PAN-AMERICAN CONGRESS OF AEROSPACE MEDICINE

Congresso Pan-Americano de Medicina Aeroespacial

ESPECIFICAÇÃO TÉCNICA E OPERACIONAL Nº 001/2026

SISTEMA DE EMISSÃO E VALIDAÇÃO DE CERTIFICADOS

Documento de requisitos funcionais, segurança, governança e validação pública

Entidade responsável	PACAM PARAGUAY E.A.S.
RUC	80173825-3
Código interno	CERT-SYS-001/2026
Evento	PACAM 2027 - Pan-American Congress of Aerospace Medicine
Documentos relacionados	Projeto Acadêmico; Regulamento de Frequência e Certificação; POP de Controle de Presença; Modelo Oficial de Certificado
Carga científico-acadêmica vigente	18 horas e 50 minutos
Frequência mínima do certificado geral	75% - mínimo operacional de 14h10 na grade vigente
Versão	1.0
Emissão	07 de outubro de 2026

Documento de especificação para contratação, desenvolvimento, homologação e operação do sistema

1. FINALIDADE E ESCOPO

A presente Especificação define os requisitos mínimos do sistema digital responsável por gerar, registrar, disponibilizar, reemitir, cancelar e validar publicamente os certificados do PACAM 2027. O sistema deverá integrar-se ao processo acadêmico já estabelecido, utilizando como fonte de verdade a base de frequência consolidada e aprovada pela Secretaria Acadêmica e pela Comissão Acadêmica.

O sistema deve ser adequado tanto para a emissão individual quanto para lotes de certificados, preservar a rastreabilidade de cada ato, reduzir a possibilidade de fraude documental e oferecer a universidades, empregadores, conselhos profissionais e demais entidades recebedoras um mecanismo simples de confirmação de autenticidade.

Princípio central

O QR Code e o código público de validação devem permitir confirmar a autenticidade do certificado sem expor CPF, documento de identidade, e-mail, telefone, data de nascimento ou outros dados pessoais desnecessários.

2. DOCUMENTOS E DADOS DE ORIGEM

• Projeto Acadêmico-Científico do PACAM 2027, que define evento, programação, carga acadêmica e responsáveis.

• Portaria de Constituição e Designação da Comissão Acadêmica e dos Responsáveis Técnicos.

• Regulamento de Frequência, Carga Horária e Certificação, que estabelece os critérios de elegibilidade e emissão.

• POP de Controle de Presença e Frequência, que define a captura, correção, auditoria e fechamento dos registros.

• Modelo Oficial de Certificado PACAM 2027, que contém os campos dinâmicos e a apresentação institucional.

• Base final de participantes, contendo identificação, carga efetivamente certificada, frequência, modalidade e status de elegibilidade.

Nenhum certificado deverá ser emitido diretamente a partir de dados preliminares de inscrição ou de registros de frequência ainda não consolidados.

3. VISÃO GERAL DA SOLUÇÃO

Componente	Função
Módulo de Administração	cadastros, perfis, parâmetros, templates, lotes e permissões.
Módulo de Importação Acadêmica	recebe a base final de frequência e executa validações de consistência.

Componente	Função
Motor de Certificação	calcula elegibilidade, preenche o modelo, gera PDF e registra versão e hash.
Repositório de Certificados	mantém o arquivo oficial, metadados, versões e status.
Portal Público de Validação	permite consulta por QR Code ou dados de validação sem autenticação do consulente.
Módulo de Reemissão/Cancelamento	controla correções, substituições, cancelamentos e justificativas.
Trilha de Auditoria	registra ações administrativas, alterações, aprovações e eventos técnicos relevantes.
Serviços de Segurança	autenticação, autorização, MFA, backups, criptografia, monitoramento e proteção contra abuso.

Fluxo lógico

Base de frequência fechada -> validação de elegibilidade -> aprovação do lote -> geração do certificado -> assinatura/selagem -> publicação da validação -> entrega ao participante -> auditoria e eventual reemissão/cancelamento.

4. PADRÃO DO CÓDIGO ÚNICO DO CERTIFICADO

4.1 Código público visível

Cada certificado deverá receber um identificador público aleatório e permanente, independente do número de inscrição do participante e independente da chave interna do banco de dados.

