de evento/ação);

- Data, hora e fuso horário, observando os mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);
- Retorno do sistema em caso de falhas ou sucesso na ação;
- Identificador da instância (para sistemas clusterizados);
- Para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;
- Parâmetros informados pelo usuário (ex: parâmetros repassados aos métodos GET ou POST);
- Tempo de resposta do sistema;
- Para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada etc.; e
- Endereço IP, nome do dispositivo, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

A aplicação não deve registrar credenciais ou detalhes de pagamento.

Os tokens de sessão só devem ser armazenados em logs de forma irreversível e com hash.

Será vedado o envio de informações sensíveis (ex: credenciais de acesso) para logs.

A solução não deverá registrar logs de auditoria em banco de dados da aplicação.

As aplicações deverão registrar logs de rastreamento distribuído (distributed tracing) de requisição.

As aplicações deverão gerar logs em formato que permita a completa identificação dos fluxos de dados

As aplicações deverão registrar eventos relevantes de segurança, incluindo eventos de autenticação bem-sucedidos e com falha, falhas de controle de acesso, falhas de desserialização e falhas de validação de entrada.

A solução deve garantir que todas as fontes de tempo estão sincronizadas com a hora e fuso horário corretos.

Dados de registro devem ser sanitizados para evitar ataques de injeção de registro.

REQUISITOS PARA APIs

A codificação de API deverá incorporar, no mínimo, proteção contra:

a) Broken Object Level Authorization

b) Broken User Authentication

c) Excessive Data Exposure

d) Lack of Resources & Rate Limiting

e) Broken Function Level Authorization

f) Mass Assignment

g) Security Misconfiguration

h) Injection (Injection flaws, tais como SQL e NoSQL, Command Injection etc.)

i) Improper Assets Management

j) Insufficient Logging & Monitoring

k) Conformidade com o OWASP Top 10 API Security Risks em vigor

Deverão ser utilizadas as classes Encoder e Validator da OWASP ESAPI (Enterprise Security API)

Deve ser imposto o menor privilégio quando se conectar ao banco de dados ou outros sistemas de back-end.

O banco de dados não deverá ser acessado por outro canal que não seja a aplicação

Os URLs da API não deverão expor informações confidenciais, tais como a chave da API, tokens de sessão etc.

Objetos serializados deverão usar verificações de integridade ou criptografados para evitar a criação de objetos hostis ou adulteração de dados.

Todos os endpoints acessíveis ao público devem usar um Certificado Digital que tenha sido assinado por uma Autoridade de Certificação aprovada e dentro do prazo de utilização.

Devem ser aplicadas políticas de limitação de taxa (ratelimit) para evitar o abuso da API.

Toda entrada pelo usuário por parâmetros da aplicação ou de forma manipulada em qualquer outra parte da aplicação, deverá ser validada, garantindo as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado."

A solução deve garantir que apenas entradas válidas, esperadas e apropriadas sejam processadas, pois caracteres especiais ou maliciosos são usados para explorar falhas como: SQL injection, XSS, Temlate Injection, entre outros.

