Manual de Procedimientos de Certificación

Jacobs Comercial S.R.L. (Egregor Labs) — Versión 1.1 — Fecha: [●] — Clase: Público (con Anexo reservado)

Versiones y modificaciones de este documento

Versión	Fecha	Elaborado por	Revisado por	Descripción
1.0	[●]	Responsable de la AC	Gerencia	Versión inicial para el licenciamiento
1.1	7/11/2026	Responsable de la AC	Gerencia	Razón social Jacobs Comercial S.R.L., nombre de fantasía Egregor Labs, aplicación Advanced Electronic Signature (AdES), domicilio y CUIT

Cómo leer este Manual

Este Manual describe las prácticas con las que Jacobs Comercial S.R.L., que gira bajo el nombre de fantasía “Egregor Labs” (en adelante, indistintamente, “Jacobs Comercial S.R.L.” o “Egregor Labs”), aplica su Política Única de Certificación (“la Política”). Sigue la misma estructura de nueve secciones. Cuando un punto no agrega nada a lo que dispone la Política, remite a ella; cuando la Política fija una obligación, este Manual describe el procedimiento con el que se cumple.

Cada procedimiento se describe con el mismo esquema: frecuencia, oportunidad y urgencia; roles que participan; acción que lo pone en marcha; tareas de cada rol; y resultado.

Este Manual no contiene cláusulas contradictorias ni incompatibles con la Política (Anexo II, Sección 2.II, de la Resolución SICYT N° 11/2025). Las secciones 1 a 9 son públicas. El Anexo A es reservado y solo se entrega al Ente Licenciante y a los auditores.

1. Introducción

1.1. Descripción general

Jacobs Comercial S.R.L. (Egregor Labs) emite certificados de firma digital para personas humanas y jurídicas, cuyos pares de claves se generan en el módulo criptográfico del teléfono del suscriptor mediante la aplicación habilitada “Advanced Electronic Signature” (“AdES”), desarrollada por la propia Jacobs Comercial S.R.L., y valida la identidad de los solicitantes con el RENAPER. El marco normativo es el indicado en el punto 1.1 de la Política.

La operación se distribuye en tres componentes, todos en la República Argentina y afectados exclusivamente a la certificación:

Componente	Función
Autoridad Certificante (AC EGREGOR)	Firma certificados, CRL y el certificado del respondedor OCSP con la clave de la AC alojada en un HSM. No es accesible desde Internet.
Autoridad de Registro Central (AR CENTRAL)	Recibe las solicitudes desde la aplicación AdES, consulta al RENAPER, verifica la CSR y la atestación de la aplicación, gestiona los legajos y las revocaciones, y opera la aplicación de la AR que usan los Oficiales de Registro.
Repositorio y servicios de estado	Publican documentos, certificados y CRL, y responden consultas OCSP.

La aplicación AdES se ejecuta en el dispositivo del suscriptor y se comunica solo con la AR CENTRAL para todo lo relativo a la certificación. La aplicación no usa otros servidores propios: la cuenta del usuario, el plan contratado y la gestión de los certificados se administran en la AR CENTRAL. Los únicos servicios de terceros que intervienen son el inicio de sesión con Apple, Google o Microsoft, cuando el usuario lo elige; la App Store, para el pago de los planes; y el servicio de atestación de Apple. Ninguno de ellos recibe datos de identidad ni documentación de los solicitantes.

1.2. Nombre e identificación del documento

Nombre	Manual de Procedimientos de Certificación de Jacobs Comercial S.R.L. (Egregor Labs)
Versión	1.1
Fecha	[●]
Política asociada	Política Única de Certificación de Jacobs Comercial S.R.L., OID [●]
URL (parte pública)	https://advancedelectronicsignature.com/politicas/manual.pdf

1.3. Participantes

1.3.1. Certificador

Según el punto 1.3.1 de la Política: Jacobs Comercial S.R.L., nombre de fantasía Egregor Labs.

1.3.2. Autoridad de Registro

Egregor Labs opera la AR CENTRAL, en las modalidades remota y presencial descriptas en el punto 1.3.2 de la Política. No habilita Autoridades de Registro delegadas. Si en el futuro lo hiciera, presentará previamente al Ente Licenciante la modificación de la Política y de este Manual.

La AR CENTRAL está integrada por el Responsable de la AR, los Oficiales de Registro y el Responsable de Soporte Técnico, conforme al artículo 29 del Anexo al Decreto N° 182/2019. Funciona en Cabello 3352, piso 3 (C1425), Ciudad Autónoma de Buenos Aires, de lunes a viernes de [●] a [●] horas para la atención presencial, y en forma permanente para la recepción de solicitudes remotas y de revocaciones.

1.3.3. Suscriptores de certificados

Según el punto 1.3.3 de la Política.

1.3.4. Terceros usuarios

Según el punto 1.3.4 de la Política.

1.4. Uso de los certificados

Según el punto 1.4 de la Política.

1.5. Administración del Manual de Procedimientos

1.5.1. Responsable del documento

El Responsable de la Autoridad Certificante es responsable de la redacción, el mantenimiento y la interpretación de este Manual. Contacto: según el punto 1.5.2 de la Política.

1.5.2. Contacto

Según el punto 1.5.2 de la Política.

1.5.3. Procedimiento de aprobación

Este Manual se presenta al Ente Licenciante junto con la Política y se aplica una vez aprobado. Sus modificaciones siguen el procedimiento del punto 9.12 de este Manual.

1.6. Definiciones y acrónimos

1.6.1. Definiciones

Rigen las definiciones del punto 1.6.1 de la Política. Además, en este Manual:

- **Aplicación de la AR:** sistema de la AR CENTRAL en el que se reciben y procesan las solicitudes, se consultan los resultados del RENAPER, se gestionan los legajos y se tramitan las revocaciones. Los Oficiales de Registro acceden a él con su certificado de firma digital.
- **Legajo del suscriptor:** conjunto de registros electrónicos que respaldan la emisión de un certificado, conforme al punto 4.2 de la Política.
- **Desafío:** valor aleatorio de un solo uso que la AR entrega a la aplicación AdES para cada solicitud, y que la atestación de la aplicación debe incluir.
- **Listado de dispositivos admitidos:** listado de modelos de iPhone y versiones de iOS cuyo módulo criptográfico cumple el punto 6.2.11 de la Política.

- **Rol de confianza:** cada uno de los roles del punto 5.2 de este Manual.

1.6.2. Acrónimos

Rigen los acrónimos del punto 1.6.2 de la Política.

2. Responsabilidades vinculadas a la publicación y a los repositorios

2.1. Repositorios

Según el punto 2.1 de la Política. El repositorio se compone de un servidor web en la zona de servicios públicos del sitio principal, con réplica en el sitio de contingencia. La CRL se copia además a una red de distribución de contenidos.

2.2. Publicación de información del Certificador

Según el punto 2.2 de la Política.

