

REGRAS TÉCNICAS DO ASSISTENTE INTELIGENTE UPFLUX NOUS

Smart Process S.A. (UpFlux)

Informações do documento

Campo	Valor
Código	PS-SEC-NOUS-001
Versão	1.0
Status	Vigente
Data de emissão	25/05/2026
Owner	Segurança da Informação e Diretoria de Engenharia
Aprovadores	Comitê de Segurança da Informação (CSI) e Diretoria Executiva
Classificação	Público
Ciclo de revisão	Semestral, ou a cada versão principal do Nous, ou sob mudança regulatória relevante

1. Objetivo

Este documento descreve as regras técnicas de operação, os limites funcionais e os controles de segurança e privacidade aplicáveis ao UpFlux Nous, a camada de inteligência artificial conversacional da plataforma UpFlux.

Ele foi elaborado para três públicos:

- Equipes de TI e Segurança da Informação de clientes e prospects que avaliam a solução, respondem por sua homologação interna ou conduzem processos de due diligence.
- Equipes de negócio que desenham soluções sobre o Nous e precisam conhecer antecipadamente as restrições que não podem ser contornadas por configuração.
- Áreas de compliance e privacidade que precisam entender como o assistente trata dados e onde estão os pontos de decisão humana.

O documento é subordinado à Política de Governança de IA Generativa da UpFlux. Em caso de conflito, prevalece a política.

Aviso: o Nous evolui de forma contínua. Este documento reflete o comportamento do produto na data de emissão. A versão vigente é sempre a publicada no site da UpFlux. Cláusulas contratuais específicas, quando existirem, prevalecem sobre o conteúdo aqui descrito.

2. Escopo

Aplica-se a todos os módulos e componentes do UpFlux Nous:

- Pergunte ao Nous e Chats, a interface conversacional.
- Comandos, ou playbooks, definidos por processo.
- Agendamento de rotinas.
- Achados e Caixa de entrada.
- Visões e Modo TV.
- Acesso mobile por aplicativo web progressivo.
- Motor de execução, ferramentas invocáveis pelo modelo de linguagem e camada de acesso a dados.

Não estão no escopo deste documento: a camada de Process Intelligence propriamente dita, ou seja, ingestão, transformação e mineração de processos, tratada na documentação de arquitetura da plataforma; os modelos de aprendizado de máquina não generativos, tratados em política específica; e os módulos, agentes e integrações comercializados separadamente, que possuem documentação e regras próprias quando contratados.

3. Definições

Termo	Definição
Nous	Plataforma de Enterprise AI da UpFlux. Camada de inteligência artificial conversacional construída sobre a base de Process Intelligence.
Destino da conversa	Combinação de organização e processo, definida antes da primeira mensagem e imutável depois dela.
Comando, ou playbook	Análise padronizada, definida na configuração de um processo e invocada por barra no campo de mensagem ou por chip de categoria.
Rotina	Análise recorrente agendada, com instrução em linguagem natural, periodicidade e canal de entrega.
Achado	Análise salva do chat na biblioteca de Achados, com título, descrição e tags.
Visão	Painel ao vivo criado a partir de uma análise de playbook, com atualização sob demanda ou automática e Modo TV.
Tier	Classificação de complexidade da pergunta, que determina quais ferramentas o modelo de linguagem pode acionar.
Ferramenta	Função que o modelo pode invocar durante a execução, como consulta de dados, execução de código ou leitura de arquivo de contexto.
RLS	Row Level Security, ou segurança em nível de linha. Restringe quais registros o motor pode ler ao produzir uma resposta.
Alucinação	Geração de informação factualmente incorreta ou inventada, apresentada com aparência de confiança. É o risco mais crítico e específico de modelos de linguagem.
Gating de módulo	Habilitação de funcionalidade conforme a capacidade contratada pela organização. Módulo não habilitado não expõe o menu correspondente.

4. Arquitetura de referência

A tabela consolida as camadas que governam o comportamento do assistente.