Formato recomendado

PACAM27-C-XXXX-XXXX-XXXX-XXXX
Exemplo: PACAM27-C-7K4M-Q9T6-H2VX-R8NP

Os 16 caracteres variáveis deverão ser gerados por fonte criptograficamente segura e utilizar alfabeto sem caracteres visualmente ambíguos, por exemplo: 23456789ABCDEFGHJKMNPQRSTUVWXYZ. O código não deverá conter CPF, iniciais do participante, data de nascimento, número de inscrição ou qualquer dado pessoal derivável.

• O prefixo PACAM27 identifica o evento e o ano.

• A letra C identifica a classe Certificate/Certificado e reserva espaço para futuras classes documentais.

• A parte aleatória deverá ser única no banco e protegida por restrição de unicidade.

• O código permanece associado à mesma credencial em caso de reemissão corretiva; a revisão do documento é controlada separadamente.

4.2 Identificador interno

O banco de dados deverá utilizar um identificador interno próprio, preferencialmente UUID, que não precisa ser exibido ao público. O ID interno não deve ser reutilizado como token de validação.

4.3 Token secreto de validação

Além do código público, cada certificado ativo deverá possuir um token aleatório de alta entropia, com no mínimo 128 bits, destinado exclusivamente à URL do QR Code. O token não deverá ser sequencial nem previsível.

Exemplo conceitual

https://cert.pacam2027.com/v/<TOKEN_ALEATORIO_128_BITS>

5. ESTRUTURA DO QR CODE

O QR Code impresso no certificado deverá conter somente uma URL HTTPS de validação. Não deverá conter JSON com dados pessoais, CPF, e-mail, telefone, data de nascimento ou dados de frequência detalhada.

Elemento	Especificação mínima
Conteúdo	URL HTTPS de validação com token aleatório.
Destino recomendado	https://cert.pacam2027.com/v/<token>
Tamanho mínimo no PDF	25 mm x 25 mm, preservando margem livre ao redor.
Zona de silêncio	mínimo de 4 módulos em todos os lados.
Correção de erro	nível M ou Q.
Contraste	fundo claro e módulos escuros, sem imagens sobrepostas que prejudiquem leitura.
Redirecionamento	permitido apenas dentro de domínio controlado pelo PACAM e com HTTPS.

Elemento	Especificação mínima
Rastreamento	o acesso pode gerar log técnico de validação, sem perfilamento desnecessário do consulente.

6. PÁGINA PÚBLICA DE VALIDAÇÃO

6.1 Acesso

A página deverá funcionar sem necessidade de login do consulente. A consulta poderá ocorrer diretamente pelo QR Code ou por formulário manual que exija o código do certificado e, se adotado, uma chave curta de verificação.

O portal não deverá oferecer busca aberta por nome, CPF, e-mail ou listagem de participantes. Páginas de validação devem ser configuradas para não serem indexadas por mecanismos de busca.

6.2 Campos públicos quando o certificado estiver ATIVO

Campo	Exibição pública
Status	ATIVO / ACTIVE
Nome do participante	nome completo exatamente como certificado.
Evento	Pan-American Congress of Aerospace Medicine - PACAM 2027.
Datas	23 a 25 de abril de 2027.
Local	Foz do Iguaçu, Paraná, Brasil.
Carga certificada	carga individual efetivamente certificada.
Frequência	percentual ou equivalente consolidado, quando previsto no certificado.
Código do certificado	identificador público completo.
Revisão	número da revisão vigente, por exemplo Rev. 01.
Data de emissão	data da primeira emissão.
Data de reemissão	quando houver revisão posterior.
Entidade emissora	PACAM PARAGUAY E.A.S. - RUC 80173825-3.

Campo	Exibição pública
Validação	mensagem explícita de autenticidade e integridade da versão vigente.

6.3 Dados que não devem ser exibidos publicamente

• CPF, cédula de identidade, passaporte ou outro documento pessoal.

• Endereço residencial, e-mail, telefone ou data de nascimento.

• Logs de presença por horário, dispositivo ou porta de acesso.

• Justificativas internas, documentos anexos e motivos detalhados de recurso.

• Usuário administrativo que realizou alterações, IPs, hashes internos ou dados de segurança.