Procedimiento de publicación de documentos

- **Frecuencia, oportunidad y urgencia:** ante cada nueva versión aprobada de un documento. Planificado. Urgencia media.
- **Roles:** Responsable de la AC; Administrador de sistemas; Responsable de Seguridad.
- **Acción que lo pone en marcha:** notificación del acto aprobatorio del Ente Licenciante o cambio en el listado de dispositivos admitidos.
- **Tareas:**
    1. El Responsable de la AC entrega al Administrador de sistemas el documento aprobado en PDF firmado digitalmente.
    2. El Administrador de sistemas lo publica en la URL correspondiente, conserva la versión anterior en la sección de versiones anteriores y registra la publicación.
    3. El Responsable de Seguridad verifica que el documento publicado coincida con el aprobado, comparando su resumen criptográfico.
    4. Si la modificación es sustancial, el Responsable de la AC ordena la notificación a los suscriptores según el punto 9.12.2 de la Política.
- **Resultado:** documento vigente publicado; versión anterior disponible; registro de la publicación.

2.3. Frecuencia de publicación

Según el punto 2.3 de la Política. La CRL se publica según el punto 4.9.7 de la Política; el listado de dispositivos admitidos, según el procedimiento del punto 6.2.11 de este Manual.

2.4. Controles de acceso a la información

Según el punto 2.4 de la Política. La información publicada es de solo lectura para el público. Solo el Administrador de sistemas puede modificarla, desde una estación de administración, con autenticación de doble factor y registro de cada cambio. Un control automático compara

cada hora los archivos publicados con sus resúmenes de referencia y alerta ante cualquier diferencia.

Las solicitudes de acceso a la propia información (artículo 21, inciso h) de la Ley N° 25.506) se reciben en privacidad@advancedelectronicsignature.com o desde la aplicación AdES y se responden dentro de los diez (10) días corridos, previa verificación de la identidad del solicitante.

3. Identificación y autenticación

3.1. Asignación de nombres de suscriptores

Según el punto 3.1 de la Política. Los datos de nombre y CUIL o CUIT que integran el certificado de una persona humana no son tipeados por el solicitante ni por el Oficial de Registro: la aplicación de la AR los toma de la respuesta del RENAPER. En los certificados de personas jurídicas, el Oficial de Registro carga la denominación y el CUIT tal como figuran en la documentación verificada, y la aplicación de la AR los compara con la constancia de CUIT.

3.2. Registro inicial

3.2.1. Métodos para comprobar la titularidad del par de claves

Según el punto 3.2.1 de la Política.

Procedimiento de verificación de la CSR y de la atestación de la aplicación

- **Frecuencia, oportunidad y urgencia:** en cada solicitud de emisión o renovación. Automático. Numerosas veces por día.
- **Roles:** aplicación AdES; sistema de la AR CENTRAL; Oficial de Registro (solo ante observaciones).
- **Acción que lo pone en marcha:** el solicitante confirma, en la aplicación AdES, los datos que contendrá el certificado.
- **Tareas:**
    1. La aplicación AdES genera el par de claves en el módulo criptográfico del dispositivo con los atributos del punto 6.1.1 de la Política.
    2. La aplicación arma la CSR (PKCS#10) con la clave pública y los datos confirmados, y la firma con la clave nueva; el sistema operativo solicita la autenticación biométrica del solicitante y su contraseña de firma.
    3. La aplicación solicita a la AR un desafío, que la AR genera con un generador de números aleatorios criptográficamente seguro, asocia a la solicitud y marca como válido por cinco (5) minutos y para un solo uso.
    4. La aplicación calcula el resumen SHA-256 de la concatenación del desafío, la clave pública y la CSR, y solicita al servicio App Attest del sistema operativo una aserción sobre ese resumen con la clave de atestación de esa instalación. Si la instalación aún no tiene clave de atestación, la genera y obtiene previamente su atestación de Apple.

5. La aplicación envía a la AR la CSR, la aserción y, en su caso, el objeto de atestación.
6. El sistema de la AR verifica, en este orden: (a) que el desafío exista, no esté vencido ni usado; (b) la cadena de certificados de la atestación hasta la raíz de App Attest de Apple; (c) que el identificador de aplicación atestado corresponda al de la aplicación AdES (equipo de desarrollo de Jacobs Comercial S.R.L. y paquete registrados) y al ambiente de producción; (d) la firma de la aserción y el resumen del paso 4; (e) que el contador de la aserción sea mayor que el último registrado para esa clave de atestación; (f) la firma de la CSR con su propia clave pública; (g) que la clave pública sea un punto válido de la curva P-256 y no se haya usado en ningún certificado anterior; y (h) que el modelo y la versión de iOS informados figuren en el listado de dispositivos admitidos.
7. Si todas las verificaciones son positivas, la solicitud continúa. Si falla (a), (b), (c), (d), (e), (f) o (g), la solicitud se rechaza y se registra el motivo. Si solo falla (h), la solicitud se rechaza y la aplicación informa al solicitante que su dispositivo o versión no está admitido.
8. El sistema de la AR guarda en el legajo la CSR, la atestación, la aserción, el desafío y el resultado de cada verificación.

- **Resultado:** solicitud con titularidad del par de claves comprobada y vinculada a la aplicación AdES, o solicitud rechazada con motivo registrado.

3.2.2. Autenticación de la identidad de personas jurídicas públicas o privadas

Según el punto 3.2.2 de la Política.

Procedimiento de verificación de la documentación de personas jurídicas

- **Frecuencia, oportunidad y urgencia:** en cada solicitud de certificado de persona jurídica y en cada renovación. Planificado. Urgencia media.
- **Roles:** representante legal o apoderado; Oficial de Registro; Responsable de la AR (ante dudas).
- **Acción que lo pone en marcha:** el solicitante completa los datos de la persona jurídica en la aplicación AdES y adjunta la documentación o solicita turno presencial.
- **Tareas:**
  1. El Oficial de Registro recibe la solicitud en la aplicación de la AR, con la documentación adjunta. Si la documentación es electrónica, verifica las firmas digitales; si es copia certificada presentada en forma presencial, la digitaliza y la firma digitalmente como copia fiel.
  2. Verifica que estén todos los documentos del punto 3.2.2 de la Política y que estén vigentes.
  3. Verifica en la constancia de CUIT y, cuando sea posible, en el registro público correspondiente, la denominación, el CUIT y la vigencia de la persona jurídica.
  4. Verifica que el solicitante sea el representante legal según la última designación de autoridades, o que el poder sea suficiente para solicitar certificados de firma digital y esté vigente.

5. Verifica que la identidad del solicitante, validada con el RENAPER según el punto 3.2.3 de la Política, coincida con la del representante o apoderado de la documentación.
6. Carga, en su caso, la unidad operativa y el cargo o función del responsable que integrarán el certificado.
7. Si la documentación es insuficiente, solicita al solicitante, desde la aplicación de la AR, la documentación faltante. Si no la recibe dentro de los treinta (30) días corridos, da de baja la solicitud.
8. Si la documentación es suficiente, aprueba esta etapa firmando digitalmente su verificación en la aplicación de la AR. El solicitante recibe el aviso para continuar con la generación de claves.
9. Ante dudas sobre la representación, consulta al Responsable de la AR antes de aprobar.

- **Resultado:** documentación verificada y firmada por el Oficial de Registro e incorporada al legajo, o solicitud observada o rechazada.

3.2.3. Autenticación de la identidad de personas humanas

Según el punto 3.2.3 de la Política.