Camada	Definição
Modelo de entrega	Software como serviço puro. Não há requisito de infraestrutura no ambiente do cliente para uso da plataforma. O acesso é por navegador.
Infraestrutura	Nuvem pública AWS, região us-east-2 (Ohio). Provisionamento gerenciado como código, com validação por pipeline de integração contínua.
Camada de IA	Camada conversacional que interpreta a pergunta do usuário, planeja a análise, consulta os dados do processo e sintetiza a resposta. Opera sempre no contexto do processo ativo e restrita aos dados que o usuário está autorizado a acessar.
Modelos de linguagem	Provedor homologado: Anthropic, família Claude, com seleção entre modelos conforme a capacidade necessária a cada etapa da execução. A orquestração usa abstração de provedores, sem acoplamento direto entre a aplicação e o modelo, o que permite substituir ou combinar modelos sem impacto nos fluxos configurados.
Camada de dados transacionais	Banco de dados documental gerenciado, com base dedicada por cliente e cluster de no mínimo três nós. Criptografia em trânsito e em repouso. O cliente controla exclusões parciais e totais, política de backup e recuperação.

Camada	Definição
Camada analítica	Camada analítica colunar vetorizada, operada em modo somente leitura pelo assistente, complementada por mecanismo de busca de alto desempenho.
Persistência do assistente	Conversas, artefatos, configurações de contexto e trilha de auditoria em base documental segregada por organização.
Identidade e acesso	Federação por OpenID Connect, com suporte a diretórios corporativos, autenticação multifator e SSO quando o cliente possui a integração configurada. Validação de token em cada requisição.
Notificações	Serviço orquestrador com filas, distribuindo por notificação no aplicativo, e-mail e webhooks.
Ingestão de dados	Ingestão de log de eventos em tempo quase real, com detecção de violações por regra, controle de vazão e reprocessamento automático. Transformação assíncrona por pipelines configuráveis e área de estágio para dados brutos. Extração por REST, SQL e arquivos, com conectores para TOTVS, SAP, ServiceNow, Tasy e MV.
Observabilidade	Monitoramento de desempenho da aplicação e rastreamento das execuções do modelo, com métricas de qualidade e de consumo.

5. Regras de contexto e sessão

ID	Regra
CTX-01	Toda conversa possui um destino, composto por organização e processo. O destino é confirmado antes da primeira mensagem e exibido no seletor abaixo do campo de mensagem.
CTX-02	O destino da conversa é imutável após o envio da primeira mensagem. A troca de processo exige a abertura de nova conversa.
CTX-03	Toda resposta é produzida no contexto do processo ativo. Não existe resposta transversal a múltiplos processos dentro de uma mesma conversa.
CTX-04	A trilha de navegação da conversa segue Organização, Processo e Título. O título é editável pelo usuário.
CTX-05	O contexto conversacional é mantido dentro da mesma conversa e não é compartilhado entre conversas distintas. Cada nova conversa inicia sem histórico anterior.
CTX-06	A interface exibe selo com a data da última carga de dados. O selo passa para âmbar quando os dados têm mais de sete dias, sinalizando ao usuário que a análise pode não refletir a operação atual.
CTX-07	Idiomas suportados: português do Brasil, inglês e espanhol.
CTX-08	Ponto de entrada padrão: no desktop a plataforma abre em Pergunte ao Nous, no mobile abre no Chat.

6. Regras de chat e artefatos

ID	Regra
CHT-01	Entrada por linguagem natural. Envio por Enter e quebra de linha por Shift mais Enter. Não é necessário conhecimento de SQL ou de programação.
CHT-02	A tela inicial exibe o cartão Pulso do processo, com Casos, Atividades, Lead time médio e Mediana, e chips de categoria agrupados por seis perfis: Analista de Processo, Auditor e Compliance, Comprador e Operacional, Executivo e CPO, Financeiro e Pagamentos, e Gestor de Compras e Sourcing.
CHT-03	A saída é composta por narrativa com indicadores citados, tabelas, visualizações e dashboards interativos.