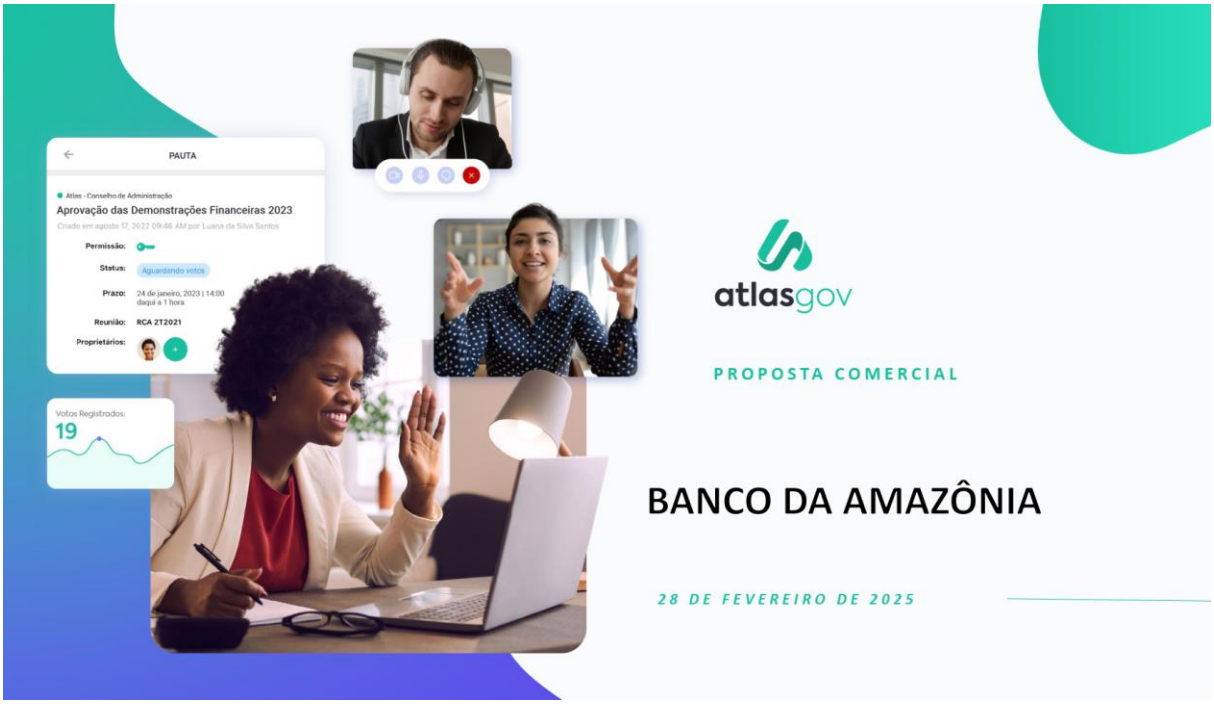
ANEXO III

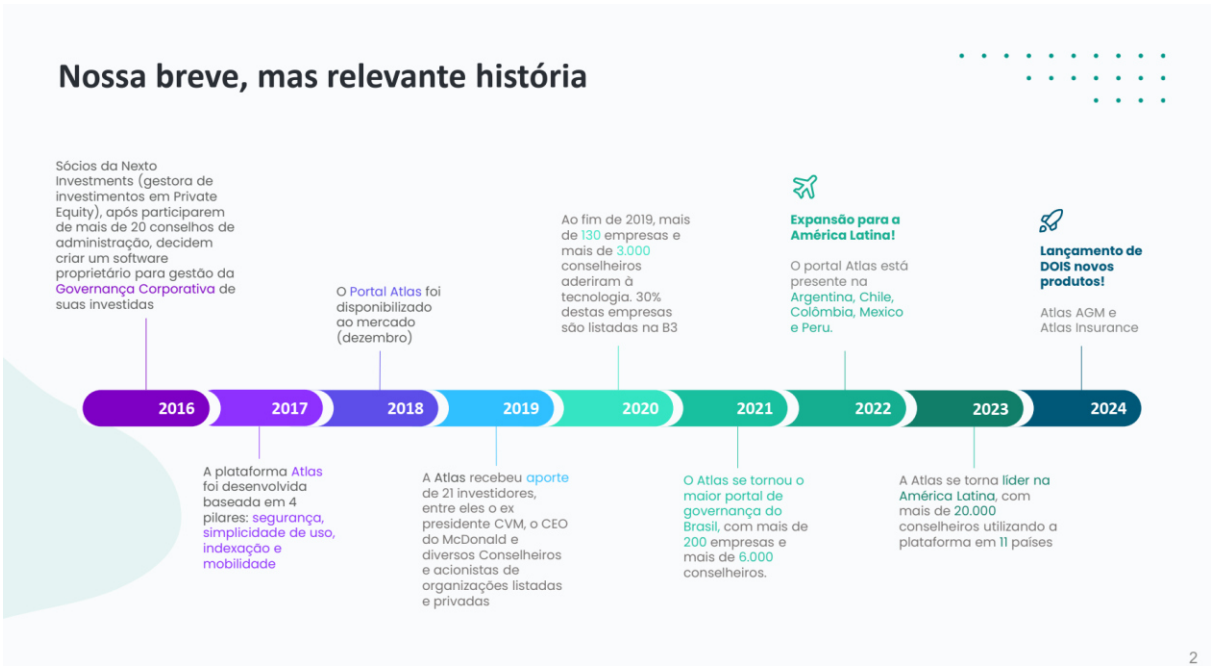
Matriz de Riscos

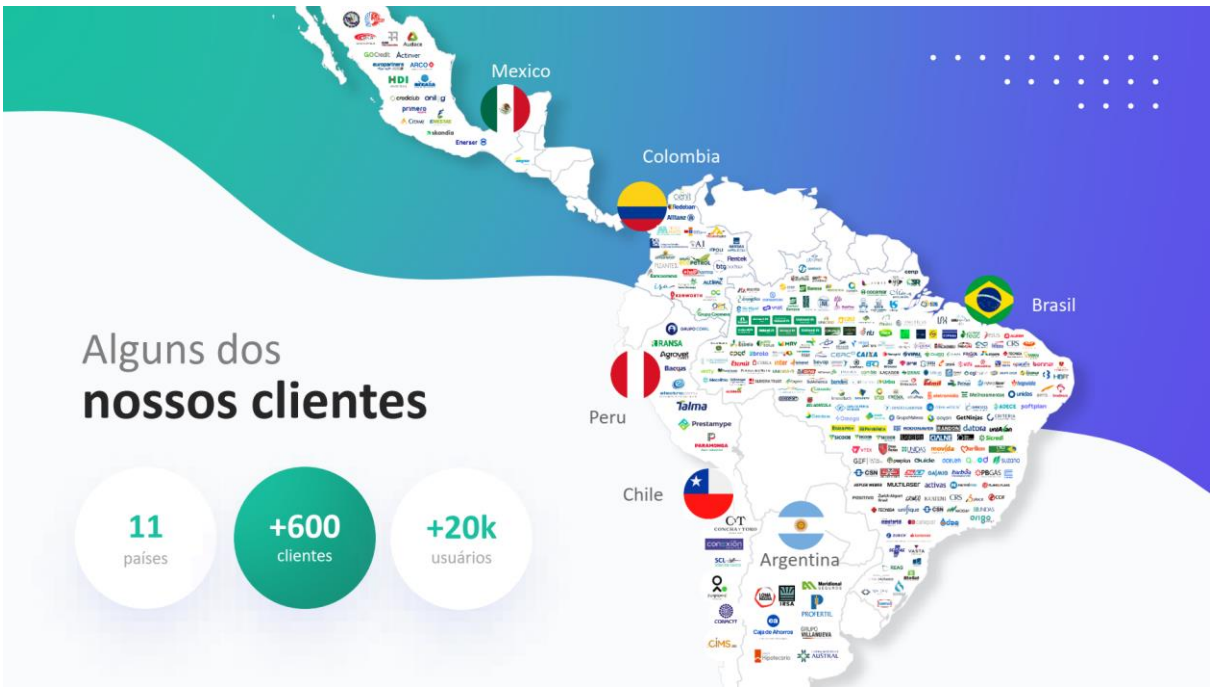
CATEGORIA DO RISCO	DESCRIÇÃO	CONSEQUÊNCIA	MEDIDAS MITIGADORAS	ALOCAÇÃO DO RISCO
Risco de tempo e Qualidade	Atraso na entrega dos serviços	Descumprimento de prazos acordados	Acionar a fornecedora e verificar possível aplicação de multa. Aplicar as sanções contratuais. Incluir no Indicador de Qualidade	**CONTRATADA**
	Não cumprimento do contrato de suporte	Descumprimento	Acionar a fornecedora e verificar possível aplicação de multa. Aplicar as multas previstas Incluir no Indicador de Qualidade	Descumprimento
Risco operacional	Pagamentos indevidos (a maior)	Influência no resultado operacional do **CONTRATANTE**	Ressarcimento do **CONTRATANTE**.	**CONTRATANTE** e **CONTRATADA**
	Provisionamento indevido	Influência no resultado operacional do **CONTRATANTE**	Ajuste contábil junto à GECON	**CONTRATANTE**
	Ausência de controle de faturas e pagamentos e/ou falta de verificação de conformidade entre as faturas e o Contrato.	Riscos de Pagamentos duplicados	Criar processo e controles	**CONTRATANTE**
Riscos internos	Não aplicação de multas e glosas	Perdas financeiras	Ressarcimento do **CONTRATANTE**.	**CONTRATADA**
	Ausência de notificações ao fornecedor	Impedimento para abertura de processo administrative tempestivo	Gestão e Fiscalização	**CONTRATANTE**
	Ausência de livro de ocorrências	Falta de evidências de acompanhamento contratual	Gestão e Fiscalização	**CONTRATANTE**
	Ausência de nomeação de fiscal	Descumprimento de normativos internos	Gestão e Fiscalização	**CONTRATANTE**