7. ESTADOS DO CERTIFICADO

Status	Visibilidade	Significado
RASCUNHO / DRAFT	Interno	Dados preparados, ainda sem aprovação; não é validável publicamente.
PENDENTE / PENDING	Interno	Aguardando aprovação, assinatura, consolidação ou processamento.
ATIVO / ACTIVE	Público	Certificado válido e vigente; página pública confirma autenticidade.
SUBSTITUÍDO / SUPERSEDED	Público	Versão anterior substituída por reemissão. Deve indicar que existe uma revisão vigente, sem expor dados internos.
CANCELADO / CANCELLED	Público	Certificado sem validade. A página deve apresentar claramente que não deve ser aceito.
ERRO TÉCNICO / TECHNICAL ERROR	Interno	Estado transitório para falha de geração, armazenamento, assinatura ou publicação.

Regra de validade

Somente certificados com status ATIVO / ACTIVE poderão ser apresentados pelo sistema como válidos. Um arquivo PDF antigo não recupera validade se a página pública indicar SUBSTITUÍDO ou CANCELADO.

8. REGRAS DE EMISSÃO

1. Receber somente a base final de frequência com fechamento definitivo.

2. Validar nome do participante, identificador interno, carga individual, frequência e modalidade de certificado.

3. Aplicar os critérios de elegibilidade do Regulamento de Certificação.

4. Bloquear automaticamente emissão quando os requisitos mínimos não forem atendidos, salvo decisão formal autorizada e registrada.

5. Gerar código público e token de validação únicos.

6. Preencher os campos dinâmicos do Modelo Oficial de Certificado.

7. Gerar o documento final em PDF; o arquivo Word permanece como template e não deve ser distribuído como certificado oficial.

8. Calcular e armazenar hash SHA-256 do PDF final emitido.

9. Aplicar assinatura eletrônica ou mecanismo institucional definido para a versão final, quando disponível.

10. Registrar data, hora, usuário/aprovador, versão do template, revisão e status.

11. Publicar a página de validação e somente então disponibilizar o certificado ao participante.

9. CAMPOS DINÂMICOS DO TEMPLATE

Campo	Origem/uso
<<NOME_PARTICIPANTE>>	Nome completo validado.
<<HORAS_CERTIFICADAS>>	Carga em português, ex.: 16h40 ou 18h50.
<<CERTIFIED_HOURS>>	Carga na versão inglesa.
<<FREQUENCIA>>	Percentual/indicador de frequência consolidada.
<<ID_CERTIFICADO>>	Código público único.
<<URL_VALIDACAO>>	URL curta/canônica da página pública.
<<DATA_EMISSAO>>	Data da emissão inicial ou campo conforme layout.
<<REPRESENTANTE_LEGAL>>	Nome do representante autorizado conforme documentação vigente.
<<REVISAO>>	Revisão da credencial, ex.: 01, 02.

Campo	Origem/uso
<<QR_CODE>>	Imagem gerada a partir da URL de validação.

10. REEMISSÃO E CONTROLE DE REVISÕES

A reemissão não deve apagar o histórico. Toda nova versão deverá ser registrada como revisão da credencial ou, nos casos definidos abaixo, como nova credencial vinculada à anterior.

Situação	Tratamento
Erro de grafia no nome, comprovado	Manter código do certificado; gerar nova revisão; versão anterior passa a SUBSTITUÍDO.
Correção de carga horária após recurso deferido	Manter código; nova revisão; registrar decisão e novo cálculo; anterior SUBSTITUÍDO.
Atualização de assinatura ou elemento visual sem alteração acadêmica	Manter código; nova revisão quando o PDF for regenerado e publicado.
Arquivo corrompido ou falha de download sem alteração de conteúdo	Pode ser regenerado; registrar evento técnico e preservar conteúdo e código.
Certificado emitido para pessoa errada	CANCELAR o certificado incorreto e emitir novo código para o destinatário correto.
Fraude, falsificação de presença ou perda de elegibilidade confirmada	CANCELAR; não reemitir automaticamente; exigir decisão formal da instância competente.
Mudança substancial de evento, modalidade ou tipo de credencial	Emitir novo código e manter vínculo de auditoria com a credencial anterior.