ID	Regra
CHT-04	Durante a execução o assistente exibe o Processo de construção, com as etapas percorridas e as ferramentas utilizadas. A transparência das chamadas de ferramenta é comportamento padrão do produto.
CHT-05	Quando o contexto é insuficiente, o assistente abre perguntas guiadas, que podem ser respondidas ou puladas. Lacuna de contexto não é preenchida por inferência não declarada ao usuário.
CHT-06	Cada resposta admite avaliação Útil ou Não útil. A avaliação negativa abre formulário de feedback, utilizado na melhoria contínua da configuração.
CHT-07	Comentários e menções permitem colaboração sobre as análises entre usuários da organização.
CHT-08	Ações de artefato disponíveis: Expandir, Baixar em HTML, Exportar Excel, Exportar PDF, Compartilhar e Apresentar em Modo Story.
CHT-09	Conversões a partir do chat: Salvar Achado, Transformar em Visão e Transformar em rotina.
CHT-10	Conversas são vinculadas ao usuário autor e não são visíveis a outros usuários da organização por padrão. O usuário pode excluir conversas do próprio histórico.
CHT-11	A exportação de artefato transfere conteúdo para fora da plataforma. A partir desse ponto, o tratamento do arquivo é responsabilidade da organização cliente, conforme sua própria política de classificação e manuseio da informação.

7. Regras de modos de raciocínio

ID	Regra
RAC-01	Nous 2.1: resposta direta e rápida, sem etapa de planejamento apresentada ao usuário.
RAC-02	Nous Deep: o assistente monta um plano de investigação, apresenta ao usuário e aguarda confirmação explícita antes de executar a análise completa, com critérios explícitos, comparação de grupos e identificação de concentração.
RAC-03	A disponibilidade do Nous Deep é definida por habilitação da organização, não por usuário.
RAC-04	A etapa de confirmação do Nous Deep é um controle de contenção de execução e não é suprimida por configuração de rotina.
RAC-05	Regras de precisão aplicadas ao motor: apresentação numérica na granularidade adequada, herança de contexto e de período em perguntas de sequência, gráficos com rótulos de valor e renderização estável entre execuções.

8. Regras de comandos e playbooks

ID	Regra
CMD-01	Comandos são análises padronizadas definidas na configuração de cada processo. São específicos por processo e não globais.
CMD-02	Invocação por barra no campo de mensagem, com filtro incremental por nome ou descrição, navegação por setas e seleção por Enter ou clique. O comando é inserido no campo e exige envio pelo usuário.
CMD-03	Invocação alternativa pelos chips de categoria, que listam os comandos do perfil correspondente.
CMD-04	Processo sem comandos publicados retorna estado vazio. Não há uso de comandos de outro processo como alternativa.
CMD-05	Somente análises originadas de comando ou playbook podem ser promovidas a Visão ao vivo. Análises ad hoc não podem.

9. Regras de rotinas agendadas

ID	Regra
ROT-01	Campos de configuração: Nome, Processo, instrução da análise em linguagem natural, Agendamento e Entrega.
ROT-02	Periodicidade diária, semanal ou mensal, com definição de dia da semana ou dia do mês e horário, além dos atalhos Dias úteis, Fins de semana, Todos os dias, Dia 1, Dia 15 e Dia 28.
ROT-03	Entrega por notificação no aplicativo e por e-mail, admitindo múltiplos endereços separados por vírgula. Pelo menos um canal de entrega é obrigatório.
ROT-04	A ação de execução imediata dispara a rotina fora do agendamento, com entrega do resultado por e-mail.
ROT-05	Ações disponíveis: pausar e reativar, editar e excluir. As abas de configuração e de histórico registram sucesso ou erro, origem automática ou manual e duração da execução.
ROT-06	Após três falhas consecutivas a rotina é pausada automaticamente, com aviso em tela.
ROT-07	Antes de agendar a partir de uma conversa, o assistente pré-analisa a pergunta e levanta os esclarecimentos necessários, de modo a evitar rotina configurada sobre premissa ambígua.
ROT-08	Resultados de rotina também chegam como mensagens na Caixa de entrada, com histórico de execuções.
ROT-09	A instrução da rotina é artefato de configuração, com histórico de alteração preservado.

