



GUIA OPERACIONAL DE COMPLIANCE E SEGURANÇA EM PROCESSOS DE CERTIFICAÇÃO - FEBRACON 2026

Diretrizes Técnicas de Proctoring e Governança Operacional para Exames de Certificação
Profissional

1. Objetivo do Guia

Este documento estabelece os padrões rigorosos de integridade, segurança e conformidade que devem reger todos os processos de certificação conduzidos pela **Febracon**. O objetivo primordial é a mitigação proativa de fraudes, garantindo a legitimidade dos certificados emitidos e a conformidade irrestrita com a **Lei Geral de Proteção de Dados (LGPD)**. Através da implementação de tecnologias de monitoramento avançado e protocolos operacionais padronizados, busca-se assegurar a isonomia entre os candidatos e a proteção da reputação institucional do setor de correspondentes bancários.

2. Escopo de Aplicação

As diretrizes contidas neste guia aplicam-se integralmente a todas as modalidades de exames de certificação operacionalizados pela Febracon, abrangendo:

- Exames presenciais realizados em centros de testes homologados.
- Exames virtuais (remotos) realizados via plataforma de *Proctoring*.
- Processos de renovação de certificação e provas de nivelamento técnico.
- Todos os colaboradores, prestadores de serviço tecnológicos e candidatos envolvidos no ciclo de vida da certificação.

3. Procedimentos para Provas Presenciais

A segurança em ambientes físicos exige controle rigoroso de acesso e supervisão humana qualificada para evitar irregularidades durante a aplicação dos exames.

3.1. Verificação de Identidade

O candidato deve apresentar obrigatoriamente um documento oficial de identificação com foto (RG,



CNH ou Passaporte) em meio físico ou digital oficial. A conferência deve ser realizada individualmente pelo fiscal, validando a autenticidade do documento e a fisionomia do portador antes do ingresso na sala de prova.

3.2. Inspeção de Ambiente e Controle de Acesso

As salas de prova devem ser isoladas acusticamente e livres de materiais didáticos, cartazes ou qualquer elemento que possa auxiliar o candidato. O acesso é restrito a candidatos agendados e fiscais autorizados, sendo proibida a entrada de acompanhantes ou circulação de terceiros durante o período de aplicação.

3.3. Treinamento de Fiscais (Proctors) e Evidências

Todos os fiscais devem passar por treinamento de **Compliance Operacional**, focado na detecção de comportamentos suspeitos e manuseio de incidentes. É obrigatória a coleta de assinaturas em lista de presença física e a lavratura de ata de sala, registrando qualquer intercorrência ou atraso.

3.4. Restrição de Materiais e Dispositivos

É terminantemente proibido o porte de dispositivos eletrônicos (smartphones, smartwatches, tablets), calculadoras não autorizadas, bolsas ou materiais de consulta. Tais itens devem ser armazenados em armários lacrados ou envelopes de segurança fornecidos pela aplicação antes do início do exame.

4. Procedimentos para Provas Virtuais (Módulo Proctoring 2026)

Baseado nas diretrizes técnicas da **Fábrica de Provas 2026**, o sistema de monitoramento remoto utiliza Inteligência Artificial para garantir a segurança do ambiente digital.

4.1. Reconhecimento Facial e Monitoramento Contínuo

O sistema realiza a captura biométrica inicial para comparação com o documento de identidade. Durante toda a prova, a IA monitora a presença do candidato em frente à câmera, detectando a ausência do usuário, a presença de terceiros no ambiente ou tentativas de substituição de pessoa.

4.2. Monitoramento de Tela e Navegação

A plataforma detecta a troca de abas no navegador ou a abertura de janelas secundárias e demais programas. Estão bloqueados comandos de sistema como **Ctrl+C** / **Ctrl+V**. Qualquer tentativa de desvio de foco da janela da prova gera um alerta no log de auditoria.



4.3. Registro de Evidências e Consentimento LGPD

Ocorre a gravação sincronizada de vídeo (webcam), áudio ambiente e *screencast* (captura de tela). Antes do início, o candidato deve fornecer o **Consentimento Informado Digital**, aceitando o tratamento de seus dados biométricos e gravações exclusivamente para fins de auditoria e segurança do exame, conforme os preceitos da LGPD.

5. Controles de Compliance e Segurança

A governança dos dados e a análise pós-prova são fundamentais para a validade jurídica do processo de certificação.

5.1. Relatório Auditável e Dossiê do Candidato

Para cada exame, é gerado um dossiê digital contendo a linha do tempo completa de eventos (logs de acesso, horários de resposta, alertas de IA e capturas de tela). Este relatório serve como prova material em caso de contestações judiciais ou administrativas.

5.2. Classificação de Nível de Risco

O sistema classifica automaticamente as provas em dois níveis de risco para revisão humana:

- **Médio:** Alertas pontuais (ex: desvio momentâneo de olhar).
- **Alto:** Violações críticas (ex: troca de aba, detecção de outra pessoa, bloqueio de câmera).