Procedimiento de validación remota de identidad (presencia telemática)

- **Frecuencia, oportunidad y urgencia:** en cada emisión y renovación, y en las revocaciones del punto 3.4.c) de la Política. Disponibilidad permanente. Numerosas veces por día.
- **Roles:** solicitante; aplicación AdES; sistema de la AR CENTRAL; RENAPER.
- **Acción que lo pone en marcha:** el solicitante elige validar su identidad en la aplicación AdES.
- **Tareas:**
  1. La aplicación solicita el CUIL o CUIT y el sexo según el DNI, y el consentimiento expreso para el cotejo con el RENAPER.
  2. La aplicación activa la cámara frontal, guía al solicitante para cumplir las recomendaciones de captura del punto 3.2.3 de la Política y ejecuta una prueba de vida. No permite cargar imágenes guardadas.
  3. La aplicación cifra la captura para la AR y la envía junto con los datos ingresados. La captura no se guarda en el dispositivo.
  4. El sistema de la AR remite la consulta al servicio de validación de identidad del RENAPER, en los términos del convenio de confronte de datos celebrado por Jacobs Comercial S.R.L.
  5. Si el resultado es negativo, la aplicación informa al solicitante y permite reintentar. Después del segundo reintento negativo, la aplicación ofrece el turno presencial. Si la falla se debe al servicio del RENAPER, se aplica el punto 3.2.4.
  6. Si el resultado es positivo, el sistema de la AR registra los datos de identificación devueltos por el RENAPER y los usa para armar los datos del certificado, que la aplicación muestra al solicitante para su conformidad.

7. El sistema de la AR guarda en el legajo la captura, el resultado de cada intento, el identificador de la transacción del RENAPER, la fecha y hora y el dispositivo desde el que se realizó.

- **Resultado:** identidad validada y datos de identificación registrados, o derivación a la modalidad presencial.

Procedimiento de validación presencial de identidad

- **Frecuencia, oportunidad y urgencia:** a pedido del solicitante, por derivación de la modalidad remota o por contingencia. Con turno. Urgencia media.
- **Roles:** solicitante; Oficial de Registro.
- **Acción que lo pone en marcha:** el solicitante concurre a la AR CENTRAL con su DNI y su dispositivo, con turno solicitado desde la aplicación AdES.
- **Tareas:**
  1. El Oficial de Registro conecta su token y se autentica con su certificado en la aplicación de la AR y en el sistema del RENAPER.
  2. Controla el DNI y su correspondencia con el solicitante.
  3. Ejecuta las capturas de rostro y huellas y su cotejo según el punto 3.2.3.b) de la Política, con los reintentos y las condiciones de procedencia allí establecidos.
  4. Atiende las excepciones de captura del punto 3.2.3 de la Política a pedido del solicitante.
  5. Si alguna condición de procedencia se cumple, registra el resultado y habilita en la aplicación de la AR la continuación del trámite en el dispositivo del solicitante; en caso contrario, se abstiene de continuar y registra el motivo.
  6. El solicitante completa en su dispositivo la generación de claves, la CSR y la aceptación del Acuerdo con Suscriptores. El Oficial de Registro no manipula el dispositivo del solicitante.
  7. El Oficial de Registro aprueba la solicitud firmándola con su certificado en la aplicación de la AR.
- **Resultado:** identidad validada en forma presencial y solicitud aprobada por el Oficial de Registro, o trámite interrumpido con motivo registrado.

3.2.4. Protocolo de contingencia ante fallos en el sistema de biometría

Según el punto 3.2.4 de la Política.

Procedimiento

- **Frecuencia, oportunidad y urgencia:** ante dos reintentos fallidos atribuibles al sistema de biometría del RENAPER. Poco frecuente. Urgencia media.
- **Roles:** solicitante; Oficial de Registro; Responsable de la AR.
- **Acción que lo pone en marcha:** el sistema de la AR registra que los dos reintentos fallaron por error del servicio biométrico del RENAPER (y no por resultado negativo del cotejo) y ofrece al solicitante un turno presencial de contingencia.
- **Tareas:**
  1. El solicitante concurre a la AR CENTRAL con su DNI y su dispositivo.

2. El Oficial de Registro realiza la toma de datos biométricos y documenta en la aplicación de la AR la falla del sistema de biometría.
3. Valida la identidad con el número de trámite (ID) del DNI mediante el Sistema de Identidad Digital (SID) del RENAPER.
4. Si la validación es positiva, continúa según los pasos 6 y 7 del procedimiento de validación presencial.
5. Incorpora al legajo la documentación presentada y los antecedentes de los reintentos fallidos.
6. El Responsable de la AR revisa semanalmente los trámites resueltos por contingencia.

- **Resultado:** identidad validada por contingencia, con constancia de la falla.

3.2.5. Información no verificada del suscriptor

Según el punto 3.2.5 de la Política. La información no verificada (por ejemplo, el nombre que el solicitante elige para su dispositivo) se conserva en el legajo identificada como tal y nunca se transfiere a la CSR.

3.2.6. Validación de autoridad

Según el punto 3.2.6 de la Política y el procedimiento del punto 3.2.2 de este Manual.

3.2.7. Criterios para la interoperabilidad

Según el punto 3.2.7 de la Política.

3.3. Identificación y autenticación para la generación de nuevo par de claves

3.3.1. Renovación con generación de nuevo par de claves

Según el punto 3.3.1 de la Política. El procedimiento se describe en el punto 4.7 de este Manual.

3.3.2. Generación de un certificado con el mismo par de claves

No se admite (punto 3.3.2 de la Política). La aplicación de la AR rechaza toda CSR cuya clave pública ya figure en un certificado emitido.

3.4. Requerimiento de revocación

Según el punto 3.4 de la Política. Los procedimientos se describen en el punto 4.9.3 de este Manual.

4. Ciclo del certificado: requerimientos operativos

4.1. Solicitud de certificado

4.1.1. Solicitantes de certificados

Según el punto 4.1.1 de la Política.

4.1.2. Solicitud de certificado

Según el punto 4.1.2 de la Política.

Procedimiento de solicitud de certificado de persona humana

- **Frecuencia, oportunidad y urgencia:** disponibilidad permanente. Numerosas veces por día. Urgencia baja.
- **Roles:** solicitante; aplicación AdES; sistema de la AR CENTRAL.
- **Acción que lo pone en marcha:** el solicitante elige “Solicitar certificado de firma digital” en la aplicación AdES.
- **Tareas:**
    1. La aplicación verifica que el dispositivo tenga código de desbloqueo y biometría configurados, que no presente indicios de modificación de sus controles de seguridad, que el modelo y la versión de iOS figuren en el listado de dispositivos admitidos y que la versión de la aplicación sea igual o posterior a la mínima vigente. Si algo no se cumple, informa qué falta y detiene el trámite.
    2. Si el solicitante no tiene cuenta, la crea con email y contraseña, o con su cuenta de Apple, Google o Microsoft, e indica el correo electrónico que figurará en el certificado, que se verifica con un código de un solo uso cuando el proveedor no lo haya verificado o sea una dirección de reenvío. La cuenta no acredita la identidad: el paso 4 es obligatorio en todos los casos.
    3. La aplicación presenta la Política, el Acuerdo con Suscriptores, los Términos y Condiciones con Terceros Usuarios y la Política de Privacidad, con enlace a su texto completo, informa que el prestador es Jacobs Comercial S.R.L. (Egregor Labs) y registra la toma de conocimiento.
    4. El solicitante valida su identidad según el procedimiento remoto del punto 3.2.3 de este Manual, o solicita turno para la modalidad presencial.
    5. La aplicación muestra los datos que contendrá el certificado (nombre, CUIL o CUIT, país, correo electrónico) y el solicitante presta su conformidad respecto de su veracidad (artículo 16 del Anexo I de la Resolución SICYT N° 11/2025).
    6. El solicitante define su contraseña de firma (punto 6.4.1 de la Política) y se ejecuta el procedimiento de verificación de la CSR y de la atestación del punto 3.2.1 de este Manual.
    7. La aplicación presenta el Acuerdo con Suscriptores; el solicitante declara haberlo leído y lo acepta. La AR registra la aceptación (versión, huella del texto, fecha, hora y dispositivo) en el legajo. El solicitante firma digitalmente el Acuerdo con su certificado al recibirlo, según el procedimiento de aceptación del punto 4.4.