ANEXO IV

PROPOSTA COMERCIAL







Conteúdo	Professional	Enterprise
		POPULAR ENTRE NOSSO CLIENTES
Boards ilimitados	✓	✓
Reuniões ilimitadas	✓	✓
Storage ilimitado	✓	✓
Assinatura eletrônica e digital	✗	✓
Personalização de segurança	✗	✓
Customer Success exclusivo	✓	✓
Treinamentos	✓	✓
Formulários de Avaliação	✗	✓
Impossible Travel	✗	✓
Condicional Access	✗	✓
Criptografia em trânsito AES 256	✓	✓
Segundo fator de autenticação	✓	✓

Inteligência Artificial

Chat (em desenvolvimento)

Todos poderão "conversar" com a IA

Benéfico para todos os usuários.

Leitura do comportamento dos usuários

. Personalização e precisão
. Identificação de tendências e melhorias
. Melhor alocação de recursos
. Inovação contínua

Resulta em crescimento e a inovação em toda a organização.

Insights e sugestões

. Aumento da produtividade
. Tomada de decisão mais rápida e embasada
. Facilidade de acesso e compartilhamento
Consistência e aprendizado contínuo

Maior eficiência e colaboração em toda a empresa.

Demais benefícios

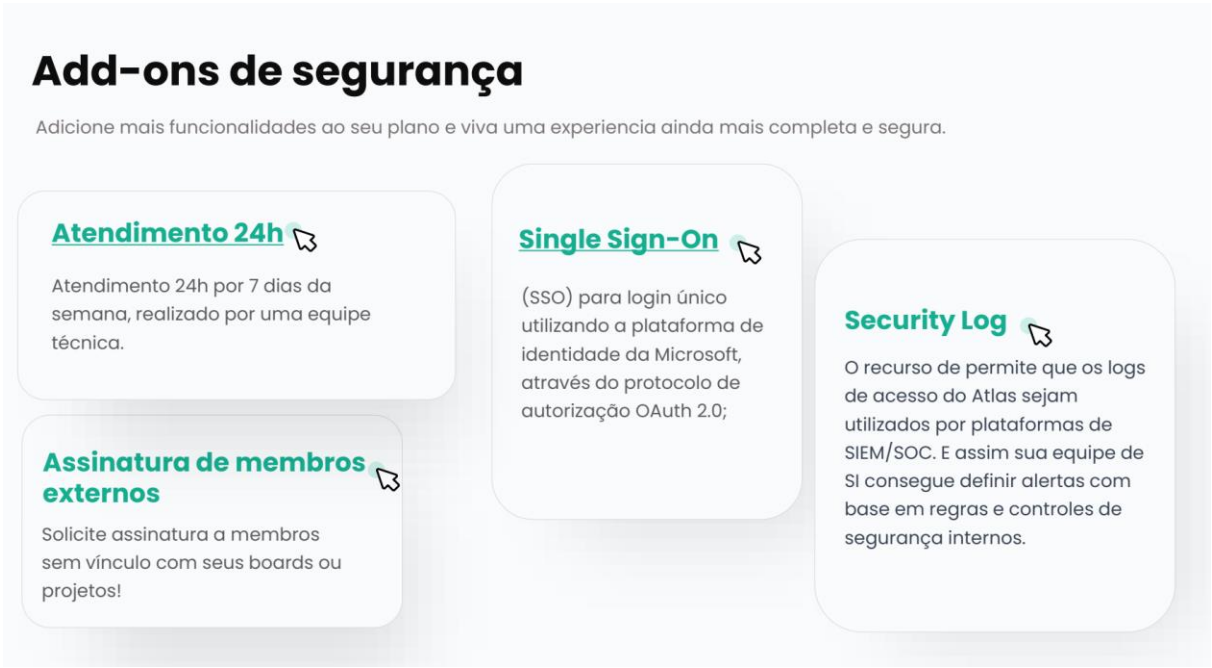
. Transcrição total da reunião
. Overview completo e organizado por tópicos da reunião

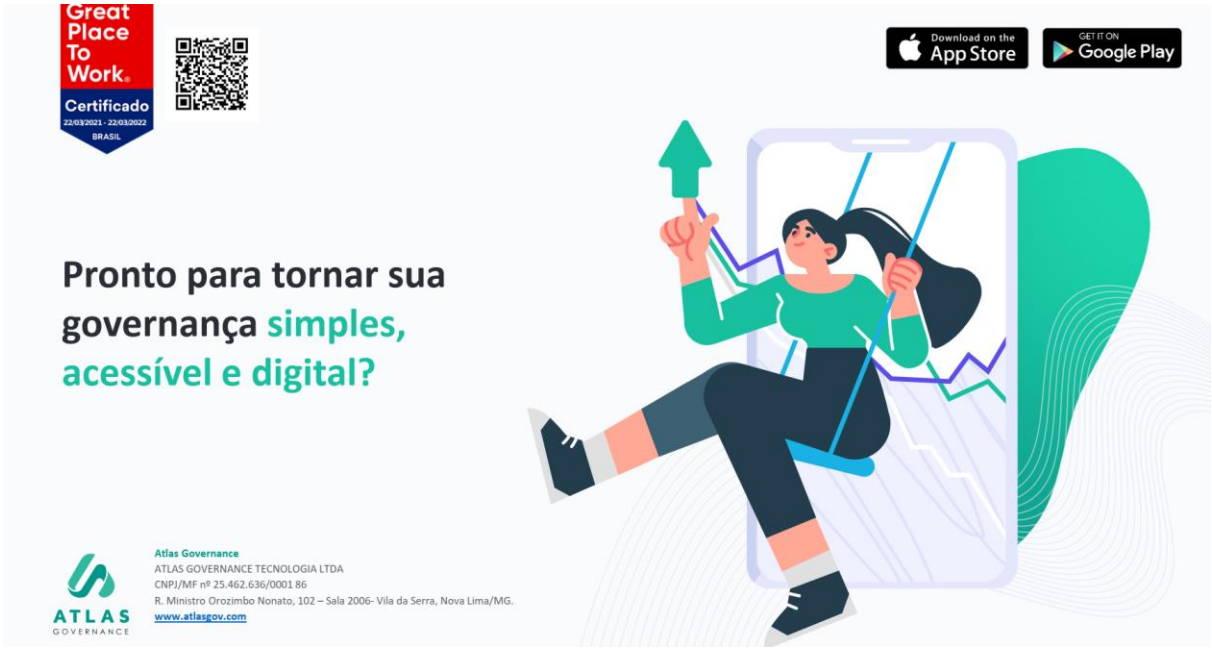
Registro do histórico da AI para consultas – Todos poderão se beneficiar.

