PAN-AMERICAN CONGRESS OF AEROSPACE MEDICINE

Congreso Panamericano de Medicina Aeroespacial

ESPECIFICACIÓN TÉCNICA Y OPERATIVA N.º 001/2026

SISTEMA DE EMISIÓN Y VALIDACIÓN DE CERTIFICADOS

Documento de requisitos funcionales, seguridad, gobernanza y validación pública

Campo	Información
Entidad responsable	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	Proyecto Académico; Reglamento de Asistencia y Certificación; POP de Control de Asistencia; Modelo Oficial de Certificado
Carga científico-académica vigente	18 horas y 50 minutos
Asistencia mínima del certificado general	75 % — mínimo operativo de 14 h 10 min según la programación vigente
Versión	1.0
Emisión	7 de octubre de 2026

Documento de especificación para contratación, desarrollo, homologación y operación del sistema

www.pacam2027.com

1. FINALIDAD Y ALCANCE

La presente Especificación define los requisitos mínimos del sistema digital responsable de generar, registrar, poner a disposición, reemitir, cancelar y validar públicamente los certificados del PACAM 2027. El sistema deberá integrarse al proceso académico ya establecido y utilizar como fuente de verdad la base de asistencia consolidada y aprobada por la Secretaría Académica y la Comisión Académica.

El sistema deberá permitir tanto la emisión individual como por lotes, preservar la trazabilidad de cada acto, reducir el riesgo de fraude documental y ofrecer a universidades, empleadores, consejos profesionales y otras entidades receptoras un mecanismo sencillo de confirmación de autenticidad.

Principio central: el código QR y el código público de validación deberán permitir confirmar la autenticidad del certificado sin exponer CPF, documento de identidad, correo electrónico, teléfono, fecha de nacimiento u otros datos personales innecesarios.

2. DOCUMENTOS Y DATOS DE ORIGEN

- Proyecto Académico-Científico del PACAM 2027, que define el evento, la programación, la carga académica y los responsables.
- Resolución de Constitución y Designación de la Comisión Académica y de los Responsables Técnicos.
- Reglamento de Asistencia, Carga Horaria y Certificación, que establece los criterios de elegibilidad y emisión.
- POP de Control de Asistencia y Frecuencia, que define la captura, corrección, auditoría y cierre de los registros.
- Modelo Oficial de Certificado PACAM 2027, que contiene los campos dinámicos y la presentación institucional.
- Base final de participantes, con identificación, carga efectivamente certificada, asistencia, modalidad y estado de elegibilidad.

Ningún certificado deberá emitirse directamente a partir de datos preliminares de inscripción ni de registros de asistencia aún no consolidados.

3. VISIÓN GENERAL DE LA SOLUCIÓN

Componente	Función
Módulo de Administración	Gestiona registros, perfiles, parámetros, plantillas, lotes y permisos.
Módulo de Importación Académica	Recibe la base final de asistencia y ejecuta validaciones de consistencia.
Motor de Certificación	Calcula la elegibilidad, completa la plantilla, genera el PDF y registra versión y hash.
Repositorio de Certificados	Conserva el archivo oficial, metadatos, versiones y estado.
Portal Público de Validación	Permite consultas mediante QR o datos de validación, sin autenticar al consultante.
Módulo de Reemisión/Cancelación	Controla correcciones, sustituciones, cancelaciones y justificaciones.
Registro de Auditoría	Registra acciones administrativas, modificaciones, aprobaciones y eventos técnicos relevantes.
Servicios de Seguridad	Gestiona autenticación, autorización, MFA, copias de seguridad, cifrado, monitoreo y protección contra abusos.

Flujo lógico: base de asistencia cerrada → validación de elegibilidad → aprobación del lote → generación del certificado → firma/sellado → publicación de la validación → entrega al participante → auditoría y eventual reemisión/cancelación.

4. ESTÁNDAR DEL CÓDIGO ÚNICO DEL CERTIFICADO

4.1. Código público visible

Cada certificado deberá recibir un identificador público aleatorio y permanente, independiente del número de inscripción del participante y de la clave interna de la base de datos.