8. La aplicación presenta los planes del punto 9.1 de la Política. El solicitante elige la prueba gratuita o un plan pago, salvo que ya tenga un plan asignado. Asignado el plan, la solicitud pasa al procesamiento del punto 4.2.

- **Resultado:** solicitud completa en la aplicación de la AR, con identidad validada, CSR y atestación verificadas, Acuerdo aceptado y plan asignado.

Procedimiento de solicitud de certificado de persona jurídica

- **Frecuencia, oportunidad y urgencia:** disponibilidad permanente. Varias veces por día. Urgencia baja.
- **Roles:** representante legal o apoderado; aplicación AdES; Oficial de Registro.
- **Acción que lo pone en marcha:** el solicitante elige "Solicitar certificado para una persona jurídica".
- **Tareas:**
  1. Se cumplen los pasos 1 a 3 del procedimiento anterior.
  2. El solicitante ingresa la denominación y el CUIT de la persona jurídica, la unidad operativa (si corresponde) y su cargo o función, y adjunta la documentación del punto 3.2.2 de la Política o solicita turno para presentarla.
  3. El solicitante valida su identidad según el punto 3.2.3 de este Manual.
  4. El Oficial de Registro ejecuta el procedimiento de verificación de la documentación del punto 3.2.2 de este Manual.
  5. Aprobada la documentación, la aplicación muestra los datos que contendrá el certificado, incluidos los datos del responsable de la custodia de la clave, y el solicitante presta su conformidad.
  6. Se cumplen los pasos 6 a 8 del procedimiento anterior.
- **Resultado:** solicitud completa, con documentación aprobada por un Oficial de Registro.

Certificados en más de un dispositivo. Cada solicitud genera claves en un solo dispositivo. Si el suscriptor quiere firmar desde otro dispositivo, repite el procedimiento en ese dispositivo. La aplicación de la AR vincula los certificados del mismo suscriptor por su CUIL o CUIT y permite al suscriptor ver y revocar cualquiera de ellos desde cualquiera de sus dispositivos con certificado vigente.

4.2. Procesamiento de la solicitud del certificado

Según el punto 4.2 de la Política.

Procedimiento

- **Frecuencia, oportunidad y urgencia:** en cada solicitud completa. Numerosas veces por día. Urgencia media.
- **Roles:** sistema de la AR CENTRAL; Oficial de Registro; Responsable de la AR.
- **Acción que lo pone en marcha:** la solicitud queda completa según el punto 4.1.2.
- **Tareas:**
  1. El sistema de la AR verifica las condiciones a) a g) del punto 4.2 de la Política y que los datos de la CSR coincidan exactamente con los validados.

2. **Aprobación automática.** En solicitudes de personas humanas en modalidad remota sin observaciones, el sistema de la AR aprueba la solicitud y la firma digitalmente con la clave de servicio de la AR, alojada en el HSM, y la remite a la AC.
3. **Aprobación por un Oficial de Registro.** En solicitudes presenciales, de personas jurídicas o con observaciones, el Oficial de Registro revisa el legajo en la aplicación de la AR y aprueba la solicitud firmándola con su certificado, o la rechaza indicando el motivo. Las observaciones se resuelven dentro de los dos (2) días hábiles.
4. Si la solicitud se rechaza, la aplicación AdES y el correo electrónico informan el motivo al solicitante, salvo que hacerlo comprometa la seguridad. El plan pago queda asignado a la persona y se aplica al certificado que obtenga después. Si no desea continuar, el reintegro de un plan comprado en la App Store se gestiona ante Apple, y el de un plan facturado directamente, ante Jacobs Comercial S.R.L.
5. El Responsable de la AR revisa semanalmente una muestra de las aprobaciones automáticas y todas las solicitudes rechazadas por fallas de la atestación de la aplicación.

- **Resultado:** solicitud aprobada y firmada por la AR, o rechazada con motivo registrado y comunicado.

4.3. Emisión del certificado

4.3.1. Proceso de emisión del certificado

Según el punto 4.3.1 de la Política.

Procedimiento

- **Frecuencia, oportunidad y urgencia:** en cada solicitud aprobada. Automático. Numerosas veces por día.
- **Roles:** sistema de la AR CENTRAL; AC.
- **Acción que lo pone en marcha:** la AR remite a la AC una solicitud aprobada y firmada.
- **Tareas:**
  1. La AC verifica la firma de la AR sobre la solicitud aprobada y que su certificado esté vigente.
  2. La AC verifica la congruencia entre la solicitud y el perfil del punto 7.1 de la Política, y que el período de validez no exceda el de su propio certificado.
  3. La AC firma el certificado con su clave en el HSM, lo registra en su base de datos y lo devuelve a la AR.
  4. La AR verifica el certificado devuelto (clave pública igual a la de la CSR, sujeto, correo electrónico y cadena) y lo entrega a la aplicación AdES con la cadena de certificación.
  5. La aplicación AdES verifica que la clave pública del certificado corresponda a la clave privada del módulo, instala el certificado y le muestra al suscriptor sus datos para que lo acepte o lo rechace.
  6. El certificado se publica en el servicio de consulta del punto 4.9.11 de la Política.

- **Resultado:** certificado emitido, instalado en el dispositivo y registrado.

4.3.2. Notificación de emisión

Según el punto 4.3.2 de la Política. El correo electrónico de notificación, enviado en nombre de Jacobs Comercial S.R.L. (Egregor Labs), indica el número de serie, el período de validez, cómo consultar el estado y cómo revocar el certificado.

4.4. Aceptación del certificado

Según el punto 4.4 de la Política.

Procedimiento

- **Frecuencia, oportunidad y urgencia:** en cada emisión. Numerosas veces por día. Urgencia baja.
- **Roles:** suscriptor; aplicación AdES; sistema de la AR CENTRAL.
- **Acción que lo pone en marcha:** instalación del certificado en la aplicación AdES.
- **Tareas:**
    1. La aplicación muestra el contenido del certificado.
    2. Si es correcto, el suscriptor firma digitalmente el Acuerdo con Suscriptores en PDF (PAdES) con el certificado nuevo, con su biometría y su contraseña de firma. La AR verifica la firma, guarda el Acuerdo firmado en el legajo y registra la aceptación expresa del certificado.
    3. Si es incorrecto, el suscriptor elige “Rechazar”; la aplicación envía la solicitud de revocación firmada y la AR revoca el certificado de inmediato.
    4. Si el suscriptor no firma ni rechaza, el certificado se considera aceptado a las cuarenta y ocho (48) horas de la notificación; la aplicación no permite firmar otros documentos hasta que el Acuerdo esté firmado.
- **Resultado:** certificado aceptado y en condiciones de ser usado, o revocado si los datos eran incorrectos.