10. Regras de achados, caixa de entrada e compartilhamento

ID	Regra
ACH-01	Achados são a biblioteca de análises salvas a partir do chat, com Título, Descrição opcional e Tags. A página oferece busca, filtro por tag, prévia lateral, abertura, download, compartilhamento, link para a conversa de origem, comentários e geração de plano de ação. Formatos disponíveis: HTML, PDF e links compartilháveis.
ACH-02	Achados são privados por padrão.
ACH-03	O compartilhamento por link opera em três escopos: Privado, restrito ao autor; Organização, para membros autenticados; e Público, acessível a qualquer pessoa que tenha o link, com data de expiração.
ACH-04	O escopo Público dispensa autenticação. Sua utilização é decisão da organização cliente e não deve ser aplicada a análises que contenham dados pessoais, dados pessoais sensíveis ou informação confidencial. Quando utilizado, recomenda-se sempre definir data de expiração.
ACH-05	A Caixa de entrada é um menu distinto de Achados. Recebe menções e resultados de rotinas, com filtros por não lidas, menções e rotinas.

11. Regras de visões e Modo TV

ID	Regra
VIS-01	Somente análises de playbook podem ser promovidas a Visão. Análises ad hoc não podem.
VIS-02	Criação a partir do chat pela ação de transformação em Visão, com definição de nome e confirmação.
VIS-03	Atualização sob demanda, com marcação do horário da última atualização, ou automática em intervalos de 15 segundos, 30 segundos, 1 minuto, 5 minutos e 15 minutos.
VIS-04	Modo TV com tela cheia, seleção de tema, link dedicado para tela de exibição e saída por ESC.
VIS-05	Falha de atualização não invalida o painel. A versão anterior é mantida com aviso ao usuário, de modo a nunca exibir painel em branco ou dado parcial.
VIS-06	A exclusão arquiva a Visão e a remove da lista. A renomeação está disponível no próprio painel.

ID	Regra
VIS-07	O link dedicado de exibição concede acesso a dados ao vivo. A definição do local de exibição é responsabilidade da organização cliente, que deve considerar a classificação da informação apresentada antes de expor o painel em área de circulação comum.

12. Regras de acesso mobile

ID	Regra
MOB-01	O acesso mobile ocorre por aplicativo web progressivo, instalado a partir de banner no navegador. No Android pela ação de instalação, no iOS por compartilhar e adicionar à tela de início. A execução é em modo autônomo e o aplicativo inicia no Chat.
MOB-02	Navegação inferior com acesso ao Chat, às Rotinas, aos Achados e ao menu Mais, que concentra configurações, tema, idioma, consumo, troca de processo e organização, e saída. Os itens exibidos variam conforme os módulos habilitados para a organização.
MOB-03	Notificação push é opt-in e exige autorização do navegador. O estado de bloqueio é sinalizado ao usuário. As notificações incluem aviso em tela, som e push com direcionamento por organização e processo.
MOB-04	O aplicativo sinaliza nova versão disponível e estado sem conexão.
MOB-05	Não há aplicativo nativo publicado em loja. O acesso é sempre por navegador, o que dispensa gestão de pacote no parque de dispositivos do cliente.