Formato recomendado: PACAM27-C-XXXX-XXXX-XXXX-XXXX. Ejemplo: PACAM27-C-7K4M-Q9T6-H2VX-R8NP.

Los 16 caracteres variables deberán generarse mediante una fuente criptográficamente segura y utilizar un alfabeto sin caracteres visualmente ambiguos, por ejemplo: 23456789ABCDEFGHJKMNPQRSTUVWXYZ. El código no deberá contener CPF, iniciales del participante, fecha de nacimiento, número de inscripción ni ningún dato personal derivable.

- El prefijo PACAM27 identifica el evento y el año.
- La letra C identifica la clase Certificate/Certificado y reserva espacio para futuras clases documentales.
- La parte aleatoria deberá ser única en la base de datos y estar protegida por una restricción de unicidad.
- El código seguirá asociado a la misma credencial en una reemisión correctiva; la revisión del documento se controlará por separado.

4.2. Identificador interno

La base de datos deberá utilizar un identificador interno propio, preferentemente UUID, que no necesita mostrarse al público. El ID interno no deberá reutilizarse como token de validación.

4.3. Token secreto de validación

Además del código público, cada certificado activo deberá tener un token aleatorio de alta entropía, de al menos 128 bits, destinado exclusivamente a la URL del código QR. El token no deberá ser secuencial ni predecible.

Ejemplo conceptual: https://cert.pacam2027.com/v/

5. ESTRUCTURA DEL CÓDIGO QR

El código QR impreso en el certificado deberá contener únicamente una URL HTTPS de validación. No deberá contener JSON con datos personales, CPF, correo electrónico, teléfono, fecha de nacimiento ni datos detallados de asistencia.

Elemento	Especificación mínima
Contenido	URL HTTPS de validación con token aleatorio.
Destino recomendado	https://cert.pacam2027.com/v/
Tamaño mínimo en PDF	25 mm × 25 mm, conservando margen libre alrededor.
Zona de silencio	Mínimo de 4 módulos en todos los lados.
Corrección de errores	Nivel M o Q.
Contraste	Fondo claro y módulos oscuros, sin imágenes superpuestas que dificulten la lectura.
Redireccionamiento	Permitido únicamente dentro de un dominio controlado por PACAM y mediante HTTPS.
Seguimiento	El acceso podrá generar un registro técnico de validación, sin elaboración innecesaria de perfiles del consultante.

6. PÁGINA PÚBLICA DE VALIDACIÓN

6.1. Acceso

La página deberá funcionar sin necesidad de inicio de sesión del consultante. La consulta podrá realizarse directamente mediante el QR o mediante un formulario manual que solicite el código del certificado y, si se adopta, una clave corta de verificación.

El portal no deberá permitir búsquedas abiertas por nombre, CPF, correo electrónico ni listados de participantes. Las páginas de validación deberán configurarse para no ser indexadas por motores de búsqueda.

6.2. Campos públicos cuando el certificado esté ACTIVO

Campo	Visualización pública
Estado	ACTIVO / ACTIVE
Nombre del participante	Nombre completo exactamente como aparece en el certificado.
Evento	Pan-American Congress of Aerospace Medicine — PACAM 2027.
Fechas	23 al 25 de abril de 2027.
Lugar	Foz do Iguaçu, Paraná, Brasil.
Carga certificada	Carga individual efectivamente certificada.
Asistencia	Porcentaje o equivalente consolidado, cuando esté previsto en el certificado.
Código del certificado	Identificador público completo.
Revisión	Número de la revisión vigente, por ejemplo Rev. 01.
Fecha de emisión	Fecha de la primera emisión.
Fecha de reemisión	Cuando exista una revisión posterior.
Entidad emisora	PACAM PARAGUAY E.A.S. — RUC 80173825-3.
Validación	Mensaje explícito de autenticidad e integridad de la versión vigente.

6.3. Datos que no deben mostrarse públicamente

- CPF, cédula de identidad, pasaporte u otro documento personal.
- Domicilio, correo electrónico, teléfono o fecha de nacimiento.
- Registros de asistencia por horario, dispositivo o puerta de acceso.
- Justificaciones internas, documentos adjuntos y motivos detallados de recursos.
- Usuario administrativo que realizó cambios, direcciones IP, hashes internos u otros datos de seguridad.