4.5. Uso del par de claves y del certificado

4.5.1. Uso de la clave privada y del certificado por parte del suscriptor

Según el punto 4.5.1 de la Política. La aplicación AdES muestra, antes de cada firma, el nombre del documento y el certificado que se usará, verifica que haya firmas de prueba disponibles o un plan vigente, y solicita la autenticación biométrica y la contraseña de firma para cada operación. Las firmas se producen en formato PAdES (documentos PDF) o CAdES (cualquier otro archivo) e incluyen el certificado del firmante y la cadena de certificación.

4.5.2. Uso de la clave pública y del certificado por parte de terceros usuarios

Según el punto 4.5.2 de la Política.

4.6. Renovación del certificado sin generación de un nuevo par de claves

No se admite (punto 4.6 de la Política).

4.7. Renovación del certificado con generación de un nuevo par de claves

Según el punto 4.7 de la Política.

Procedimiento

- **Frecuencia, oportunidad y urgencia:** a pedido del suscriptor, desde treinta (30) días antes del vencimiento, o en cualquier momento después de la revocación o expiración. Urgencia baja.
- **Roles:** suscriptor; aplicación AdES; sistema de la AR CENTRAL; Oficial de Registro (personas jurídicas).
- **Acción que lo pone en marcha:** aviso de vencimiento de la aplicación AdES, o pedido del suscriptor.
- **Tareas:**
    1. Si el certificado anterior está vigente, la aplicación firma con su clave la constancia de inicio del trámite de renovación, que la AR verifica y registra.
    2. El suscriptor valida su identidad con el RENAPER según el punto 3.2.3 de este Manual.
    3. En certificados de personas jurídicas, el Oficial de Registro verifica nuevamente la documentación según el punto 3.2.2 de este Manual.
    4. Se ejecutan los pasos 5 a 8 del procedimiento de solicitud del punto 4.1.2 de este Manual, con generación de un nuevo par de claves.
    5. Emitido y aceptado el nuevo certificado, si el anterior estaba asociado al mismo dispositivo, la AR lo revoca con el motivo “superseded” y la aplicación elimina su clave privada.
- **Resultado:** nuevo certificado con nuevo par de claves; certificado anterior revocado o vencido.

4.8. Modificación del certificado

Según el punto 4.8 de la Política. El suscriptor informa el cambio desde la aplicación AdES, que inicia la revocación del certificado y ofrece una nueva solicitud.

4.9. Suspensión y revocación de certificados

Según el punto 4.9 de la Política.

4.9.1. Causas de revocación

Según el punto 4.9.1 de la Política. Las causas se registran con el código de motivo (reasonCode) de la CRL y del servicio OCSP que corresponda: keyCompromise (j, incluidos la pérdida o el robo del dispositivo y el cambio de los datos biométricos registrados en él), affiliationChanged (b e i, incluido el cese de la representación en personas jurídicas), superseded (renovación) y cessationOfOperation (n, y el rechazo del certificado por el suscriptor). En los demás casos, incluida la revocación a pedido del suscriptor sin otra causa, la entrada no lleva código de motivo, como recomienda el RFC 5280 en lugar de “unspecified”. El estado “certificateHold” no se usa.

4.9.2. Autorizados a solicitar la revocación

Según el punto 4.9.2 de la Política.

4.9.3. Procedimientos para la solicitud de revocación

Procedimiento de revocación desde la cuenta

- **Frecuencia, oportunidad y urgencia:** disponibilidad permanente. Poco frecuente. No planificado. Urgencia muy alta.
- **Roles:** suscriptor; aplicación AdES o portal web; sistema de la AR CENTRAL; AC.
- **Acción que lo pone en marcha:** el suscriptor elige "Revocar" en la aplicación AdES (en el dispositivo del certificado o en otro) o en el portal web; perdió o le robaron su dispositivo; olvidó su contraseña de firma; informa un cambio de datos o de los datos biométricos del dispositivo; o elimina su cuenta.
- **Tareas:**
    1. El suscriptor inicia sesión en la aplicación AdES, en cualquier dispositivo, con su email y contraseña o con su cuenta de Apple, Google o Microsoft, o en el portal web https://advancedelectronicsignature.com/cuenta, desde cualquier navegador, con un código de un solo uso que recibe en el correo electrónico de su cuenta.
    2. Elige el certificado en la lista de sus dispositivos, la opción de revocarlo y, en forma optativa, el motivo.
    3. Escribe la frase "revocar mi certificado" en la ventana de confirmación (no se distinguen mayúsculas, tildes ni espacios de más). Si no coincide, la revocación no se ejecuta. No se piden autenticación biométrica, contraseña de firma ni códigos.
    4. La AR registra el pedido con la cuenta, el método de inicio de sesión, la dirección IP, la fecha y la hora, y ordena la revocación a la AC.
    5. La AC marca el certificado como revocado, actualiza el servicio OCSP y emite una nueva CRL dentro de la hora.
    6. Si el pedido se hizo desde el dispositivo del certificado, la aplicación elimina la clave privada y el certificado revocado. En los demás dispositivos, la aplicación lo hace la próxima vez que se abre. El dispositivo sigue habilitado para pedir un certificado nuevo desde Perfil.
    7. La AR notifica la revocación por correo electrónico y en la aplicación, con la fecha, la hora y el origen del pedido.
- **Resultado:** certificado revocado en forma inmediata y registrado.

Procedimiento de baja de la cuenta

- **Frecuencia, oportunidad y urgencia:** disponibilidad permanente. Poco frecuente. No planificado.
- **Roles:** usuario; aplicación AdES o portal web; sistema de la AR CENTRAL; AC.
- **Acción que lo pone en marcha:** el usuario elige "Eliminar mi cuenta" en Perfil o en el portal web.
- **Tareas:**

1. El usuario, con la sesión iniciada, escribe la frase “eliminar mi cuenta”.
2. La AR revoca todos los certificados vigentes de la cuenta según el procedimiento de revocación desde la cuenta y cancela los trámites en curso.
3. La AR borra los datos de acceso (correo electrónico, resumen de la contraseña, vínculos con Apple, Google o Microsoft, sesiones y códigos), revoca la autorización otorgada a Apple y marca la cuenta como eliminada.
4. Conserva las solicitudes, los certificados, los legajos y el registro de eventos por diez (10) años (artículo 21, inciso i) de la Ley N° 25.506).
5. La aplicación elimina del dispositivo las claves y los certificados. La AR confirma la baja por correo electrónico.

- **Resultado:** cuenta eliminada y certificados revocados, con registro. El mismo correo electrónico puede usarse para una cuenta nueva.