13. Regras do motor de execução e das ferramentas do modelo

ID	Regra
EXE-01	A execução segue um pipeline de cinco estágios: classificação da pergunta, planejamento, execução, renderização e síntese da resposta.
EXE-02	A classificação atribui um nível de complexidade entre simples, médio, complexo e investigativo. A maior parte das classificações ocorre sem chamada ao modelo de linguagem, por regra determinística.
EXE-03	As ferramentas disponíveis ao modelo são liberadas conforme o nível de complexidade. Níveis mais simples operam apenas com consulta de dados. A execução de código e a renderização enriquecida são liberadas apenas nos níveis que as exigem.
EXE-04	A consulta de dados opera em modo somente leitura. Aceita exclusivamente instruções de seleção, bloqueia comandos de alteração ou remoção, bloqueia múltiplas instruções em uma mesma chamada e valida as colunas referenciadas contra o esquema real da base.
EXE-05	A execução de código ocorre em ambiente isolado, sem acesso a rede e sem acesso ao sistema de arquivos, com bloqueio de bibliotecas de sistema, de subprocesso e de acesso a recursos do servidor, e lista de permissão para as bibliotecas analíticas utilizadas.
EXE-06	A leitura de arquivos de contexto opera somente leitura, com caminho restrito ao diretório de configuração de contexto.
EXE-07	Na renderização, o modelo produz configuração estruturada consumida por biblioteca de componentes padronizados. O modelo não gera marcação livre para as visualizações padrão, o que elimina erro de execução e garante consistência visual.
EXE-08	Quando há geração de conteúdo enriquecido, os dados são injetados por código a partir do resultado da consulta, não pelo modelo de linguagem.
EXE-09	A resolução do contexto de domínio ocorre em cascata, do mais específico ao mais genérico: configuração específica de cliente e processo, template do processo, contexto de domínio e, por último, execução sem contexto configurado.
EXE-10	A execução sem contexto configurado é condição degradada, monitorada e não admitida como estado permanente em produção.

ID	Regra
EXE-11	Há cache de contexto segmentado por organização e processo. Segmentos de cache não são compartilhados entre organizações distintas.
EXE-12	Há limite de taxa de requisições por minuto, aplicado por usuário e por organização.

14. Regras de ancoragem e mitigação de alucinação

A mitigação de alucinação é o controle mais crítico de qualquer aplicação baseada em modelos de linguagem. Em contexto de auditoria e de processos financeiros, uma informação inventada pode gerar decisão indevida com impacto direto. As regras abaixo são cumulativas.

ID	Regra
ANC-01	O prompt de sistema contém regra explícita que veda a apresentação de qualquer valor numérico não apurado nos dados.
ANC-02	Toda resposta é ancorada em dados recuperados na execução. Quando o dado não existe ou está fora do escopo configurado, o assistente informa que não sabe e não improvisa.
ANC-03	As visualizações apontam para os dados efetivamente recuperados. Não há geração de série ou de valor ilustrativo.
ANC-04	Quando há conteúdo enriquecido, os dados são injetados por código, o que impede a introdução de valor pelo modelo na etapa de apresentação.
ANC-05	O usuário pode solicitar os registros de exemplo que sustentam qualquer número apresentado.
ANC-06	Nenhuma decisão regulatória ou financeira é executada exclusivamente com base em saída de modelo, sem validação automatizada ou humana. Saídas do assistente são recomendações.
ANC-07	Quando a confiança é insuficiente, o sistema sinaliza explicitamente que a informação requer verificação humana. Conteúdo incerto não é apresentado como fato.
ANC-08	Precedência regulatória: normas setoriais aplicáveis e a legislação vigente sobrepõem qualquer saída generativa do modelo.
ANC-09	Configurações de contexto e de rotina não podem reduzir ou remover a exigência de ancoragem, a sinalização de incerteza ou a exibição do processo de construção da resposta.