7. ESTADOS DEL CERTIFICADO

Estado	Visibilidad	Significado
BORRADOR / DRAFT	Interna	Datos preparados, aún sin aprobación; no validable públicamente.
PENDIENTE / PENDING	Interna	A la espera de aprobación, firma, consolidación o procesamiento.
ACTIVO / ACTIVE	Pública	Certificado válido y vigente; la página pública confirma su autenticidad.
SUSTITUIDO / SUPERSEDED	Pública	Versión anterior sustituida por reemisión; debe indicar que existe una revisión vigente, sin exponer datos internos.
CANCELADO / CANCELLED	Pública	Certificado sin validez; la página debe indicar claramente que no debe aceptarse.
ERROR TÉCNICO / TECHNICAL ERROR	Interna	Estado transitorio por fallo de generación, almacenamiento, firma o publicación.

Regla de validez: solamente los certificados con estado ACTIVO / ACTIVE podrán presentarse como válidos. Un PDF antiguo no recupera validez si la página pública indica SUSTITUIDO o CANCELADO.

8. REGLAS DE EMISIÓN

- Recibir únicamente la base final de asistencia con cierre definitivo.
- Validar nombre del participante, identificador interno, carga individual, asistencia y modalidad del certificado.
- Aplicar los criterios de elegibilidad del Reglamento de Certificación.
- Bloquear automáticamente la emisión cuando no se cumplan los requisitos mínimos, salvo decisión formal autorizada y registrada.
- Generar código público y token de validación únicos.
- Completar los campos dinámicos del Modelo Oficial de Certificado.
- Generar el documento final en PDF; el archivo Word permanece como plantilla y no debe distribuirse como certificado oficial.
- Calcular y almacenar el hash SHA-256 del PDF final emitido.
- Aplicar firma electrónica o el mecanismo institucional definido para la versión final, cuando esté disponible.
- Registrar fecha, hora, usuario/aprobador, versión de la plantilla, revisión y estado.
- Publicar la página de validación y solo entonces poner el certificado a disposición del participante.

9. CAMPOS DINÁMICOS DE LA PLANTILLA

Campo	Origen/uso
<>	Nombre completo validado.
<>	Carga en portugués, por ejemplo 16h40 o 18h50.
<>	Carga en la versión inglesa.
<>	Porcentaje/indicador de asistencia consolidada.
<>	Código público único.
<>	URL corta/canónica de la página pública.
<>	Fecha de emisión inicial o campo conforme al diseño.
<>	Nombre del representante autorizado conforme a la documentación vigente.
<>	Revisión de la credencial, por ejemplo 01, 02.
<>	Imagen generada a partir de la URL de validación.

10. REEMISIÓN Y CONTROL DE REVISIONES

La reemisión no debe borrar el historial. Cada nueva versión se registrará como revisión de la credencial o, en los casos indicados, como una nueva credencial vinculada a la anterior.

Situación	Tratamiento
Error ortográfico en el nombre, comprobado	Mantener el código; generar una nueva revisión; la versión anterior pasa a SUSTITUIDO.
Corrección de carga horaria tras recurso aceptado	Mantener el código; nueva revisión; registrar decisión y nuevo cálculo; versión anterior SUSTITUIDO.
Actualización de firma o elemento visual sin cambio académico	Mantener el código; nueva revisión si se regenera y publica el PDF.
Archivo dañado o fallo de descarga sin cambio de contenido	Puede regenerarse; registrar evento técnico y conservar contenido y código.
Certificado emitido a la persona equivocada	CANCELAR el certificado incorrecto y emitir un nuevo código para el destinatario correcto.
Fraude, falsificación de asistencia o pérdida de elegibilidad confirmada	CANCELAR; no reemitir automáticamente; exigir decisión formal de la instancia competente.
Cambio sustancial de evento, modalidad o tipo de credencial	Emitir nuevo código y mantener vínculo de auditoría con la credencial anterior.

La página pública de una versión sustituida deberá informar que ese documento no es la versión vigente. Cuando sea técnicamente adecuado, podrá ofrecer un enlace seguro para validar la versión actual, sin permitir enumerar otros certificados.

