

ANEXO XX - PROCEDIMENTO DE AUTORIZAÇÃO, CONTROLE E REGISTRO DO USO DE IA

Regra padrão: O uso de IA é proibido até que exista autorização expressa e específica. A autorização de uma ferramenta não se estende automaticamente a outra versão, finalidade, ambiente, categoria de informação, integração ou Ordem de Serviço.

1. OBJETIVO E ABRANGÊNCIA

1.1 - Este Anexo disciplina a solicitação, avaliação, autorização, utilização, registro, fiscalização, suspensão e encerramento do uso de ferramentas, modelos ou serviços de IA como apoio à execução contratual. Aplica-se a todos os profissionais, vínculos, ambientes e artefatos da CONTRATADA.

1.2 - O desenvolvimento assistido por IA não se confunde com a implementação de funcionalidade de IA no produto. Quando a IA integrar o software entregue, também se aplicará a seção 9 deste Anexo.

2. RESPONSABILIDADES

Papel	Responsabilidades mínimas
Gestor do Contrato	Decidir sobre a autorização, condicionamento, suspensão ou revogação, com base nas manifestações técnicas e de risco; assegurar o registro no processo de fiscalização.
Fiscal Técnico	Avaliar necessidade, adequação técnica, finalidade, ambiente, controles, evidências e impacto no processo de desenvolvimento; fiscalizar o uso e os artefatos.
Área requisitante / Product Owner	Validar a aderência à finalidade de negócio e os critérios de aceite, especialmente quando a IA integrar o produto entregue.
Instâncias de segurança, privacidade e dados	Manifestar-se quando houver processamento externo, informação não pública, dado pessoal, integração relevante ou risco que exija avaliação especializada.
CONTRATADA / Preposto	Solicitar autorização, comprovar controles, orientar profissionais, manter registros, comunicar incidentes e responder integralmente pelos usos e resultados.
Profissional validador	Revisar o resultado, executar verificações, registrar evidências e assumir responsabilidade técnica por sua incorporação ao artefato.

3. PROCEDIMENTO DE AUTORIZAÇÃO

3.1 - A CONTRATADA apresentará solicitação antes do primeiro uso e antes de qualquer mudança relevante, utilizando o formulário da seção 10.1.

3.2 - A solicitação identificará ferramenta, provedor, versão, modalidade de contratação, finalidade, atividades, usuários, ambiente, integrações, categorias de informação, processamento externo, retenção, uso para treinamento, compartilhamento, licenças, controles, custos e profissional responsável pela validação.

3.3 - O Fiscal Técnico analisará a compatibilidade com a OS, o processo de desenvolvimento, a arquitetura, a segurança, a privacidade, a propriedade intelectual, os critérios de aceite e a capacidade de fiscalização.

3.4 - Quando houver dado pessoal, informação não pública, processamento externo ou integração relevante, a decisão dependerá de avaliação de riscos e das manifestações institucionais aplicáveis.

3.5 - A decisão será formalizada no formulário da seção 10.2 e vinculada à OS. Poderá autorizar, autorizar com condicionantes, rejeitar, suspender ou revogar o uso.

3.6 - Autorização genérica, silêncio, uso anterior, disponibilidade comercial, licença adquirida ou menção da ferramenta em catálogo não substituem a decisão expressa.

4. VEDAÇÕES

4.1 - Inserir dados pessoais, informações não públicas, credenciais, segredos, chaves, códigos-fonte, requisitos, regras de negócio, arquitetura, vulnerabilidades, logs, bases, documentos ou artefatos da PREVIC em serviço público, gratuito, compartilhado ou não autorizado.

4.2 - Utilizar informação da PREVIC para treinamento, ajuste, aperfeiçoamento ou avaliação de modelo de terceiro sem autorização específica.

4.3 - Permitir retenção, compartilhamento, reutilização, acesso humano pelo provedor ou transferência a suboperador em desacordo com as condições autorizadas.

4.4 - Incorporar resultado sem revisão humana, ocultar o uso de IA, suprimir evidências, contornar controles, utilizar conta pessoal ou compartilhar credenciais.

4.5 - Implantar autonomamente em produção, executar decisão automatizada sem supervisão prevista ou introduzir componente, dado ou conteúdo sem licença compatível.

