DECLARAÇÃO E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

1. OBJETIVO E ESCOPO

A **Guuh Analytics** (Gustavo Henrique Concheto Sistemas e Informática Ltda, CNPJ 36.472.608/0001-66) processa dados críticos, financeiros e de faturamento (SAP SD/FI/DRC). Por isso, a Segurança da Informação não é um recurso adicional, é o núcleo central do nosso serviço. Esta declaração resume nossas práticas de segurança Enterprise-Grade.

2. ARQUITETURA E CLEAN CORE

Nossa solução foi arquitetada sob o princípio *SAP Clean Core*. Não instalamos "Z-programs" intrusivos, transportes não homologados ou customizações no *core* do S/4HANA ou ECC do cliente. A integração ocorre via **SAP Business Technology Platform (BTP)** ou conectores de API REST/OData criptografados, garantindo isolamento e estabilidade do ambiente produtivo.

3. COMPLIANCE E FRAMEWORK SOC 2

Nossos processos, controles lógicos e físicos operam em alinhamento aos critérios dos *Trust Services Criteria* do AICPA (SOC 2), focando fundamentalmente em:

- **Segurança:** Proteção contra acesso não autorizado (lógico e físico).
- **Disponibilidade:** Sistemas resilientes e com alta disponibilidade para monitoramento contínuo.
- **Confidencialidade:** Dados financeiros dos clientes restritos a um grupo mínimo de pessoas, seguindo o princípio de *Need-to-Know* e *Least Privilege*.

4. PROTEÇÃO DE DADOS E CRIPTOGRAFIA

- **Dados em Trânsito:** Toda a comunicação entre o ambiente do cliente e a Guuh Analytics ocorre sob protocolos seguros (TLS 1.2 ou superior).
- **Dados em Repouso:** Os dados analíticos armazenados em nossos bancos de dados (temporários ou históricos) são encriptados utilizando o padrão AES-256.
- **Retenção Zero:** Para clientes com regulamentações rígidas, operamos no modelo *Zero Data Retention*, onde os dados são cruzados pela IA em memória, os relatórios de anomalia são gerados, e os dados brutos são imediatamente expurgados.

5. SEGURANÇA NA INTELIGÊNCIA ARTIFICIAL

Nossos Agentes de IA operam em ambientes *Tenant-Isolated* (Isolamento de Inquilino). Isso garante que o modelo de IA que analisa os contratos de um cliente **nunca** utiliza esses dados para treinar modelos base (*foundation models*) abertos ao público ou misturar contextos com bases de outros clientes corporativos.

6. GESTÃO DE VULNERABILIDADES E INCIDENTES
Mantemos rotinas de monitoramento contínuo (SIEM) e estamos preparados para atuar de forma imediata em conformidade com as diretrizes do nosso Plano de Resposta a Incidentes, notificando o cliente previamente em caso de qualquer anomalia sistêmica.

Documento classificado como: PÚBLICO.
Aprovado por: Gustavo Concheto - Especialista InfoSec e Fundador.