A página pública de uma versão substituída deverá informar que aquele documento não é a versão vigente. Quando tecnicamente adequado, poderá oferecer link seguro para a validação da versão atual, sem permitir enumeração de outros certificados.

11. CANCELAMENTO

O cancelamento deverá exigir perfil autorizado, justificativa obrigatória e registro da autoridade que aprovou a medida. O arquivo não deverá ser apagado do repositório institucional; deverá permanecer preservado para auditoria, com acesso restrito.

- A página pública exibirá status CANCELADO / CANCELLED de forma destacada.

• O sistema não deverá exibir publicamente o motivo detalhado do cancelamento; poderá utilizar mensagem neutra: "Este certificado não possui validade vigente. Contate a Secretaria Acadêmica do PACAM para esclarecimentos."

• O QR Code do documento cancelado continuará resolvendo para a página de validação, que exibirá o status correto.

• O cancelamento deverá gerar evento de auditoria com data, hora, usuário, motivo interno, aprovador e referência documental quando aplicável.

• Caso o cancelamento tenha sido equivocado, a reativação somente poderá ocorrer por procedimento formal, com dupla autorização e registro integral da reversão.

12. PERFIS E CONTROLE DE ACESSO

Perfil	Escopo mínimo
Administrador do Sistema	configuração técnica, usuários e integrações; não deve alterar carga acadêmica sem autorização acadêmica.
Secretaria Acadêmica	consulta participantes, solicita emissão, corrige dados permitidos e acompanha reemissões.
Supervisor de Frequência	fornece/valida a base consolidada e consulta dados de frequência necessários.
Aprovador Acadêmico	aprova lotes, exceções e correções que afetem carga ou elegibilidade.
Representante Institucional/Signatário	aprova ou assina documentos quando aplicável, conforme poderes vigentes.
Auditor/Consulta	acesso somente leitura a relatórios e trilha de auditoria.
Participante	acesso apenas aos próprios documentos, se houver portal autenticado; a validação pública permanece separada.

Segregação de funções

Sempre que possível, a mesma pessoa não deve ser a única responsável por alterar carga horária, aprovar a exceção e publicar o certificado. Alterações acadêmicas relevantes devem exigir dupla validação.

13. SEGURANÇA DA INFORMAÇÃO

Controle	Requisito
Transporte	HTTPS obrigatório em todo o portal, APIs e páginas públicas.
Autenticação administrativa	credenciais individuais; MFA obrigatório para perfis privilegiados.
Senhas	armazenamento com algoritmo de hash de senha resistente e parâmetros atualizados; nunca em texto puro.
Autorização	controle por perfis e princípio do menor privilégio.
Banco de dados	criptografia em repouso quando suportada pela infraestrutura e backups protegidos.
Tokens de validação	geração criptograficamente segura; não sequenciais; não reutilizados.
Logs	imutabilidade lógica ou controles contra alteração; retenção conforme política institucional.
Backups	rotina automatizada, testes periódicos de restauração e cópia segregada.
Proteção contra abuso	rate limiting, bloqueio progressivo e mecanismos adicionais após tentativas anômalas.
Segredos	chaves, senhas, tokens de serviços e certificados digitais fora do código-fonte e com rotação controlada.
Ambientes	separação entre desenvolvimento/homologação e produção; dados reais não devem ser usados em testes sem necessidade e proteção adequada.
Monitoramento	alertas para falhas de emissão, mudanças massivas de status, tentativas de acesso privilegiado e padrões anormais de validação.

14. PROTEÇÃO DE DADOS E PRIVACIDADE

O sistema deverá adotar minimização de dados, controle de acesso e separação entre informações necessárias para emissão e informações efetivamente divulgadas na validação pública. A página pública deverá revelar somente os elementos necessários para verificar a credencial.

- Não incluir dados pessoais sensíveis ou documentos de identificação no QR Code.
- Não permitir consulta pública por CPF ou enumeração de participantes.

• Exibir aviso de privacidade apropriado no portal e identificar canal de contato institucional.

• Definir política de retenção para certificados, registros de emissão, logs e documentos de suporte, respeitando obrigações aplicáveis e necessidades de defesa/auditoria.

• Registrar acessos administrativos a dados pessoais e alterações de cadastro.