11. CANCELACIÓN

La cancelación exigirá un perfil autorizado, justificación obligatoria y registro de la autoridad que aprobó la medida. El archivo no deberá eliminarse del repositorio institucional; deberá conservarse para auditoría, con acceso restringido.

- La página pública mostrará claramente el estado CANCELADO / CANCELLED.
- El sistema no mostrará públicamente el motivo detallado de la cancelación; podrá utilizar el mensaje neutro: «Este certificado no tiene validez vigente. Contacte con la Secretaría Académica del PACAM para aclaraciones».
- El QR del documento cancelado seguirá dirigiendo a la página de validación, que mostrará el estado correcto.
- La cancelación generará un evento de auditoría con fecha, hora, usuario, motivo interno, aprobador y referencia documental cuando corresponda.
- Si la cancelación fue errónea, la reactivación solo podrá realizarse mediante procedimiento formal, doble autorización y registro íntegro de la reversión.

12. PERFILES Y CONTROL DE ACCESO

Perfil	Alcance mínimo
Administrador del Sistema	Configuración técnica, usuarios e integraciones; no debe modificar la carga académica sin autorización académica.
Secretaría Académica	Consulta participantes, solicita emisión, corrige datos permitidos y supervisa reemisiones.
Supervisor de Asistencia	Proporciona/valida la base consolidada y consulta los datos de asistencia necesarios.
Aprobador Académico	Aprueba lotes, excepciones y correcciones que afecten la carga o la elegibilidad.
Representante Institucional/Firmante	Aprueba o firma documentos cuando corresponda, conforme a las facultades vigentes.
Auditor/Consulta	Acceso de solo lectura a informes y registro de auditoría.
Participante	Acceso únicamente a sus propios documentos, si existe un portal autenticado; la validación pública permanece separada.

Separación de funciones: siempre que sea posible, una misma persona no deberá ser la única responsable de modificar la carga horaria, aprobar la excepción y publicar el certificado. Las modificaciones académicas relevantes exigirán doble validación.

13. SEGURIDAD DE LA INFORMACIÓN

Control	Requisito
Transporte	HTTPS obligatorio en todo el portal, las API y las páginas públicas.
Autenticación administrativa	Credenciales individuales; MFA obligatorio para perfiles privilegiados.
Contraseñas	Almacenamiento con algoritmo de hash resistente y parámetros actualizados; nunca en texto plano.
Autorización	Control por perfiles y principio de mínimo privilegio.
Base de datos	Cifrado en reposo cuando la infraestructura lo permita y copias de seguridad protegidas.
Tokens de validación	Generación criptográficamente segura; no secuenciales ni reutilizados.
Registros (logs)	Inmutabilidad lógica o controles contra modificaciones; conservación según política institucional.
Copias de seguridad	Rutina automatizada, pruebas periódicas de restauración y copia segregada.
Protección contra abuso	Limitación de solicitudes, bloqueo progresivo y medidas adicionales tras intentos anómalos.
Secretos	Claves, contraseñas, tokens de servicio y certificados digitales fuera del código fuente, con rotación controlada.
Entornos	Separación entre desarrollo/homologación y producción; no usar datos reales en pruebas sin necesidad y protección adecuadas.
Monitoreo	Alertas por fallos de emisión, cambios masivos de estado, accesos privilegiados y patrones anómalos de validación.

14. PROTECCIÓN DE DATOS Y PRIVACIDAD

El sistema deberá aplicar minimización de datos, control de acceso y separación entre la información necesaria para emitir y la que se divulga en la validación pública. La página pública revelará únicamente los elementos necesarios para verificar la credencial.

- No incluir datos personales sensibles ni documentos de identidad en el código QR.
- No permitir consultas públicas por CPF ni enumeración de participantes.
- Mostrar un aviso de privacidad apropiado en el portal e identificar un canal de contacto institucional.
- Definir una política de conservación de certificados, registros de emisión, logs y documentos de soporte, respetando las obligaciones aplicables y las necesidades de defensa/auditoría.
- Registrar los accesos administrativos a datos personales y las modificaciones de registros.
- Permitir la corrección de datos registrales mediante un flujo controlado que preserve el historial.

