

ANEXO 4

ESCOPO DA CERTIFICADORA DE SEGURANÇA

Além do escopo acima mencionado, deve ser contratado o Serviço de Avaliação e Certificação Independente de Segurança Funcional, a ser realizada por Avaliador de Segurança Funcional Independente (ISA) devidamente acreditado, que assumirá a função de Certificadora de Segurança, aplicável exclusivamente aos seguintes subsistemas da Fase III da Linha 4 – Amarela do Metrô de São Paulo, até o Município de Taboão da Serra:

- Sinalização e Controle;
- Portas de Plataforma;
- Material Rodante.

O Serviço de Avaliação e Certificação Independente de Segurança Funcional Independente deve ter como objetivo assegurar a manutenção da conformidade da Linha 4 frente às modificações, ampliações e integrações introduzidas na Fase III, garantindo que tais alterações não comprometam a segurança operacional, a integridade do sistema nem a operação e manutenção da Linha existente e de sua extensão.

ESCOPO DE SISTEMAS, AVALIAÇÕES E CERTIFICAÇÃO PARA LINHA 4

A avaliação deve ser conduzida em conformidade com as normas CENELEC aplicáveis, em especial:

- **EN 50126-1 e EN 50126-2** – Processo RAMS e ciclo de vida;
- **EN 50128** – Software para sistemas ferroviários;
- **EN 50129** – Sistemas eletrônicos relacionados à segurança.

Destaca-se que o Avaliador de Segurança Funcional Independente deve certificar que a metodologia de demonstração de segurança funcional adotada para os subsistemas avaliados esteja alinhada aos mais altos padrões internacionais de segurança ferroviária, em conformidade com as normas CENELEC aplicáveis, assegurando sua correta aplicação ao longo de todo o Ciclo de Vida dos sistemas, até a fase de Aceite Final para operação.

O Avaliador de Segurança Funcional Independente deve avaliar de forma independente a adequação técnica, a integração e as interfaces:

- Entre os subsistemas de Sinalização e Controle, Portas de Plataforma e Material Rodante;
- Com sistemas externos ou terceiros que possuam interface física, lógica, operacional ou de dados com esses subsistemas, na medida em que tais interfaces possam impactar a segurança funcional, sem caracterizar ampliação de escopo para certificação de sistemas não listados.

Sem prejuízo do escopo da Certificação de Segurança Funcional Independente, limitada aos subsistemas acima definidos, no âmbito do mesmo contrato, o Avaliador de Segurança Funcional Independente deve realizar o Assessment de Cibersegurança aplicável a todo o sistema da Linha 4 – Amarela, abrangendo todas as suas fases (Fase I, Fase II e Fase III).

A avaliação deve ser conduzida com base na CLC/TS 50701 – *Railway Applications – Cybersecurity*, utilizando como referência técnica os requisitos aplicáveis da série IEC 62443, e deverá abranger, no mínimo, a avaliação da:

- Arquitetura técnica global do sistema da Linha 4;
- Interfaces internas e externas, incluindo interfaces entre subsistemas e com sistemas terceiros;
- Definição de zonas e condutos ao nível de sistema;

ESCOPO DE SISTEMAS, AVALIAÇÕES E CERTIFICAÇÃO PARA LINHA 4

- Ativos críticos e funções essenciais da linha;
- Cenários de ameaça e vulnerabilidades relevantes;
- Medidas de proteção e controles existentes, considerando os impactos à segurança funcional, disponibilidade, integridade operacional e continuidade do serviço ao longo de toda a linha.

O resultado formal da Avaliação de Cibersegurança deve ser a emissão de um Relatório de *Gap Analysis* de Cibersegurança, elaborado de forma independente pelo ISA, no qual serão:

- Identificadas as vulnerabilidades técnicas e organizacionais existentes no sistema da Linha 4;
- Evidenciadas as não conformidades e lacunas em relação aos requisitos da CLC/TS 50701 e às referências da IEC 62443;
- Apresentados os riscos residuais e seus potenciais consequências para a operação e segurança do sistema;
- Registradas recomendações técnicas de mitigação, sem caráter de certificação cibernética, aprovação de soluções ou emissão de certificado específico de cibersegurança.

A Avaliação de Segurança Funcional Independente, bem como todos os relatórios, pareceres, conclusões e demais documentos que a fundamentam, deverão ser emitidos por Certificadora de Segurança isenta de quaisquer conflitos de interesse, diretos ou indiretos, atuais ou potenciais, com os Empreendimentos da Fase III da Linha 4 – Amarela, bem como com quaisquer outros projetos, contratos ou empreendimento da Concessionária, independentemente de fase, linha ou escopo.

A Certificadora de Segurança deverá possuir acreditação válida e reconhecida, conforme aplicável, com base nas seguintes normas:

- **ISO 17011** - *Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies*;
- **ISO 17020** - *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*;
- **ISO 17025** - *Testing and calibration laboratories*;

ESCOPO DE SISTEMAS, AVALIAÇÕES E CERTIFICAÇÃO PARA LINHA 4

- **ISO 17065** - *Conformity assessment — Requirements for bodies certifying products, Processes and services.*

Para fins de caracterização do processo de Avaliação e Certificação de Segurança Funcional Independente, estabelece-se que o conjunto documental produzido ao longo do projeto constitui um corpo técnico integrado, estruturado por subsistema (Sinalização e Controle, Portas de Plataforma e Material Rodante) e consolidado em nível de sistema, composto por registros, análises, verificações e evidências desenvolvidas de forma progressiva ao longo do ciclo de vida da avaliação.

Nesse contexto, distinguem-se, quanto à sua natureza e finalidade, os documentos de caráter analítico e evolutivo — tais como relatórios intermediários (ISAR), Technical Notes, matrizes de verificação (clause by clause), relatórios de análise (gap analysis), registros de acompanhamento e demais evidências técnicas —, dos documentos de caráter conclusivo e formal, representados, para cada subsistema e para o sistema integrado, pelo Relatório Final de Avaliação de Segurança (Final Safety Assessment Report – FSAR) e pelos respectivos Certificados de Avaliação de Segurança.

Os documentos de natureza analítica e evolutiva têm como finalidade suportar, registrar e demonstrar o desenvolvimento do processo de avaliação, incluindo a identificação de pendências, iterações técnicas, esclarecimentos e consolidação progressiva das evidências, não refletindo, por sua própria natureza, posicionamento conclusivo ou julgamento definitivo da Certificadora de Segurança, seja em nível de subsistema ou de sistema.

A manifestação formal, conclusiva e juridicamente válida quanto à conformidade é expressa exclusivamente por meio dos documentos finais de certificação aplicáveis a cada subsistema e ao sistema integrado, os quais consolidam e integram o resultado de todo o processo avaliativo. Assim, qualquer análise, interpretação ou entendimento técnico do conjunto documental deve

ESCOPO DE SISTEMAS, AVALIAÇÕES E CERTIFICAÇÃO PARA LINHA 4

necessariamente considerar essa estrutura por níveis e distinção de natureza e finalidade, assegurando-se que conclusões formais sejam fundamentadas nos instrumentos conclusivos de certificação e não em registros intermediários de caráter evolutivo.

O tratamento como um corpo técnico integrado visa garantir a rastreabilidade, a coerência técnica e a unicidade de interpretação do processo de avaliação, tanto em nível de subsistema quanto do sistema global, evitando leituras parciais, descontextualizadas ou inconsistentes dos documentos produzidos ao longo do ciclo de vida do projeto.