Procedimiento de revocación por la Mesa de Ayuda con validación de identidad

- **Frecuencia, oportunidad y urgencia:** disponibilidad permanente en la modalidad remota; con turno en la presencial. Poco frecuente. Urgencia alta.
- **Roles:** suscriptor; Mesa de Ayuda u Oficial de Registro; sistema de la AR CENTRAL; AC.
- **Acción que lo pone en marcha:** el suscriptor no puede acceder a su dispositivo ni a su cuenta.
- **Tareas:**
  1. El suscriptor se comunica con la Mesa de Ayuda o concurre a la AR CENTRAL. El Oficial de Registro, con su passkey en el panel interno, busca el certificado por CUIL, CUIT o número de serie.
  2. En la modalidad remota, el Oficial realiza una videollamada en vivo, que no se graba. La persona muestra su DNI físico a cámara, de frente y de dorso. El Oficial compara el rostro con la foto del DNI y con la foto validada con el RENAPER que figura en el legajo, y carga el número de DNI leído, que el sistema compara con el validado. En la modalidad presencial, se valida la identidad según el punto 3.2.3 de este Manual.
  3. La persona confirma de viva voz con la frase “revocar mi certificado”. El Oficial marca en el panel cada control realizado y el motivo. Si el DNI no coincide o falta algún control, el sistema no permite la revocación y registra el intento.
  4. Validada la identidad, la AR revoca el certificado indicado y registra el Oficial, los controles y la fecha y hora. Cada consulta de la foto del legajo queda registrada.
  5. Se ejecutan los pasos 5 a 7 del procedimiento de revocación desde la cuenta.
- **Resultado:** certificado revocado dentro de las veinticuatro (24) horas; con la videollamada, en forma inmediata.

Procedimiento de revocación a pedido de terceros autorizados o de oficio

- **Frecuencia, oportunidad y urgencia:** no planificado. Poco frecuente. Urgencia alta.
- **Roles:** persona jurídica titular, Ente Licenciante, autoridad judicial o Autoridad de Aplicación; Responsable de la AR; Oficial de Registro; Responsable de la AC.

- **Acción que lo pone en marcha:** recepción de una nota firmada digitalmente u ológrafa con firma certificada, de un oficio judicial o de un acto administrativo; o detección por Egregor Labs de alguna causa del punto 4.9.1 de la Política.
- **Tareas:**
    1. El Oficial de Registro verifica la identidad y la legitimación del solicitante (firma digital, certificación de firma, oficio o acto administrativo) y la causa invocada, y digitaliza la documentación.
    2. En los casos de fallecimiento, ausencia o incapacidad, verifica la partida o la resolución judicial presentada por los herederos o la autoridad judicial.
    3. Si la causa es de oficio, el Responsable de la AC documenta la causa y autoriza la revocación.
    4. El Oficial de Registro selecciona el certificado en la aplicación de la AR y firma la revocación con su certificado.
    5. Se ejecutan los pasos 5 y 7 del procedimiento de revocación desde la cuenta. Si el suscriptor no fue quien la solicitó, la notificación indica la causa.
    6. Si no pueden verificarse las condiciones de la revocación, el Oficial de Registro la rechaza y comunica el motivo al solicitante.
- **Resultado:** certificado revocado dentro de las veinticuatro (24) horas, con la documentación respaldatoria en el legajo.

En todos los casos, la AR CENTRAL conserva la solicitud de revocación y su respaldo, y el certificado revocado se incluye en la CRL según el punto 4.9.7.

4.9.4. Plazo para la solicitud de revocación

Según el punto 4.9.4 de la Política. Los canales de la cuenta (aplicación AdES y portal web) y de la Mesa de Ayuda telefónica funcionan siete (7) días por veinticuatro (24) horas, los trescientos sesenta y cinco (365) días del año, sin intervención de la AR.

4.9.5. Plazo para el procesamiento de la solicitud de revocación

Según el punto 4.9.5 de la Política. La aplicación de la AR alerta al Responsable de la AR cuando una solicitud de revocación que requiere intervención humana lleva doce (12) horas sin procesar.

4.9.6. Requisitos para la verificación de la lista de certificados revocados

Según el punto 4.9.6 de la Política.

4.9.7. Frecuencia de emisión de listas de certificados revocados

Según el punto 4.9.7 de la Política.

Procedimiento de emisión de la CRL

- **Frecuencia, oportunidad y urgencia:** automático, dentro de la hora de cada revocación y cada doce (12) horas. Urgencia muy alta.
- **Roles:** AC; Administrador de sistemas; Responsable de Seguridad.

- **Acción que lo pone en marcha:** una revocación procesada o el vencimiento del intervalo de doce (12) horas.
- **Tareas:**
    1. La AC genera la CRL con todos los certificados revocados, la firma en el HSM e incrementa el número de CRL.
    2. El sistema verifica la firma de la nueva CRL, la compara con la anterior (todas las entradas anteriores deben seguir presentes) y la publica en el repositorio, en el sitio de contingencia y en la red de distribución.
    3. El monitoreo verifica que la CRL publicada sea la nueva y que su campo "nextUpdate" sea posterior al momento actual en más de doce (12) horas.
    4. Si la emisión o la publicación fallan, el monitoreo alerta al Administrador de sistemas y al Responsable de Seguridad, que resuelven el problema o activan el Plan de Contingencia antes del vencimiento de la CRL vigente.
    5. Semanalmente, el Responsable de Seguridad verifica que todos los certificados revocados figuren en la CRL.
- **Resultado:** CRL vigente, firmada y publicada.

4.9.8. Vigencia de la lista de certificados revocados

Según el punto 4.9.8 de la Política.

4.9.9. Disponibilidad del servicio de consulta sobre revocación y de estado del certificado

Según el punto 4.9.9 de la Política. En el repositorio se publica la última CRL emitida; las anteriores se conservan en los archivos de Egregor Labs según el punto 5.5.

4.9.10. Requisitos para la verificación en línea del estado de revocación

Según el punto 4.9.10 de la Política. Para determinar el estado de un certificado mediante la CRL, el tercero usuario obtiene la CRL vigente, verifica su firma y su vigencia, y constata si el certificado figura en ella. Si no puede obtener una CRL vigente ni una respuesta OCSP, debe optar entre rechazar el documento, aceptarlo bajo su exclusiva responsabilidad o postergar la decisión.

La aplicación AdES verifica automáticamente, mediante OCSP, el estado de los certificados que muestra al verificar una firma.

4.9.11. Otras formas disponibles para la divulgación de la revocación

Según el punto 4.9.11 de la Política.

4.9.12. Requisitos específicos para casos de compromiso de claves

Según el punto 4.9.12 de la Política. Si Egregor Labs toma conocimiento de una vulnerabilidad que compromete un modelo o versión de módulo admitido, aplica el procedimiento del punto 6.2.11 de este Manual.

4.9.13. a 4.9.16. Suspensión

El estado de suspensión no está contemplado en el marco de la Ley N° 25.506 y su modificatoria.

4.10. Estado del certificado

4.10.1. Características técnicas

Según el punto 4.10.1 de la Política.

4.10.2. Disponibilidad del servicio

Según el punto 4.10.2 de la Política. El servicio OCSP y la publicación de la CRL funcionan en modo activo en el sitio principal y en espera activa en el de contingencia; la conmutación se realiza por DNS según el Plan de Contingencia.

4.10.3. Aspectos operativos

El respondedor OCSP consulta la base de estado de la AC en tiempo real. Cada respuesta se arma al momento de la consulta, con una validez (campo “nextUpdate”) de doce (12) horas, y devuelve el “nonce” de la consulta cuando lo trae. El servicio atiende en https://ocsp.advancedelectronicsignature.com y en https://advancedelectronicsignature.com/ocsp, por GET y por POST; las respuestas a consultas por GET pueden guardarse en caché hasta sesenta (60) segundos.

