

ANEXO XIV - ROTEIRO DE CODIFICAÇÃO E QUALIDADE

Abrangência: Aplica-se a código, scripts, infraestrutura como código, pipelines, consultas, componentes de dados, modelos, testes e documentação técnica, produzidos manualmente ou com auxílio de IA.

1. PRINCÍPIOS

- aderência à arquitetura, padrões e tecnologias autorizadas pela CONTRATANTE;
- código legível, modular, testável, documentado e sem duplicação desnecessária;
- segurança e privacidade desde o desenho, com mínimo privilégio e proteção de segredos;
- versionamento, revisão por pares e rastreabilidade entre OS, história, commit, build, teste e implantação;
- dependências identificadas, atualizadas, licenciadas e submetidas a análise de vulnerabilidades;
- mesmo nível de qualidade e responsabilidade para artefatos assistidos por IA.

2. CONTROLES OBRIGATÓRIOS

Dimensão	Critério mínimo	Evidência
Padrão e arquitetura	Conformidade com guia de estilo, arquitetura, APIs, integrações e padrões aprovados.	Revisão, decisão arquitetural, relatório de ferramenta.
Versionamento	Branch, commit e revisão associados à OS/história; vedado código fora do repositório oficial.	PR/MR, histórico e aprovação.
Segredos	Nenhuma credencial, chave, token ou dado sensível no código, prompt, log ou repositório.	Secret scan e inspeção.
Segurança	SAST, análise de dependências e testes compatíveis com o risco; correção de achados conforme severidade.	Relatórios e justificativas.
Testes	Testes unitários, integrados, funcionais, regressivos e não funcionais conforme OS.	Resultados e cobertura aplicável.
Dados	Validação, minimização, mascaramento, qualidade e rastreabilidade de dados.	Scripts, catálogo, relatório.
Desempenho	Atendimento aos requisitos mensuráveis e ausência de degradação não aceita.	Teste e comparação.
Acessibilidade	Conformidade com requisitos aplicáveis e correção dos achados.	Ferramenta e inspeção.
Documentação	Instruções de build, implantação, operação, rollback e manutenção atualizadas.	Documentos versionados.
Dependências e PI	Origem, versão e licença compatíveis; vedados componentes sem direitos de uso.	SBOM, licenças e análise.
IA autorizada	Ferramenta, versão, finalidade, ambiente e informação dentro da autorização da OS/ANEXO XX.	Registro auditável.

Dimensão	Critério mínimo	Evidência
Validação humana	Revisão integral do resultado de IA por profissional qualificado, sem implantação autônoma.	Validador, revisão, testes.
Proveniência de IA	Artefato afetado, uso material, verificações de licença, segurança e qualidade identificados.	Registro ANEXO XX e PR/MR.
Reprodutibilidade	Build, teste e implantação reproduzíveis em ambiente autorizado.	Pipeline, pacote e logs.
Eficiência e sustentabilidade	Eficiência mensurável, uso racional de CPU, memória, armazenamento, rede e energia; ausência de processamento, consultas, logs ou transferência de dados desnecessários.	Métricas, profiling, planos de execução, testes comparativos e justificativa técnica.

3. INTELIGÊNCIA ARTIFICIAL

3.1 - IA somente poderá ser usada nas condições expressamente autorizadas. Informações e códigos da CONTRATANTE não serão enviados a serviço não autorizado.

3.2 - Sugestão de IA será tratada como insumo não confiável até revisão humana, execução dos testes e aprovação nos controles deste Anexo.

3.3 - A CONTRATADA verificará vulnerabilidades, dependências inventadas, obsolescência, licenças, similaridade indevida, vazamento de informação e comportamento não documentado.

3.4 - Uso de IA não reduz teste, revisão, documentação ou responsabilidade e não gera SPP, prazo ou remuneração adicionais.

3.5 - Desconformidade imputável à CONTRATADA será corrigida sem custo e sem nova contagem, sem prejuízo do tratamento contratual cabível.

4. MATRIZ DE CONFORMIDADE E IQC

A OS definirá quais critérios são aplicáveis ao stack e ao artefato. Critério não aplicável exigirá justificativa.

A fiscalização poderá utilizar ferramenta automatizada, inspeção e amostragem.

ID	Critério	Aplicável?	Atendido?	Evidência / achado	Providência
1	Arquitetura e padrão	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
2	Versionamento e revisão	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
3	Segredos	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
4	SAST	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
5	Dependências/ SBOM	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
6	Testes	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
7	Dados e privacidade	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>

ID	Critério	Aplicável?	Atendido?	Evidência / achado	Providência
8	Desempenho	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
9	Acessibilidade	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
10	Documentação	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
11	Licenças/PI	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
12	IA autorizada	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
13	Validação humana de IA	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
14	Reprodutibilidade	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>
15	Eficiência e codificação sustentável	☐ Sim ☐ Não	☐ Sim ☐ Não	<Registrar>	<Registrar>

IQC: $IQC = 100 \times (Qrc/Qtr)$, em que Qrc é a quantidade de requisitos aplicáveis atendidos e Qtr a quantidade total de requisitos aplicáveis. Itens não aplicáveis, motivadamente, não integram Qtr.