5. CONTROLES MÍNIMOS

Controle	Requisito
Conta e acesso	Conta corporativa, menor privilégio, autenticação adequada, usuários identificados e revogação tempestiva.
Dados e conteúdo	Classificação prévia, minimização, anonimização ou dados sintéticos quando cabível e proibição de conteúdo não autorizado.
Retenção e treinamento	Condição comprovada de retenção compatível, exclusão segura e não utilização para treinamento, quando exigido.
Segurança	Criptografia aplicável, segregação, registros de eventos, proteção de segredos, gestão de integrações e resposta a incidentes.
Qualidade	Revisão humana, testes, análise estática, dependências, vulnerabilidades, desempenho, acessibilidade e documentação conforme o artefato.
Propriedade intelectual	Verificação de licenças, procedência, atribuições e direitos suficientes para uso, manutenção, modificação e evolução pela PREVIC.
Rastreabilidade	Relação entre OS, história ou atividade, ferramenta, finalidade, artefato, validador, verificações e decisão de aceite.
Fiscalização	Evidências acessíveis à CONTRATANTE e preservadas pelo prazo contratual e legal aplicável, sem exposição desnecessária de conteúdo protegido.

6. VALIDAÇÃO E ACEITE

6.1 - O profissional qualificado revisará integralmente o resultado e documentará as verificações realizadas. A identificação do validador não transfere a responsabilidade da CONTRATADA.

6.2 - O artefato assistido por IA cumprirá os mesmos critérios técnicos, funcionais, de segurança, privacidade, acessibilidade, desempenho, documentação e propriedade intelectual dos demais artefatos.

6.3 - O registro de IA não constitui produto autônomo, não recebe SPP e não altera a pontuação da história. Retrabalho ou correção decorrente do uso de IA não gera nova contagem ou custo adicional.

6.4 - A fiscalização poderá solicitar evidência adicional proporcional ao risco. O comando integral somente será exigido quando necessário e seguro; quando não for adequado preservá-lo, poderão ser utilizados resumo controlado, identificador, hash, referência da sessão ou evidência equivalente.

7. REGISTRO AUDITÁVEL

7.1 - Cada uso material de IA será registrado na ferramenta oficial ou no formulário da seção 10.3 antes do aceite do artefato. Usos repetitivos sob a mesma autorização poderão ser agrupados por sprint ou lote, desde que preservada a identificação dos artefatos e validadores.

7.2 - A CONTRATADA assegurará integridade, completude, disponibilidade e rastreabilidade dos registros. A ausência ou inconsistência relevante impedirá o aceite do artefato até saneamento.

8. INCIDENTE, SUSPENSÃO E DESCONTINUAÇÃO

8.1 - A CONTRATADA comunicará imediatamente suspeita ou confirmação de uso não autorizado, exposição, vazamento, retenção indevida, alteração de condição do provedor, comprometimento de conta, licença incompatível ou outro incidente relacionado à IA.

8.2 - A CONTRATADA interromperá o uso, revogará acessos quando cabível, preservará evidências, identificará informações e artefatos afetados, executará contenção e correção e preencherá o registro da seção 10.4.

8.3 - A CONTRATANTE poderá suspender ou revogar a autorização a qualquer tempo por risco, incidente, mudança de condição, desconformidade, insuficiência de evidências ou necessidade institucional.

8.4 - A suspensão não gera reembolso, revisão de preço ou indenização quando decorrer da escolha da ferramenta pela CONTRATADA, de alteração previsível de seus termos ou de desconformidade imputável à CONTRATADA.

9. IA COMO FUNCIONALIDADE DO PRODUTO

9.1 - Quando a IA integrar o software entregue, a OS deverá completar a matriz abaixo, sem prejuízo das demais exigências deste Anexo.

Dimensão	Definição obrigatória na OS
Finalidade e escopo	Problema, usuários, decisões apoiadas, usos permitidos e usos proibidos.
Dados	Fontes, base legal, qualidade, representatividade, preparação, atualização e restrições.