15. Regras de isolamento, acesso e segurança de dados

ID	Regra
ISO-01	Cada organização possui espaço isolado, com base de dados dedicada. Em nenhuma situação os dados de uma organização são compartilhados ou tornados visíveis para outra.
ISO-02	O isolamento lógico é aplicado por identificador de organização, com validação de token em cada requisição e propagação de contexto de organização, processo e papel do usuário em toda a cadeia de execução.
ISO-03	A identidade é federada por OpenID Connect, com suporte a diretório corporativo, autenticação multifator e SSO quando o cliente possui a integração configurada.
ISO-04	O controle de acesso é baseado em papéis e grupos, administrado em central de segurança própria, com políticas de acesso e auditoria exportável.
ISO-05	A segurança em nível de linha é aplicada em todo o caminho de consulta, restringindo quais registros o motor pode ler ao produzir uma resposta. O controle não depende da formulação da pergunta.
ISO-06	Regra de precedência de acesso: a capacidade contratada define o que existe, o grupo define quem vê, e a segurança em nível de linha define quais registros o motor pode ler.
ISO-07	O Admin Center define quais processos e informações cada usuário acessa e está disponível apenas a perfis administradores da organização cliente.

ID	Regra
ISO-08	Criptografia de dados em repouso com AES-256 e em trânsito com TLS 1.2 ou superior. Gestão de chaves com rotação automática e controle de acesso por política.
ISO-09	Toda alteração de grupo, de política de acesso ou de regra de segurança em nível de linha é registrada em trilha auditável e exportável.

16. Regras de privacidade e tratamento de dados pessoais

ID	Regra
PRI-01	Dados de clientes não são utilizados para treinar nem para ajustar modelos de linguagem, próprios ou de terceiros. Qualquer exceção depende de autorização formal e específica do cliente, com manifestação prévia do Encarregado de Proteção de Dados.
PRI-02	A interface de programação do provedor de modelo é configurada para não retenção de dados e não utilização para treinamento, com previsão contratual correspondente.
PRI-03	Prompts não são retidos após o processamento da requisição, salvo registro de auditoria interno, com retenção controlada conforme a política de retenção de logs da UpFlux.
PRI-04	Cada requisição é processada em contexto isolado, sem compartilhamento entre organizações.
PRI-05	Antes do envio ao modelo de linguagem, aplica-se higienização de contexto, com remoção ou mascaramento de dados pessoais e de dados de saúde, além da minimização do contexto ao estritamente necessário à tarefa.
PRI-06	A hospedagem em nuvem na região us-east-2, nos Estados Unidos, e a utilização de provedor de modelo de linguagem sediado no exterior caracterizam transferência internacional de dados pessoais, nos termos dos artigos 33 a 36 da LGPD e do Regulamento de Transferência Internacional de Dados aprovado pela Resolução nº 19/2024 da ANPD. A UpFlux declara essa condição de forma expressa em seus questionários de segurança e no Registro de Atividades de Tratamento. As salvaguardas aplicadas estão detalhadas na seção 16.1.
PRI-07	A relação de suboperadores envolvidos no tratamento é disponibilizada contratualmente e mantida atualizada pelo Encarregado de Proteção de Dados.
PRI-08	O titular tem direito à revisão de decisões automatizadas, nos termos do artigo 20 da LGPD. Saídas do assistente são recomendações sujeitas a validação, o que preserva o ponto de decisão humana.
PRI-09	A anonimização e a pseudonimização são capacidades configuráveis, aplicadas conforme o desenho acordado com cada cliente, e podem ser executadas na origem, antes do envio à plataforma.
PRI-10	O cliente controla exclusões parciais e totais da sua base dedicada, bem como a política de backup e de recuperação.
PRI-11	Funcionalidade que trate dados pessoais é submetida a Relatório de Impacto à Proteção de Dados aprovado pelo Encarregado antes da disponibilização.
PRI-12	Toda saída do assistente passa por filtros de prevenção de vazamento antes da apresentação. Saídas reprovadas são bloqueadas e encaminhadas para revisão, com registro do bloqueio.

16.1 Salvaguardas aplicáveis à transferência internacional

As salvaguardas abaixo são aplicadas de forma cumulativa a toda transferência internacional decorrente da operação do Nous.