• Permitir correção de dados cadastrais mediante fluxo controlado e preservação do histórico.

15. INTEGRIDADE DO ARQUIVO E ASSINATURA

O certificado oficial entregue ao participante deverá ser um PDF gerado pelo sistema. O arquivo Word constitui apenas o modelo de origem. Para cada PDF publicado, o sistema deverá armazenar ao menos seu hash SHA-256 e a referência à versão do template usada na geração.

Caso seja adotada assinatura digital criptográfica, o sistema deverá manter os certificados/chaves sob controle institucional e registrar o momento e a identidade do processo de assinatura. A adoção de assinatura digital não elimina a necessidade da validação pública por QR Code e código único.

Resultado esperado

A autenticidade deve ser verificável por duas camadas complementares: (1) integridade do arquivo/assinatura quando disponível e (2) confirmação do status e dos dados essenciais no portal oficial do PACAM.

16. TRILHA DE AUDITORIA

Evento	Registro mínimo
Emissão	quem solicitou, quem aprovou, data/hora, lote, participante, versão do template, ID e hash.
Reemissão	revisão anterior/nova, motivo categorizado, solicitante, aprovadores e datas.
Cancelamento	certificado, motivo interno, aprovador, data/hora e referência documental.
Reativação	justificativa, dupla autorização e histórico completo.
Alteração cadastral	campo alterado, valor anterior/novo quando permitido, usuário e data/hora.
Importação de frequência	arquivo/lote, hash ou identificador da base, responsável e resultado das validações.

Evento	Registro mínimo
Acesso privilegiado	login, falhas relevantes, criação/desativação de usuários e mudança de permissões.
Validação pública	data/hora, certificado consultado e resultado; coletar somente dados técnicos necessários à segurança e estatística.

17. MODELO MÍNIMO DE DADOS

Campo lógico	Finalidade
certificate_id_internal	UUID/chave interna.
certificate_public_id	PACAM27-C-...
validation_token_hash	hash do token ou mecanismo equivalente; evitar armazenar segredo em claro quando arquitetura permitir.
participant_id	referência interna do participante.
participant_name	nome certificado.
event_code	PACAM2027.
certificate_type	participação, palestrante, moderador, instrutor, trabalho científico, comissão etc.
certified_minutes	carga certificada em minutos.
attendance_percent	percentual consolidado quando aplicável.
status	draft, pending, active, superseded, cancelled, technical_error.
revision	inteiro sequencial por credencial.
first_issued_at	data/hora da primeira emissão.
reissued_at	data/hora da revisão vigente, se houver.
pdf_storage_ref	referência segura ao arquivo oficial.
pdf_sha256	hash SHA-256 do PDF.

Campo lógico	Finalidade
template_version	versão do modelo utilizado.
issuer_entity	PACAM PARAGUAY E.A.S.
issuer_ruc	80173825-3.
approval_ref	referência ao lote/ato de aprovação.
created_by / approved_by	usuários responsáveis.
created_at / updated_at	timestamps de auditoria.

18. REQUISITOS FUNCIONAIS

ID	Requisito
RF-01	Importar base de participantes elegíveis com validação de esquema e inconsistências.
RF-02	Gerar certificados individualmente e em lote.
RF-03	Gerar código público e token únicos automaticamente.
RF-04	Gerar QR Code e inseri-lo no template.
RF-05	Gerar PDF bilíngue conforme modelo oficial.
RF-06	Publicar página pública de validação imediatamente após ativação.
RF-07	Permitir consulta por QR Code e por formulário manual.
RF-08	Permitir reemissão com controle de revisão e preservação do histórico.
RF-09	Permitir cancelamento com justificativa e autorização.
RF-10	Exibir claramente status ATIVO, SUBSTITUÍDO ou CANCELADO.
RF-11	Emitir relatórios de lotes, pendências, falhas, reemissões e cancelamentos.
RF-12	Exportar lista de certificados com ID, nome, tipo, carga, status e datas, respeitando permissões.
RF-13	Armazenar hash do PDF e versão do template.

ID	Requisito
RF-14	Registrar trilha de auditoria de ações administrativas.
RF-15	Permitir bloqueio de emissão quando frequência/carga não atenderem ao Regulamento.
RF-16	Suportar diferentes modalidades de certificado sem alterar a lógica de validação pública.