15. INTEGRIDAD DEL ARCHIVO Y FIRMA

El certificado oficial entregado al participante deberá ser un PDF generado por el sistema. El archivo Word constituye únicamente la plantilla de origen. Para cada PDF publicado, el sistema almacenará al menos su hash SHA-256 y la referencia a la versión de la plantilla utilizada.

Si se adopta una firma digital criptográfica, el sistema mantendrá los certificados y claves bajo control institucional y registrará el momento y la identidad del proceso de firma. La firma digital no elimina la necesidad de validación pública mediante QR y código único.

Resultado esperado: la autenticidad se verificará mediante dos capas complementarias: (1) integridad del archivo/firma, cuando esté disponible, y (2) confirmación del estado y de los datos esenciales en el portal oficial del PACAM.

16. REGISTRO DE AUDITORÍA

Evento	Registro mínimo
Emisión	Quién solicitó, quién aprobó, fecha/hora, lote, participante, versión de plantilla, ID y hash.
Reemisión	Revisión anterior/nueva, motivo categorizado, solicitante, aprobadores y fechas.
Cancelación	Certificado, motivo interno, aprobador, fecha/hora y referencia documental.
Reactivación	Justificación, doble autorización e historial completo.
Cambio registral	Campo modificado, valor anterior/nuevo cuando esté permitido, usuario y fecha/hora.
Importación de asistencia	Archivo/lote, hash o identificador de la base, responsable y resultado de las validaciones.
Acceso privilegiado	Inicio de sesión, fallos relevantes, creación/desactivación de usuarios y cambios de permisos.
Validación pública	Fecha/hora, certificado consultado y resultado; recopilar solo los datos técnicos necesarios para seguridad y estadísticas.

17. MODELO MÍNIMO DE DATOS

Campo lógico	Finalidad
certificate_id_internal	UUID/clave interna.
certificate_public_id	PACAM27-C-...
validation_token_hash	Hash del token o mecanismo equivalente; evitar almacenar el secreto en claro cuando la arquitectura lo permita.
participant_id	Referencia interna del participante.
participant_name	Nombre certificado.
event_code	PACAM2027.
certificate_type	Participación, ponente, moderador, instructor, trabajo científico, comisión, etc.
certified_minutes	Carga certificada en minutos.
attendance_percent	Porcentaje consolidado cuando corresponda.
status	draft, pending, active, superseded, cancelled, technical_error.
revision	Entero secuencial por credencial.
first_issued_at	Fecha/hora de la primera emisión.
reissued_at	Fecha/hora de la revisión vigente, si existe.
pdf_storage_ref	Referencia segura al archivo oficial.
pdf_sha256	Hash SHA-256 del PDF.
template_version	Versión de la plantilla utilizada.
issuer_entity	PACAM PARAGUAY E.A.S.
issuer_ruc	80173825-3.
approval_ref	Referencia al lote/acto de aprobación.
created_by / approved_by	Usuarios responsables.
created_at / updated_at	Marcas de tiempo de auditoría.

18. REQUISITOS FUNCIONALES

ID	Requisito
RF-01	Importar la base de participantes elegibles con validación de esquema e inconsistencias.
RF-02	Generar certificados individualmente y por lotes.
RF-03	Generar automáticamente códigos públicos y tokens únicos.
RF-04	Generar el código QR e insertarlo en la plantilla.
RF-05	Generar PDF bilingüe conforme al modelo oficial.
RF-06	Publicar la página pública de validación inmediatamente después de la activación.
RF-07	Permitir consultas por QR y mediante formulario manual.
RF-08	Permitir reemisión con control de revisiones y conservación del historial.
RF-09	Permitir cancelación con justificación y autorización.
RF-10	Mostrar claramente los estados ACTIVO, SUSTITUIDO o CANCELADO.
RF-11	Emitir informes de lotes, pendientes, fallos, reemisiones y cancelaciones.
RF-12	Exportar lista de certificados con ID, nombre, tipo, carga, estado y fechas, respetando permisos.
RF-13	Almacenar el hash del PDF y la versión de la plantilla.
RF-14	Registrar el historial de auditoría de acciones administrativas.
RF-15	Permitir bloquear la emisión cuando asistencia/carga no cumpla el Reglamento.
RF-16	Admitir diferentes modalidades de certificado sin alterar la lógica de validación pública.