5. CLASSIFICAÇÃO DOS ACHADOS

Cada achado deverá ser classificado por severidade e natureza, com fundamento objetivo, evidência, responsável e prazo. A classificação não substitui as faixas e fórmulas dos indicadores do TR; serve para priorizar correção, aceite e rastreabilidade.

Severidade	Critério	Tratamento mínimo
Crítica	Exploração ativa, exposição relevante, perda de integridade/disponibilidade, credencial/secredo exposto ou bloqueio de função essencial.	Correção imediata; não aceitar nem implantar; acionar resposta a incidente quando cabível.
Alta	Risco elevado de segurança, privacidade, indisponibilidade, defeito grave ou violação de requisito obrigatório.	Corrigir antes do aceite/implantação, salvo decisão formal excepcional da CONTRATANTE.
Média	Desvio material de qualidade, desempenho, acessibilidade, manutenibilidade ou conformidade, sem efeito crítico imediato.	Plano e prazo definidos; aceite condicionado somente quando o TR e o risco permitirem.
Baixa	Desvio localizado, sem comprometimento material imediato, mas que exige regularização ou registro.	Corrigir no prazo formalizado e acompanhar até o encerramento.

Natureza	Exemplos de enquadramento
Segurança e privacidade	Autenticação, autorização, criptografia, segredo, vulnerabilidade, dado pessoal, log e incidente.
Qualidade e arquitetura	Padrão, modularidade, duplicação, complexidade, rastreabilidade, observabilidade e aderência arquitetural.
Testes e desempenho	Cobertura, regressão, robustez, disponibilidade, latência e capacidade.

Natureza	Exemplos de enquadramento
Acessibilidade e usabilidade	Requisitos e evidências de acessibilidade, interação e experiência.
Dependências, licença e PI	SBOM, origem, versão, vulnerabilidade, licença e similaridade indevida.
IA	Autorização, informação usada, proveniência, validação humana, comportamento e registro auditável.
Eficiência e sustentabilidade	Consumo desnecessário de processamento, memória, armazenamento, rede, energia, consultas ou logs.
Documentação e entrega	Documentação mínima, instruções, evidência, versionamento e implantação.

O relatório de inspeção registrará, para cada achado: ID, OS/artefato, critério da matriz, severidade, natureza, evidência, responsável, prazo, situação e decisão de aceite.

6. ACEITE

A entrega somente será aceita quando os critérios aplicáveis estiverem demonstrados ou quando eventual exceção tiver sido formalmente aprovada pela autoridade competente. A aprovação de exceção não apaga o risco: deverá registrar fundamento, prazo, responsável, controle compensatório e plano de tratamento.

7. COBERTURA DE TESTES - ICT

7.1. A unidade de cobertura será a linha executável de código novo ou alterado no escopo da OS, identificada pela comparação entre a linha de base versionada e a versão entregue. Essa unidade é única para o indicador; não se somam instruções, ramificações, caminhos e elementos de dados como unidades equivalentes.

7.2. $ICT = 100 \times (Lc/Lt)$, em que Lt é o total de linhas executáveis elegíveis e Lc a quantidade dessas linhas executadas pelos testes automatizados. Na consolidação, somam-se os contadores Lc e Lt dos artefatos elegíveis, sem média simples de percentuais. Permanecem a meta de 100% e as faixas de ajuste previstas no TR.

7.3. A OS registrará repositório, versões de referência, ferramenta e versão, comando ou configuração de execução, escopo e exclusões justificadas. A apuração será reproduzível sobre o universo integral elegível. Amostragem poderá auditar evidências, mas não substituir Lt por uma amostra. Poderá ser usado procedimento equivalente que reproduza a medição integral na mesma unidade.

7.4. Excluem-se linhas em branco, comentários, bibliotecas de terceiros não alteradas, código preexistente não modificado, arquivos gerados automaticamente sem edição própria e conteúdo declarativo sem lógica executável. Código produzido ou alterado com auxílio de IA e incorporado à solução pela CONTRATADA permanece sujeito aos mesmos critérios do código de autoria humana.

7.5. Quando não houver linhas executáveis mensuráveis, inclusive em configuração visual sem código elegível, registrar ICT como não aplicável, com justificativa e evidências, preservados os testes funcionais e demais critérios de aceite. Ausência de testes, falha de instrumentação ou dificuldade de cobertura não justificam, por si só, excluir código elegível. Se $Lt = 0$, não haverá ajuste automático por ICT.

Campo	Registro obrigatório
OS / parcela / artefato / competência	<Preencher>
Linha de base e versão entregue	<Preencher>
Ferramenta, versão e configuração	<Preencher>
Lt: linhas executáveis elegíveis	<Preencher>

Campo	Registro obrigatório
Lc: linhas elegíveis executadas nos testes	<Preencher>
Exclusões e justificativas	<Preencher>
ICT e faixa do TR	<Preencher>
Evidência reproduzível e validação fiscal	<Preencher>