1. Introdução

1.1. O presente documento estabelece as diretrizes, padrões técnicos e controles de segurança da informação que devem ser obrigatoriamente observados por todos os fornecedores, prestadores de serviços e parceiros de negócio (doravante denominados **CONTRATADA**) que mantenham relação contratual com o **ASSAÍ**. Estes Termos visam garantir a confidencialidade, integridade e disponibilidade dos dados e ativos tecnológicos, em conformidade com as melhores práticas de mercado e a legislação vigente.

2. Governança e Conformidade

2.1. A **CONTRATADA** deve manter uma estrutura de governança de segurança da informação compatível com o porte e a criticidade dos serviços prestados, observando os seguintes requisitos:

a) manter políticas e normas de segurança da informação formalizadas, aprovadas pela alta direção e baseadas em frameworks internacionais como ISO/IEC 27001 ou NIST CSF;

b) garantir o direito de auditoria ao **ASSAÍ**, permitindo a realização de avaliações, vistorias ou auditorias remotas e presenciais para validar a eficácia dos controles implementados;

c) designar um ponto de contato formal para tratar de temas relacionados à segurança e conformidade durante toda a vigência do contrato.

3. Segurança dos Acessos e Dados

3.1. O controle de acesso e a proteção de dados devem seguir o princípio do privilégio mínimo e da necessidade de conhecimento.

3.2. Todo acesso remoto ao ambiente do **ASSAÍ** deve ser realizado exclusivamente via **VPN corporativa** com múltiplo fator de autenticação (**MFA**).

3.3. É terminantemente proibida a utilização de dispositivos pessoais (BYOD) para o processamento de dados do **ASSAÍ**, salvo autorização expressa e formal.

3.4. Dados sensíveis ou classificados como confidenciais devem ser protegidos por criptografia em repouso e em trânsito, utilizando algoritmos de mercado robustos (ex.: AES-256, TLS 1.2+).

4. Testes de Segurança

4.1. A **CONTRATADA** deve assegurar que os ativos tecnológicos utilizados na prestação dos serviços sejam submetidos a validações periódicas:

a) realização de varreduras de vulnerabilidades (scans) mensais em todos os servidores e aplicações que compõem o escopo do serviço;

b) execução de testes de invasão (Pentest) anuais no escopo da prestação de serviço, realizados por empresa independente ou equipe interna qualificada, com o compartilhamento do sumário executivo e plano de remediação com o **ASSAÍ**.

5. Gestão de Vulnerabilidades e Correções (SLAs)

5.1. A **CONTRATADA** declara possuir e manter programa formal de gestão de vulnerabilidades técnicas, contemplando: (i) varreduras periódicas com ferramentas apropriadas; (ii) processo de priorização baseado em criticidade (CVSS ou equivalente); (iii) SLAs de remediação definidos; (iv) evidências documentadas de remediação.

5.2. A **CONTRATADA** deverá apresentar evidências do programa ao **CONTRATANTE** sempre que solicitado.

6. Resposta a Incidentes

6.1. Em caso de suspeita ou confirmação de incidente de segurança que possa afetar os dados ou a operação do **ASSAÍ**, a **CONTRATADA** deverá:

a) notificar o **ASSAÍ** em até **24 horas** para incidentes críticos e **48 horas** para os demais casos, através dos canais oficiais de comunicação;

b) fornecer relatórios detalhados contendo a causa raiz, o impacto e as medidas de erradicação e recuperação adotadas, em até **72 horas** após a conclusão do incidente;

c) abster-se de realizar comunicações públicas ou a terceiros sobre o incidente sem a prévia e expressa autorização do **ASSAÍ**.

7. Segurança de Software (SDLC) e Entregas

7.1. Para serviços que envolvam desenvolvimento de software, a **CONTRATADA** deve adotar práticas de DevSecOps:

a) implementar análise estática (SAST) e dinâmica (DAST) de código durante o ciclo de desenvolvimento;

b) garantir a segregação de ambientes (Desenvolvimento, Homologação e Produção), sendo vedado o uso de dados reais de produção em ambientes não produtivos sem que haja aplicação de técnicas de anonimização ou mascaramento dos dados.

8. Gestão de Pessoas e Subcontratados

8.1. A segurança deve ser mantida por meio do controle rigoroso dos recursos humanos:

a) realizar treinamentos anuais de conscientização em segurança da informação e proteção de dados para todos os colaboradores alocados no projeto;

b) revogar todos os acessos de colaboradores desligados ou transferidos em, no máximo, **24 horas** após o evento;

c) garantir que eventuais subcontratados autorizados adiram formalmente a estes Termos e Condições.

9. Continuidade de Negócios e Recuperação de Desastres

9.1. A **CONTRATADA** deve assegurar a resiliência dos serviços prestados:

a) manter Planos de Continuidade de Negócios (PCN) e Planos de Recuperação de Desastres (PRD) atualizados e testados anualmente;

b) garantir que os backups sejam realizados conforme política definida, armazenados em local seguro e testados periodicamente quanto à sua integridade e capacidade de restauração.

10. Encerramento do Contrato, Devolução e Expurgo

10.1. Ao término da relação contratual, por qualquer motivo, a **CONTRATADA** obriga-se a:

a) devolver todos os ativos e dados de propriedade do **ASSAÍ** em formato legível e estruturado;

b) realizar o expurgo seguro de todas as cópias de dados remanescentes em seus sistemas e mídias, utilizando métodos que impeçam a recuperação da informação;

c) fornecer, em até 30 dias após o encerramento, o **Certificado de Destruição Segura de Dados** devidamente assinado por seu representante legal.