19. REQUISITOS NO FUNCIONALES

ID	Requisito
RNF-01	Portal adaptable y utilizable en teléfonos móviles, ya que el QR será la forma principal de consulta.
RNF-02	Tiempo de respuesta de la validación pública adecuado para consultas en entornos académicos e institucionales.
RNF-03	Disponibilidad y copias de seguridad suficientes para mantener la validación tras finalizar el congreso.
RNF-04	Arquitectura capaz de admitir emisión por lotes sin duplicación de ID ni documentos.
RNF-05	Compatibilidad con acentos y nombres internacionales mediante UTF-8.
RNF-06	Registros con horario normalizado y referencia de zona horaria para auditoría.
RNF-07	Accesibilidad básica de la página pública: contraste, navegación por teclado y texto alternativo cuando corresponda.
RNF-08	Capacidad para mantener futuras versiones de plantillas y eventos sin sobrescribir el historial del PACAM 2027.
RNF-09	Las exportaciones administrativas deberán respetar el conjunto mínimo de datos necesario.
RNF-10	El sistema deberá poder homologarse en un entorno separado antes de entrar en producción.

20. API E INTEGRACIONES — DIRECTRICES

Si el sistema utiliza API, estas deberán estar autenticadas y versionadas. El portal público podrá consumir una API de lectura restringida, pero nunca deberá exponer endpoints que devuelvan listas de participantes o datos administrativos.

Ruta de ejemplo	Finalidad
POST /admin/certificates/batch	Crear un lote a partir de una base aprobada; acceso restringido.
POST /admin/certificates/{id}/issue	Emitir/activar certificado; acceso restringido.
POST /admin/certificates/{id}/reissue	Crear una nueva revisión; acceso restringido.
POST /admin/certificates/{id}/cancel	Cancelar; restringido y auditado.
GET /public/v/{token}	Devolver los datos mínimos de validación de la credencial.
POST /public/verify	Validar código manual; aplicar protección contra abuso.

Las rutas anteriores son referenciales y podrán adaptarse por el proveedor, siempre que se preserven los controles de seguridad, auditoría y minimización de datos.

21. MENSAJES DE LA PÁGINA PÚBLICA

Estado	Portugués (original)	English (original)
ACTIVO	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.
SUSTITUIDO	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.
NO ENCONTRADO	Não foi possível localizar um certificado com os dados informados. Verifique o código e tente novamente.	No certificate could be found with the information provided. Check the code and try again.

22. HOMOLOGACIÓN Y PRUEBAS DE ACEPTACIÓN

Prueba	Criterio de aceptación
TA-01	Emitir certificado de prueba con 18h50 y confirmar todos los campos/QR.
TA-02	Emitir certificado con carga parcial y confirmar que el valor individual no se sustituya por la carga máxima.
TA-03	Validar el QR en Android e iOS y en al menos dos navegadores.
TA-04	Intentar consultar con código inválido y confirmar que no haya filtración de datos.
TA-05	Reemitir por corrección de nombre y confirmar estado SUSTITUIDO en la versión anterior.
TA-06	Cancelar certificado y confirmar estado CANCELADO inmediatamente en el portal.
TA-07	Probar concurrencia de lotes para confirmar ausencia de ID duplicados.
TA-08	Confirmar que CPF/correo/documento no aparezcan en el QR ni en la página pública.
TA-09	Verificar el hash del PDF almacenado y la integridad del archivo.
TA-10	Probar permisos: un perfil no autorizado no puede cancelar, cambiar la carga ni emitir.
TA-11	Probar copia de seguridad y restauración de una muestra de certificados y metadatos.
TA-12	Verificar el registro de auditoría para emisión, reemisión y cancelación.
TA-13	Probar nombres con acentos, guiones, apóstrofos y caracteres internacionales.
TA-14	Confirmar que la página pública no esté indexada por motores de búsqueda.
TA-15	Realizar una prueba final con el Modelo Oficial de Certificado antes de la emisión en producción.