Investimento:

LICENCIAMENTO	Qtd.	VALOR POR USUÁRIO	VALOR ANUAL (R$)
Plano Enterprise	30	R$ 2.584,38	R$ 77.531,40
Total Global de 5 anos			R$ 387.657,00

atiasgov





ANEXO V

TIPO I_ MODELO DE CONTRATO SIMPLIFICADO
BASA_CONTROLADOR_VS_OPERADOR

DO TRATAMENTO DE DADOS

CLÁUSULA PRIMEIRA – A RESPONSÁVEL afirma que adota todas as medidas necessárias para garantir a privacidade, o sigilo, a segurança da informação e concorda que eventual tratamento de dados pessoais que ocorrer em virtude deste contrato deve seguir todas as diretrizes da Lei 13.709/2018, ainda que este Contrato venha a ser resolvido, e independentemente dos motivos que derem causa ao seu término ou resolução, sendo estritamente proibido o compartilhamento dessas informações e dados pessoais com quaisquer terceiros, exceto nas hipóteses previstas neste contrato, ou caso haja autorização prévia e expressa do Titular dos dados.

PARAGRÁFO ÚNICO - Para fins deste contrato, esclarece-se que os dados pessoais são entendidos na forma da Lei Geral de Proteção de Dados, Lei nº 13.709/2018, como os dados relativos a pessoas naturais que as identifique ou tenham o potencial de identificá-las, portanto, excluídos os dados de pessoas jurídicas. Esses dados serão tratados na execução dos deveres e obrigações estipulados neste Contrato e, em todos os casos, somente quando o tratamento for lícito e cumprir com os princípios estabelecidos nas normas aplicáveis.

Belém-PA, data da última assinatura eletrônica.

BANCO DA AMAZÔNIA S.A.

Assinado por:
Bruna Eline da Silva Cavalcante
248C4EF61D234EA...

BRUNA ELINE DA SILVA CAVALCANTE
Gerente Executiva de Contratações e Gestão
Administrativa de Contratos – GECOG

ATLAS GOVERNANCE TECNOLOGIA LTDA

Signed by:
Eduardo Shakir Carone
D5EA9DD9090F43F...

EDUARDO SHAKIR CARONE
Administrador

TESTEMUNHAS:

Nome: DocuSigned by:
Camila Sanches Mendes Lage
C45F183FCFF44F6...

Assinado por:
Alan Barros Costa
9F28051825B64F5...

Certificado de Conclusão

Identificação de envelope: B9C46512-28A3-4D2A-9564-9550CDC227DF
Status: Concluído
Assunto: Complete com o Docusign: ATLAS GOVERNANCE TECNOLOGIA LTDA - CONTRATO 2025-135.pdf
Envelope fonte:
Documentar páginas: 40
Assinaturas: 12
Certificar páginas: 5
Rubrica: 0
Assinatura guiada: Ativado
Selo com EnvelopeId (ID do envelope): Ativado
Fuso horário: (UTC-03:00) Brasília

Remetente do envelope:
assinatura.contratos@basa.com.br
Rua Santo Antonio, N.17 - Sala F - Centro
Eusebio, CE 61760000
assinatura.contratos@basa.com.br
Endereço IP: 163.116.230.117

Rastreamento de registros

Status: Original
25/06/2025 11:17:19
Portador: assinatura.contratos@basa.com.br
assinatura.contratos@basa.com.br
Local: DocuSign