19. REQUISITOS NÃO FUNCIONAIS

ID	Requisito
RNF-01	Portal responsivo e utilizável em celular, pois o QR Code será a forma principal de consulta.
RNF-02	Tempo de resposta da validação pública compatível com consulta em ambiente acadêmico e institucional.
RNF-03	Disponibilidade e backups suficientes para manter a validação após o encerramento do congresso.
RNF-04	Arquitetura capaz de suportar emissão em lote sem duplicidade de IDs ou documentos.
RNF-05	Compatibilidade com caracteres acentuados e nomes internacionais em UTF-8.
RNF-06	Logs com horário padronizado e referência de fuso para auditoria.
RNF-07	Acessibilidade básica da página pública: contraste, navegação por teclado e texto alternativo quando pertinente.
RNF-08	Capacidade de manter versões futuras de templates e eventos sem sobrescrever o histórico do PACAM 2027.
RNF-09	Exportações administrativas devem respeitar o menor conjunto de dados necessário.
RNF-10	O sistema deve poder ser homologado em ambiente separado antes da entrada em produção.

20. API E INTEGRAÇÕES - DIRETRIZES

Caso o sistema utilize APIs, elas deverão ser autenticadas e versionadas. O portal público poderá consumir uma API de leitura restrita, mas nunca deverá expor endpoints que retornem listas de participantes ou dados administrativos.

Exemplo de rota	Finalidade
POST /admin/certificates/batch	criar lote a partir de base aprovada; restrito.
POST /admin/certificates/{id}/issue	emitir/ativar certificado; restrito.
POST /admin/certificates/{id}/reissue	criar nova revisão; restrito.
POST /admin/certificates/{id}/cancel	cancelar; restrito e auditado.
GET /public/v/{token}	retornar dados mínimos de validação da credencial.
POST /public/verify	validar código manual; aplicar proteção contra abuso.

As rotas acima são referenciais e podem ser adaptadas pelo fornecedor, desde que os controles de segurança, auditoria e minimização de dados sejam preservados.

21. MENSAGENS DA PÁGINA PÚBLICA

Status	Português	English
ATIVO	Certificado válido. Os dados abaixo correspondem ao registro oficial vigente do PACAM 2027.	Valid certificate. The information below matches the current official PACAM 2027 record.
SUBSTITUÍDO	Esta versão foi substituída e não é a versão vigente do certificado.	This version has been superseded and is not the current valid version of the certificate.
CANCELADO	Este certificado não possui validade vigente. Contate a Secretaria Acadêmica do PACAM para esclarecimentos.	This certificate is not currently valid. Contact the PACAM Academic Secretariat for further information.
NÃO ENCONTRADO	Não foi possível localizar um certificado com os dados	No certificate could be found with the information provided. Check the code and try again.

Status	Português	English
	informados. Verifique o código e tente novamente.	

22. HOMOLOGAÇÃO E TESTES DE ACEITE

Teste	Critério de aceite
TA-01	Emitir certificado de teste com 18h50 e confirmar todos os campos/QR.
TA-02	Emitir certificado com carga parcial e confirmar que o valor individual não é substituído pela carga máxima.
TA-03	Validar QR Code em Android e iOS e em ao menos dois navegadores.
TA-04	Tentar consultar por código inválido e confirmar que não há vazamento de dados.
TA-05	Reemitir por correção de nome e confirmar status SUBSTITUÍDO na versão anterior.
TA-06	Cancelar certificado e confirmar status CANCELADO imediatamente no portal.
TA-07	Testar concorrência de lote para confirmar ausência de IDs duplicados.
TA-08	Confirmar que CPF/e-mail/documento não aparecem no QR nem na página pública.
TA-09	Verificar hash do PDF armazenado e integridade do arquivo.
TA-10	Testar permissões: perfil sem autorização não pode cancelar, alterar carga ou emitir.
TA-11	Testar backup e restauração de amostra de certificados e metadados.
TA-12	Verificar trilha de auditoria para emissão, reemissão e cancelamento.
TA-13	Testar nomes com acentos, hífens, apóstrofos e caracteres internacionais.
TA-14	Confirmar que a página pública não está indexável por mecanismos de busca.
TA-15	Realizar teste final com o Modelo Oficial de Certificado antes da emissão em produção.