4.11. Desvinculación del suscriptor

Según el punto 4.11 de la Política. La eliminación de la cuenta en la aplicación AdES revoca todos los certificados del suscriptor según el punto 4.9.1.n) de la Política, pero no elimina el legajo, que se conserva según el punto 5.5.

4.12. Recuperación y custodia de claves privadas

Según el punto 4.12 de la Política.

5. Controles de seguridad física, operativos y de gestión

5.1. Controles de seguridad física

Según el punto 5.1 de la Política. Los sistemas de la AC se encuentran en el recinto exclusivo de Jacobs Comercial S.R.L. en el centro de datos principal, con los niveles de seguridad física descriptos en la Política y detallados en el Plan de Seguridad. El ingreso de cualquier persona a los niveles 3 a 6 se registra en el libro de accesos del sitio, con nombre, DNI, motivo, hora de ingreso y de egreso y acompañante.

5.2. Controles de gestión

Los roles son asignados por la Gerencia de Jacobs Comercial S.R.L. a propuesta del Responsable de la AC, respetando estos criterios: (a) cada rol tiene un titular y un suplente; (b) los roles se

asignan a personal de Jacobs Comercial S.R.L.; y (c) se respeta la separación de funciones del punto 5.2 de la Política.

Rol	Funciones principales	Cantidad mínima
Responsable de la AC	Dirige la AC; es el nexo con el Ente Licenciante; autoriza revocaciones de oficio y cambios; custodio	1 + suplente
Responsable de Seguridad	Mantiene el Plan de Seguridad; aprueba cambios y versiones de la aplicación AdES; revisa registros; gestiona incidentes; custodio	1 + suplente
Operadores de HSM	Ejecutan las ceremonias de clave y las operaciones sobre el HSM	2
Custodios	Guardan las credenciales de activación de la clave de la AC	5 (activación 3 de 5)
Administrador de sistemas	Opera servidores, redes, repositorio y copias de respaldo; sin acceso a credenciales de activación	1 + suplente
Auditor interno	Revisa en forma independiente registros y procedimientos; testigo de ceremonias	1
Responsable de la AR	Dirige la AR CENTRAL; supervisa a los Oficiales de Registro; revisa aprobaciones automáticas	1 + suplente
Oficiales de Registro	Validación presencial; verificación de documentación de personas jurídicas; resolución de observaciones; revocaciones de terceros	2
Responsable de Soporte Técnico	Mesa de Ayuda; atención y capacitación de suscriptores	1 + suplente

En la AC y en la AR CENTRAL se aplican los siguientes controles funcionales:

- Toda aprobación de una solicitud queda firmada digitalmente, por el Oficial de Registro o por la clave de servicio de la AR, lo que impide la manipulación posterior de los datos. La AC verifica esa firma antes de emitir.
- Los datos de identidad del certificado provienen de la respuesta del RENAPER o de la documentación verificada, y la AR controla su coincidencia con la CSR antes de aprobar.
- Previo a la emisión, la AC verifica la congruencia entre la solicitud aprobada y el certificado a emitir.
- Antes de poner en producción una nueva versión del software de la AC, de la AR o de la aplicación AdES, se ejecutan pruebas de aceptación y de seguridad, y el Responsable de Seguridad aprueba el pase.
- La base de datos registra todos los accesos y transacciones, y se ejecutan controles de consistencia diarios.

- Los servidores se monitorean en forma permanente para detectar archivos agregados o reemplazados sin autorización, y las alertas se envían al Administrador de sistemas y al Responsable de Seguridad.
- Si una alerta crítica no puede resolverse en cuatro (4) horas, o un HSM presenta una falla que no puede resolverse en dieciséis (16) horas, se trasladan las operaciones al sitio de contingencia.
- La emisión de cada CRL se monitorea y se compara con la anterior, y semanalmente se verifica que todos los certificados revocados estén incluidos.
- Se revisa periódicamente una muestra de las solicitudes y certificados contra la documentación del legajo.
- La Mesa de Ayuda está capacitada para asistir a los suscriptores por correo electrónico y teléfono.

5.3. Controles de seguridad del personal

Los controles de seguridad del personal que ocupa roles de confianza son establecidos por Jacobs Comercial S.R.L. e implementados por el Responsable de la AC con el apoyo de [Recursos Humanos / asesor externo].

a) Antecedentes, calificaciones, experiencia e idoneidad. Para cada persona vinculada a la certificación se mantiene un legajo con sus antecedentes laborales, calificaciones, experiencia e idoneidad. Los antecedentes se evalúan antes de asignar un rol, por el Responsable de la AC y, para los Oficiales de Registro, también por el Responsable de la AR. El proceso de selección incluye:

- certificado de antecedentes penales sin registros, que se conserva en el legajo;
- verificación de identidad con el DNI;
- comprobación de la veracidad del currículum, de los títulos y de las referencias laborales;
- entrevistas personales y una evaluación de conocimientos para el rol;
- firma de un acuerdo de confidencialidad antes de la designación.

b) Antecedentes laborales. Se verifican las referencias de los empleos anteriores declarados y, para los roles con acceso a la clave de la AC, se repite la verificación de antecedentes penales cada dos (2) años.

c) Entrenamiento y capacitación inicial. Antes de asumir el rol, cada persona recibe capacitación sobre: la Infraestructura de Firma Digital y su normativa; la Política, este Manual y el Plan de Seguridad; las responsabilidades de su rol; el uso del hardware y software que opera (HSM, aplicación de la AR, sistema del RENAPER, aplicación AdES); el manejo de incidentes; el Plan de Contingencia; y la protección de datos personales. Se registran la asistencia y la evaluación, y se extiende una constancia.

d) Frecuencia de actualización técnica. Al menos una (1) vez por año, y ante cada cambio en la normativa, en las plataformas o en los dispositivos admitidos. El Responsable de la AC informa al personal las novedades relevantes de firma digital y seguridad.

e) Rotación de cargos. No hay rotación programada entre roles. Los suplentes ejercen el rol durante las ausencias del titular, para mantener su práctica.

f) Sanciones por acciones no autorizadas.

1. Quien detecta una conducta que puede constituir una infracción la comunica de inmediato al Responsable de Seguridad.
2. Mientras se analiza, la persona involucrada queda suspendida en sus accesos físicos y lógicos a las áreas sensibles.
3. Dentro de los tres (3) días, el Responsable de Seguridad califica la infracción como leve, grave o muy grave. Las leves se sancionan con apercibimiento. Las graves y muy graves se elevan al Responsable de la AC, que instruye un expediente escrito, escucha a la persona involucrada y resuelve en forma fundada.
4. Las sanciones van desde el apercibimiento hasta la desvinculación y, para los Oficiales de Registro, la revocación de su certificado. Se notifican por medio fehaciente dentro de los dos (2) días de resueltas. Las sanciones muy graves se informan a la Gerencia.
5. Si hubo mala fe en el uso de los recursos de Jacobs Comercial S.R.L., se ejercen las acciones legales que correspondan. Las sanciones son revisables ante la jurisdicción competente.

g) Requisitos para la contratación de personal. El personal debe tener el conocimiento y la formación necesarios para su rol. Los requisitos mínimos de cada rol se definen en el Plan de Seguridad. El personal de proveedores que accede a las instalaciones lo hace siempre acompañado por personal autorizado y con registro.

h) Documentación y materiales provistos al personal. Al asumir el rol, cada persona recibe su designación escrita, las credenciales de acceso físico, su usuario y su segundo factor de autenticación y, según el rol, su token criptográfico o sus credenciales de custodio. Firma un acuse de recibo y el compromiso de confidencialidad. Al desvincularse, devuelve todo el material y sus accesos se dan de baja el mismo día.