Salvaguarda	Descrição
Instrumento contratual de transferência	Incorporação das cláusulas-padrão contratuais aprovadas pela ANPD, na forma do Anexo II da Resolução nº 19/2024, aos instrumentos firmados com cada suboperador que receba dados no exterior.
Contrato de tratamento de dados	Firmado com cada suboperador, com obrigações de confidencialidade, restrição de finalidade, segurança da informação, notificação de incidentes e vedação de tratamento posterior incompatível com a finalidade informada.

Salvaguarda	Descrição
Não retenção e não treinamento	Interface de programação do provedor de modelo configurada para não retenção de dados e não utilização do conteúdo para treinamento, com previsão contratual correspondente.
Criptografia em todo o percurso	TLS 1.2 ou superior em trânsito e AES-256 em repouso, incluindo o trecho de comunicação com o provedor de modelo.
Minimização e higienização	Envio apenas do contexto estritamente necessário à tarefa, com remoção ou mascaramento de dados pessoais e de dados de saúde antes do envio ao modelo.
Avaliação prévia do suboperador	Análise de política de uso de dados, localização de processamento, retenção, subcontratação e controles de segurança do provedor antes da contratação, com reavaliação periódica.
Registro e transparência	A operação é registrada no Registro de Atividades de Tratamento, com finalidade, país de destino, categorias de dados e base legal. A íntegra das cláusulas relativas à transferência é disponibilizada ao titular que a solicite, no prazo de 15 dias, observados os segredos comerciais e industriais.
Canal de atendimento ao titular	Solicitações relativas à transferência internacional são recebidas pelo canal do Encarregado de Proteção de Dados e respondidas nos prazos legais.

17. Regras de registro e auditoria

ID	Regra
AUD-01	A central de segurança disponibiliza auditoria de acessos exportável pela organização cliente.
AUD-02	Rotinas mantêm histórico de execuções, com estado, origem automática ou manual e duração.
AUD-03	A aplicação mantém registro de auditoria estruturado e observabilidade de desempenho, com rastreamento das execuções do modelo e métricas de qualidade e consumo.
AUD-04	A retenção e a imutabilidade dos registros seguem a política de retenção de logs da UpFlux, com proteção contra alteração indevida e disponibilidade para auditorias e investigações.
AUD-05	Registros de auditoria relacionados a autenticação e manutenção de dados podem ser consumidos por interface de programação, apoiando a rastreabilidade no ambiente do cliente.

18. Limites operacionais e requisitos de ambiente

18.1 Limites operacionais

ID	Regra
LIM-01	O consumo é vinculado ao pacote contratado pela organização e acompanhado no menu Consumo.
LIM-02	Há limite de taxa de requisições por minuto no motor de execução.
LIM-03	Rotina pausada automaticamente após três falhas consecutivas.
LIM-04	Intervalo mínimo de atualização automática de Visão: 15 segundos.

18.2 Requisitos mínimos do console web

Categoria	Mínimo	Recomendado
Navegador desktop	Chrome 90 ou superior é o recomendado, por melhor desempenho na renderização de diagramas e gráficos. Firefox 88 ou superior é suportado, com desempenho inferior na renderização gráfica. Edge 90 ou superior é suportado. Safari 14 ou superior tem suporte limitado por restrições de WebGL. Internet Explorer não é suportado.	Chrome 90 ou superior
Navegador mobile	iOS Safari 14 ou superior, Chrome Android 90 ou superior e Samsung Internet 13 ou superior são suportados. Firefox Mobile 88 ou superior tem suporte limitado.	Chrome Android ou iOS Safari em versão atual
Processador	i3 ou Ryzen 3, com dois núcleos ou mais	i5 ou Ryzen 5, com quatro núcleos ou mais. Para alto volume de dados, i7 ou Ryzen 7 com oito núcleos ou mais
Memória	4 GB	8 GB. Para alto volume de dados, 16 GB
Gráficos	WebGL 1.0	WebGL 2.0 com 1 GB de memória de vídeo. Para alto volume de dados, GPU dedicada com WebGL 2.0
Resolução	1024 por 768	1920 por 1080. Para alto volume de dados, 2560 por 1440
Conectividade	Acesso HTTPS na porta 443 aos endpoints da UpFlux. Não há dependência de VPN para o usuário final.	Conexão corporativa estável