23. FLUXO OPERACIONAL DE PRODUÇÃO

Etapa	Ação
1	Encerrar período de contestação de frequência e consolidar base final.
2	Secretaria Acadêmica importa ou disponibiliza o lote aprovado.
3	Sistema executa validações de elegibilidade e consistência.
4	Pendências são resolvidas antes da emissão.
5	Aprovador Acadêmico autoriza o lote.
6	Sistema gera IDs, tokens, QR Codes, PDFs e hashes.
7	Assinatura/selagem institucional é aplicada, quando configurada.
8	Certificados passam a ATIVO e páginas públicas são publicadas.
9	Participantes recebem acesso/download do PDF oficial.
10	Relatório de emissão é arquivado no dossiê acadêmico.
11	Reemissões e cancelamentos posteriores seguem fluxo específico e auditado.

24. RESPONSABILIDADES DE GOVERNANÇA

Responsável	Atribuição
PACAM PARAGUAY E.A.S.	titular institucional do sistema e da política de emissão.
Comissão Acadêmica	aprovação de regras acadêmicas, exceções e critérios de elegibilidade.
Secretaria Acadêmica	qualidade cadastral, processamento operacional e atendimento de correções.
Equipe de Tecnologia / Fornecedor	segurança, disponibilidade, implementação, logs, backup e suporte técnico.
Responsável autorizado pela emissão	aprovação formal dos lotes e documentos, conforme governança definida.

Responsável	Atribuição
Auditoria institucional	verificação periódica de trilhas, amostras de certificados e controles de acesso.

25. CONTROLE DE MUDANÇAS

Qualquer alteração que modifique formato do código, dados públicos, critérios de status, regras de reemissão/cancelamento, campos do certificado ou arquitetura de segurança deverá gerar nova versão desta Especificação. Alterações meramente técnicas que não afetem requisitos poderão ser registradas em histórico de implementação.

Versão	Data	Alteração	Responsável
1.0	07/10/2026	Emissão inicial da especificação do sistema de emissão e validação.	PACAM PARAGUAY E.A.S.

26. APROVAÇÃO

A entrada do sistema em produção deverá ocorrer somente após homologação funcional, teste de segurança compatível com o risco, validação do Modelo Oficial de Certificado e aprovação institucional desta Especificação.

PACAM PARAGUAY E.A.S. Representante autorizado Nome: _____ Assinatura: _____ Data: ____/____/_____	Presidência da Comissão Acadêmica Prof. Dr. Guilherme Weiss Freccia CREF 010199-G/SC Assinatura: _____ Data: ____/____/_____
Secretaria Acadêmica Géssica Pereira Assinatura: _____ Data: ____/____/_____	Aprovação Técnica do Sistema Nome/Função: _____ Assinatura: _____ Data: ____/____/_____
Responsável Técnico Médico - Brasil Dr. Neidson Ricart Ribeiro CRM-RJ 714470 Assinatura: _____ Data: ____/____/_____	Responsável Técnico Médico - Paraguai Dr. Pablo H. Diniz Registro médico PY 42.970 Assinatura: _____ Data: ____/____/_____
Observações de homologação / versão de produção: _____ _____	

PACAM
1st Pan American Congress
Of Aerospace Medicine

ANEXO I - EXEMPLO DE REGISTRO PÚBLICO DE VALIDAÇÃO

Status	ATIVO / ACTIVE
Participante	NOME COMPLETO DO PARTICIPANTE
Evento	PACAM 2027 - Pan-American Congress of Aerospace Medicine
Datas	23-25/04/2027
Local	Foz do Iguaçu, Paraná, Brasil
Carga certificada	18h50
Frequência	100%
Código	PACAM27-C-7K4M-Q9T6-H2VX-R8NP
Revisão	01
Emitido em	30/04/2027
Emissor	PACAM PARAGUAY E.A.S. - RUC 80173825-3

CERTIFICADO VÁLIDO / VALID CERTIFICATE

A página deverá apresentar identidade visual institucional, mas sua função principal é fornecer uma resposta inequívoca sobre a validade atual do certificado e os dados essenciais da credencial.