Dimensão	Definição obrigatória na OS
Validação	Métricas, limiares, conjuntos de teste, critérios de aceite e responsável.
Vieses e impactos	Grupos ou situações afetadas, testes, limitações e medidas de mitigação.
Explicabilidade e reprodutibilidade	Documentação, versionamento, parâmetros, rastreabilidade e explicação adequada ao risco.
Supervisão humana	Ponto de intervenção, decisão final, possibilidade de contestação e tratamento de exceções.
Segurança e privacidade	Ameaças, controles, dados pessoais, retenção, acesso, logs e incidentes.
Operação	Monitoramento, deriva, desempenho, atualização, reversão, desativação e responsabilidades.

10. FORMULÁRIOS

10.1 Solicitação de autorização

Campo	Preenchimento
Contrato / OS / sprint	<Identificação>
Ferramenta / provedor / versão	<Identificação exata>
Licença / modalidade / custos	<Plano, titularidade e confirmação de inclusão nos preços>
Finalidade e atividades	<Delimitar>
Usuários / perfis	<Identificar>
Ambiente / integração	<Tenant, região, API, extensão, repositório ou IDE>
Categorias de informação	<Permitidas, proibidas e classificação>
Processamento externo / suboperadores	<Descrição>
Retenção / treinamento / compartilhamento	<Termos e evidências>
Controles de segurança e privacidade	<Descrição e anexos>
Propriedade intelectual	<Licenças, termos e verificações>
Validador humano	<Nome, perfil e identificação>
Riscos e mitigação	<Descrição>
Responsável da CONTRATADA	<Nome, assinatura e data>

10.2 Decisão da CONTRATANTE

Campo	Registro
Resultado	☐ Autorizado ☐ Autorizado com condições ☐ Não autorizado ☐ Suspenso ☐ Revogado
Escopo da autorização	<Ferramenta, versão, finalidade, ambiente, usuários e informações>
Condições e vedações	<Registrar>

Campo	Registro
Validade / reavaliação	<Período ou evento>
Manifestações consideradas	<Fiscalização, segurança, privacidade, requisitante e outras>
Gestor do Contrato	<Nome, matrícula, decisão, data e assinatura>

10.3 Registro de uso e validação

Campo	Registro
ID / data / autorização	<Identificação>
OS / sprint / HU ou atividade	<Rastreabilidade>
Ferramenta / versão / ambiente	<Identificação>
Finalidade	<Descrição objetiva>
Informação utilizada	<Categorias; não reproduzir conteúdo protegido desnecessariamente>
Artefatos afetados	<Repositório, arquivo, versão, commit ou referência>
Validador humano	<Nome, perfil e identificação>
Qualidade e testes	<Revisões e evidências>
Segurança e dependências	<Verificações e evidências>
Propriedade intelectual	<Verificação e resultado>
Comando / sessão	<Resumo, ID, hash ou conteúdo integral quando exigido e seguro>
Resultado	[] Aprovado [] Corrigido [] Rejeitado [] Incidente

10.4 Registro de incidente ou desconformidade

Campo	Registro
Data / hora / comunicante	<Preencher>
Ferramenta / autorização / OS	<Identificar>
Descrição e informações afetadas	<Preencher>
Artefatos / usuários / ambientes afetados	<Preencher>
Contenção imediata	<Suspensão, revogação, preservação e outras medidas>
Comunicações realizadas	<Destinatários, datas e referências>
Análise de causa e impacto	<Preencher>
Correção / exclusão / recuperação	<Preencher>
Decisão da CONTRATANTE	<Manter, condicionar, suspender, revogar ou outras providências>
Encerramento	<Responsáveis, data, evidências e lições aprendidas>

11. DISPOSIÇÕES FINAIS

11.1 - Todos os custos da opção da CONTRATADA pelo uso de IA estão incluídos nos preços e não geram pagamento separado.

11.2 - A autorização não modifica SPP, produtividade, critérios de aceite, indicadores, PPA-mês, NMS ou remuneração. Qualquer calibração futura será prospectiva e sustentada por memória técnica baseada em sprints comparáveis.

11.3 - Este Anexo será interpretado em conjunto com o TR, a POSIN/PREVIC, a LGPD e os Anexos I, VII, XIV, XV, XVIII e XIX. Em caso de conflito, prevalecerá a regra mais protetiva aplicável e, quanto à execução contratual, o Termo de Referência.