Eventos do signatário	Assinatura	Registro de hora e data
Alan Barros Costa alan.costa@basa.com.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	Assinado por: Alan Barros Costa 9F28051825B64F5... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 163.116.230.117	Enviado: 25/06/2025 11:26:19 Visualizado: 25/06/2025 11:28:02 Assinado: 25/06/2025 11:31:44
Termos de Assinatura e Registro Eletrônico: Aceito: 25/06/2025 11:28:02 ID: 5e14868f-c743-4c59-803e-888bf50681fa		
Bruna Eline da Silva Cavalcante bruna.cavalcante@basa.com.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	Assinado por: Bruna Eline da Silva Cavalcante 246C4EF61D234EA... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 163.116.230.114	Enviado: 25/06/2025 11:26:19 Visualizado: 25/06/2025 19:27:14 Assinado: 25/06/2025 19:30:46
Termos de Assinatura e Registro Eletrônico: Aceito: 25/06/2025 19:27:14 ID: 3463a05a-8b22-41d2-a5ae-03334d0635f4		
Camila Sanches Mendes Lage camila.sanches@atlasgov.com Head Legal Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	DocuSigned by: Camila Sanches Mendes Lage C45F183FCFF44F6... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 170.85.20.202	Enviado: 25/06/2025 11:26:18 Reenviado: 30/06/2025 10:33:15 Visualizado: 30/06/2025 16:06:25 Assinado: 30/06/2025 16:06:38
Termos de Assinatura e Registro Eletrônico: Aceito: 27/06/2025 13:57:54 ID: e3b8f751-0e4f-4080-bf1b-fd658be9fb1c		
Eduardo Shakir Carone eduardo@atlasgov.com CEO Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	Signed by: Eduardo Shakir Carone D5EA9DD9090F43F... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 201.69.251.34	Enviado: 25/06/2025 11:26:18 Visualizado: 25/06/2025 13:04:40 Assinado: 26/06/2025 10:15:09
Termos de Assinatura e Registro Eletrônico: Aceito: 25/06/2025 13:04:40 ID: 5a28dade-9f3f-4dc6-b224-5bac7b2e2b9b		

Eventos do signatário presencial	Assinatura	Registro de hora e data

Eventos de entrega do editor	Status	Registro de hora e data

Evento de entrega do agente	Status	Registro de hora e data

Eventos de entrega intermediários	Status	Registro de hora e data

Eventos de entrega certificados	Status	Registro de hora e data

Eventos de cópia	Status	Registro de hora e data
Dayse de fatima Pereira dayse.pereira@basa.com.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma) **Termos de Assinatura e Registro Eletrônico:** Aceito: 12/12/2022 11:47:43 ID: c7dc1673-0f05-4755-accf-868112644f6d	**Copiado**	Enviado: 25/06/2025 11:26:19

Eventos com testemunhas	Assinatura	Registro de hora e data

Eventos do tabelião	Assinatura	Registro de hora e data

Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	25/06/2025 11:26:19
Entrega certificada	Segurança verificada	25/06/2025 13:04:40
Assinatura concluída	Segurança verificada	26/06/2025 10:15:09
Concluído	Segurança verificada	30/06/2025 16:06:38

Eventos de pagamento	Status	Carimbo de data/hora

Termos de Assinatura e Registro Eletrônico

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, HCITIS ISV OBO BASA BANCO DA AMAZONIA (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

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

Withdrawing your consent

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

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

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

How to contact HCITIS ISV OBO BASA BANCO DA AMAZONIA:

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

To advise HCITIS ISV OBO BASA BANCO DA AMAZONIA of your new email address

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

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from HCITIS ISV OBO BASA BANCO DA AMAZONIA

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to jonatas.nobre@basa.com.br and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with HCITIS ISV OBO BASA BANCO DA AMAZONIA

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

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

ii. send us an email to jonatas.nobre@basa.com.br and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify HCITIS ISV OBO BASA BANCO DA AMAZONIA as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by HCITIS ISV OBO BASA BANCO DA AMAZONIA during the course of your relationship with HCITIS ISV OBO BASA BANCO DA AMAZONIA.