19. Gestão de mudanças e versionamento

ID	Regra
CIC-01	Prompts de sistema e configurações de recuperação de contexto são artefatos versionados, com validação de integridade no pipeline antes da implantação. Toda alteração passa por revisão e aprovação.
CIC-02	O backend do assistente mantém suíte de testes automatizados, incluindo testes específicos de segurança do ambiente isolado de execução de código.
CIC-03	Cada versão principal passa por testes de injeção de prompt com cargas conhecidas e por exercício de red team antes da liberação.
CIC-04	Implantação controlada, com ativação gradual, possibilidade de reversão e monitoramento intensivo no período subsequente.
CIC-05	Mudança que altere o provedor ou a família de modelo, introduza nova ferramenta acessível ao modelo, ou introduza novo canal de entrega de dados, é submetida ao Comitê de Segurança da Informação e reflete-se na atualização deste documento.
CIC-06	O descomissionamento de integração com provedor de modelo exige confirmação contratual de expurgo dos dados no provedor.

20. Restrições rígidas consolidadas

As restrições abaixo não são contornáveis por configuração e devem ser consideradas em qualquer desenho de solução sobre o Nous.

- O destino da conversa é imutável após a primeira mensagem.

- Somente análises de playbook podem ser promovidas a Visão.
- Comandos existem apenas se publicados na configuração do processo.
- Rotina é pausada automaticamente após três falhas consecutivas.
- Rotina exige pelo menos um canal de entrega.
- O contexto conversacional não é compartilhado entre conversas distintas.
- A consulta de dados pelo modelo é somente leitura e aceita apenas instruções de seleção.
- A execução de código pelo modelo não tem acesso a rede nem ao sistema de arquivos.
- Internet Explorer não é suportado.

21. Conformidade, referências e contato

Legislação e regulação aplicável

LGPD, Lei nº 13.709/2018, com atenção ao artigo 20, sobre revisão de decisões automatizadas, e aos artigos 33 a 36, sobre transferência internacional. Regulamento de Transferência Internacional de Dados, aprovado pela Resolução nº 19/2024 da ANPD. Normas setoriais aplicáveis ao contexto de cada cliente, incluindo as da ANS e os padrões TISS e TUSS no setor de saúde.

Referências metodológicas

Os frameworks abaixo são utilizados como referência na definição e na avaliação dos controles descritos neste documento, e não como declaração de conformidade certificada.

- OWASP Top 10 for LLM Applications.
- ISO/IEC 42001:2023, sistema de gestão de inteligência artificial.
- ISO/IEC 27001, controles de segurança da informação.
- NIST AI Risk Management Framework 1.0.
- MITRE ATLAS.

Sobre certificações. Na data desta versão, a UpFlux não possui certificação formal nem relatório de auditoria independente de terceira parte em ISO/IEC 27001, ISO/IEC 42001 ou SOC 2. Os frameworks citados são adotados como referência metodológica na construção dos controles. A verificação independente do programa de segurança é feita por testes de intrusão semestrais, executados por empresa especializada externa, cujo sumário executivo é disponibilizado a clientes mediante acordo de confidencialidade.

O conjunto de políticas internas de Segurança da Informação, privacidade e governança de inteligência artificial que sustentam este documento é disponibilizado a clientes e prospects mediante acordo de confidencialidade.

Contato para questões de privacidade e proteção de dados: dpo@upflux.net

22. Histórico de revisões

Versão	Data	Tipo	Descrição
1.0	25/05/2026	Emissão	Publicação inicial das regras técnicas do assistente inteligente UpFlux Nous.