5.3. Criptografia e Logs Administrativos

Todos os dados sensíveis e evidências de vídeo são armazenados com criptografia de ponta a ponta. O acesso administrativo aos logs é restrito a auditores da Febracon, com registro de *log* de quem acessou, quando e para qual finalidade.

6. Riscos e Mitigação

Risco Identificado	Estratégia de Mitigação	Ferramenta Aplicada
Fraude de Identidade	Validação biométrica e conferência documental rigorosa.	IA de Reconhecimento Facial
Uso de Dispositivos Ocultos	Inspeção de ambiente e	Gravação de Webcam e

Endereço: R. José Maria Lisboa, 860 - 30 andar cj 33 jd - Jardim Paulista, São Paulo - SP, 01423-001
Telefone: (11) 91288-5487 - contato@febracon.org.br - <https://www.febracon.org.br/> -



	monitoramento de áudio e tela.	Microfone
Falhas Técnicas de Conexão	Checklist de hardware pré-prova e suporte em tempo real.	Módulo de Diagnóstico Técnico

7. Matriz de Responsabilidades

7.1. Febracon

Responsável pela governança macro, definição das regras de negócio, homologação de conteúdos e auditoria final dos resultados. Cabe à federação a decisão soberana sobre a anulação de provas em caso de fraude comprovada.

7.2. Candidato

Responsável por garantir um ambiente privado, silencioso e iluminado para a prova, além de possuir hardware compatível. Deve cumprir rigorosamente as normas de conduta, sob pena de desclassificação imediata.

7.3. Provedor Tecnológico (Fábrica de Provas)

Responsável pela disponibilidade da plataforma, integridade dos algoritmos de IA, segurança cibernética dos dados armazenados e suporte técnico operacional aos candidatos e fiscais.

8. Conclusão e Recomendações Finais

A segurança dos processos de certificação da Febracon em 2026 baseia-se na convergência entre tecnologia de ponta e processos operacionais rígidos. A recomendação central é a manutenção da **rastreabilidade total** de cada exame, permitindo que qualquer certificação emitida possa ser validada e auditada a qualquer tempo. Este guia deve ser revisado anualmente para incorporar novas defesas contra ameaças emergentes à integridade acadêmica e profissional.

Diretoria de Compliance e Certificação — Febracon

Endereço: R. José Maria Lisboa, 860 - 3o andar cj 33 jd - Jardim Paulista, São Paulo - SP, 01423-001
Telefone: (11) 91288-5487 - contato@febracon.org.br - <https://www.febracon.org.br/> -



Anexo I – Protocolos Técnicos de Segurança (Fábrica de Provas 2026)

Este anexo detalha as especificações técnicas e os protocolos de segurança cibernética implementados pela **Fábrica de Provas** para a **Febracon**, conforme as diretrizes de 2026.

A1. Requisitos Técnicos de Hardware e Software

Para garantir a estabilidade do monitoramento via *Proctoring*, o ambiente do candidato deve atender aos seguintes critérios mínimos:

- **Processador:** Mínimo de 2.0 GHz (Dual-core ou superior).
- **Memória RAM:** Mínimo de 4GB disponíveis.
- **Conexão de Internet:** Banda larga estável com velocidade mínima de **5 Mbps** de upload/download.
- **Periféricos:** Webcam com resolução mínima de **720p** e microfone funcional.
- **Navegador:** Versão mais recente do Google Chrome ou Microsoft Edge com suporte a extensões de segurança.

A2. Algoritmos de Inteligência Artificial e Monitoramento Comportamental

O sistema utiliza redes neurais convolucionais para análise em tempo real:

1. **Eye-Tracking (Rastreamento Ocular):** Identifica padrões de desvio de olhar para fora da área da prova por períodos superiores a **5 segundos**.
2. **Deteção de Objetos:** Identificação automática de smartphones, livros, fones de ouvido e outras pessoas no campo de visão da câmera.
3. **Análise de Áudio:** Filtros de ruído para identificar conversas humanas ou comandos de voz, ignorando ruídos brancos ambientais.
4. **Verificação de Integridade de Processos:** Monitoramento de processos em segundo plano para detectar softwares de acesso remoto (ex: AnyDesk, TeamViewer).

A3. Segurança de Dados e Criptografia

- **Tráfego de Dados:** Toda a comunicação entre o terminal do candidato e os servidores da Fábrica de Provas é protegida por protocolo **TLS 1.3 ou TLS 1.2**.



- **Armazenamento:** As evidências de vídeo e áudio são armazenadas em servidores com criptografia **AES-256** em repouso.

A4. Fluxo de Resposta a Incidentes Técnicos

Em caso de queda de conexão ou falha de hardware:

- O sistema permite até **3 tentativas** de reconexão automática dentro de um intervalo de **10 minutos** de forma configurável.
- Cada desconexão é registrada com um *timestamp*.

A5. Auditoria e Retenção de Provas

Conforme a política de governança da **Febracon**, todos os logs e gravações de exames serão mantidos em ambiente seguro por um período de **5 anos**, permitindo auditorias retroativas em processos de investigação de fraude ou renovação de selos de qualidade.