23. FLUJO OPERATIVO DE PRODUCCIÓN

Etapa	Acción
1	Cerrar el período de impugnación de asistencia y consolidar la base final.
2	La Secretaría Académica importa o pone a disposición el lote aprobado.
3	El sistema ejecuta validaciones de elegibilidad y consistencia.
4	Resolver las incidencias pendientes antes de la emisión.
5	El Aprobador Académico autoriza el lote.
6	El sistema genera IDs, tokens, códigos QR, PDF y hashes.
7	Aplicar firma/sellado institucional, cuando esté configurado.
8	Los certificados pasan a ACTIVO y se publican las páginas públicas.
9	Los participantes reciben acceso/descarga del PDF oficial.
10	Archivar el informe de emisión en el expediente académico.
11	Las reemisiones y cancelaciones posteriores siguen un flujo específico y auditado.

24. RESPONSABILIDADES DE GOBERNANZA

Responsable	Atribución
PACAM PARAGUAY E.A.S.	Titular institucional del sistema y de la política de emisión.
Comisión Académica	Aprobación de reglas académicas, excepciones y criterios de elegibilidad.
Secretaría Académica	Calidad de los datos registrales, procesamiento operativo y atención de correcciones.
Equipo de Tecnología / Proveedor	Seguridad, disponibilidad, implementación, registros, copias de seguridad y soporte técnico.
Responsable autorizado de emisión	Aprobación formal de lotes y documentos, conforme a la gobernanza definida.
Auditoría institucional	Verificación periódica de registros, muestras de certificados y controles de acceso.

25. CONTROL DE CAMBIOS

Toda modificación que cambie el formato del código, los datos públicos, los criterios de estado, las reglas de reemisión/cancelación, los campos del certificado o la arquitectura de seguridad deberá generar una nueva versión de esta Especificación. Los cambios meramente técnicos que no afecten los requisitos podrán registrarse en el historial de implementación.

Versión	Fecha	Cambio	Responsable
1.0	07/10/2026	Emisión inicial de la especificación del sistema de emisión y validación.	PACAM PARAGUAY E.A.S.

26. APROBACIÓN

La entrada del sistema en producción deberá ocurrir únicamente después de la homologación funcional, de una prueba de seguridad acorde con el riesgo, de la validación del Modelo Oficial de Certificado y de la aprobación institucional de esta Especificación.

Responsable / función	Nombre y firma
PACAM PARAGUAY E.A.S. — Representante autorizado	Nombre: _____\nFirma: _____\nFecha: ____/____/_____
Presidencia de la Comisión Académica	Prof. Dr. Guilherme Weiss Freccia\nCREF 010199-G/SC\nFirma: _____\nFecha: ____/____/_____
Secretaría Académica	Géssica Pereira\nFirma: _____\nFecha: ____/____/_____
Aprobación Técnica del Sistema	Nombre/función: _____\nFirma: _____\nFecha: ____/____/_____
Responsable Técnico Médico — Brasil	Dr. Neidson Ricart Ribeiro\nCRM-RJ 714470\nFirma: _____\nFecha: ____/____/_____
Responsable Técnico Médico — Paraguay	Dr. Pablo H. Diniz\nRegistro médico PY 42.970\nFirma: _____\nFecha: ____/____/_____

Observaciones de homologación / versión de producción: _____

ANEXO I — EJEMPLO DE REGISTRO PÚBLICO DE VALIDACIÓN

Campo	Ejemplo
Estado	ACTIVO / ACTIVE
Participante	NOMBRE COMPLETO DEL PARTICIPANTE
Evento	PACAM 2027 — Pan-American Congress of Aerospace Medicine
Fechas	23–25/04/2027
Lugar	Foz do Iguaçu, Paraná, Brasil
Carga certificada	18h50
Asistencia	100 %
Código	PACAM27-C-7K4M-Q9T6-H2VX-R8NP
Revisión	01
Emitido el	30/04/2027
Emisor	PACAM PARAGUAY E.A.S. — RUC 80173825-3

«CERTIFICADO VÁLIDO / VALID CERTIFICATE». La página deberá presentar la identidad visual institucional, pero su función principal será ofrecer una respuesta inequívoca sobre la validez actual del certificado y los datos esenciales de la credencial.