5.4. Procedimientos de auditoría de seguridad

Egregor Labs mantiene registros de auditoría de todas las operaciones de la AC y de la AR CENTRAL, protegidos en medios seguros y conservados por diez (10) años como mínimo. Se usan para el monitoreo habitual, para las auditorías internas y para las auditorías del punto 8.

Los eventos de todos los componentes (AC, AR, repositorio, OCSP, firewalls, sistemas operativos y bases de datos) se envían en tiempo real a un servidor de registro centralizado, en la red de la AC, que los encadena criptográficamente. El sistema de gestión de eventos alerta por correo electrónico y mensaje al Administrador de sistemas y al Responsable de Seguridad ante eventos críticos. El Administrador de sistemas revisa diariamente las alertas y el Responsable de Seguridad revisa semanalmente los registros.

Los accesos físicos de solicitantes, visitantes y proveedores se registran en el libro de accesos de la AR CENTRAL, del sitio principal y del sitio de contingencia.

5.5. Conservación de registros de eventos

Egregor Labs genera y conserva registros de eventos con la siguiente información mínima: fecha y hora (año, mes, día, hora, minuto, segundo y huso horario), número de secuencia, tipo de registro, fuente e identificación de la entidad que efectuó el registro.

Ámbito	Eventos registrados
Ciclo de vida de las claves del Certificador	Generación y almacenamiento; resguardo; recuperación; retiro de datos relacionados con las claves; destrucción; identificación de quien autoriza cada operación; identificación de quien administra los datos de las claves (componentes, credenciales, dispositivos); compromiso de la clave privada
Ciclo de vida de los certificados	Recepción de solicitudes (inicial y de renovación); cambios en los datos de la solicitud; generación de certificados; aceptación o rechazo por el suscriptor; solicitudes de revocación y su resultado; emisión de CRL
Ciclo de vida de los dispositivos criptográficos	Ingreso o retiro de HSM y tokens del lugar de almacenamiento; envío a servicio técnico; retiro, baja o borrado; entrega de tokens a Oficiales de Registro con su número de serie
Información de la solicitud	Método de identificación (remoto o presencial) y documentos presentados; resultado y transacción del RENAPER; ubicación del legajo; Oficial de Registro o servicio que recibió y aprobó la solicitud; verificación de la atestación de la aplicación; modelo de dispositivo, versión de iOS y versión de la aplicación AdES
Eventos de seguridad	Lectura, modificación o borrado de archivos o registros críticos, incluido el registro de eventos; cambios en perfiles de seguridad; intentos exitosos y fallidos de acceso; caídas y fallas de hardware o software; acciones de operadores, administradores y responsables de seguridad; modificaciones en procesos de cifrado o autenticación; accesos a la AC o a sus componentes

Los registros no contienen claves privadas ni contraseñas en texto plano. Los relojes se sincronizan por NTP con un desvío menor a un (1) segundo, en UTC y configurados en UTC-3.

Conservación. Los registros y legajos se conservan diez (10) años desde la expiración o revocación del certificado al que se refieren. Se guardan cifrados con claves gestionadas en el HSM, con copia diaria en el sitio de contingencia. Solo los roles de auditoría y el Responsable de Seguridad pueden leerlos, y cada lectura queda registrada.

Obtención y verificación de la información archivada. Ante un requerimiento judicial o administrativo, o del titular, el Responsable de Seguridad extrae la información, verifica la integridad del encadenamiento criptográfico, la entrega en forma segura y registra la entrega.

Libros de actas. El Responsable de la AC registra en el libro de actas de la AC las ceremonias de clave, los resguardos y las pruebas de contingencia. El Responsable de la AR registra en el libro de actas de la AR las revocaciones resueltas por Oficiales de Registro y las contingencias. Los libros se guardan en la caja de seguridad del sitio correspondiente.

5.6. Cambio de claves criptográficas

Según el punto 5.6 de la Política.

Procedimiento de renovación de la clave de la AC

- **Frecuencia, oportunidad y urgencia:** cuando el período restante del certificado de la AC sea de dos (2) años más el período de validez de los certificados que emite. Planificado. Urgencia alta.
- **Roles:** Responsable de la AC; Operadores de HSM; Custodios; Responsable de Seguridad; Auditor interno.
- **Acción que lo pone en marcha:** alerta del monitoreo de vencimientos.
- **Tareas:**
    1. El Responsable de la AC convoca la ceremonia de generación de la nueva clave según el Anexo A.
    2. Los Operadores de HSM generan el nuevo par de claves y la solicitud de certificado, con la presencia de los custodios requeridos y del Auditor interno.
    3. El Responsable de la AC presenta la solicitud a la Autoridad de Aplicación para su firma por la AC-RAÍZ.
    4. Recibido el nuevo certificado, el Responsable de la AC autoriza su instalación y los Operadores lo instalan y lo copian al sitio de contingencia.
    5. El Administrador de sistemas publica el nuevo certificado en el repositorio y el Responsable de la AC lo publica en el Boletín Oficial.
    6. Desde ese momento, los nuevos certificados se firman con la clave nueva. La clave anterior solo firma CRL hasta el vencimiento del último certificado emitido con ella y luego se destruye según el punto 6.2.10 de la Política.
    7. Todo se registra en el libro de actas de la AC.
- **Resultado:** nueva clave y certificado de la AC en uso; clave anterior limitada a CRL.

5.7. Plan de respuesta a incidentes y recuperación ante desastres

Según el punto 5.7 de la Política. El Plan de Contingencia se aplica desde la declaración de la contingencia por el Responsable de la AC hasta el restablecimiento de la operación normal. Ante un incidente de seguridad:

1. Quien lo detecta lo informa al Responsable de Seguridad, que lo clasifica como crítico, alto, medio o bajo. Los críticos se escalan al Responsable de la AC en menos de una (1) hora.
2. Se contiene el incidente, se preserva la evidencia y se evalúa si afecta la clave de la AC, la emisión o los servicios de estado.
3. Todo incidente que afecte la clave de la AC, la emisión de certificados o la validación de identidad se informa al Ente Licenciante dentro de las veinticuatro (24) horas.

4. Se analiza la causa, se documentan las acciones correctivas y se actualizan los planes si corresponde.

5.8. Plan de Cese de Actividades

Según el punto 5.8 de la Política y el Plan de Cese de Actividades.

6. Controles de seguridad técnica

6.1. Generación e instalación del par de claves criptográficas

Según el punto 6.1 de la Política. La generación de la clave de la AC se realiza en la ceremonia descripta en el Anexo A. La generación de las claves de los suscriptores se realiza según el procedimiento del punto 3.2.1 de este Manual.

Entrega de tokens a los Oficiales de Registro. El Responsable de la AR entrega a cada Oficial de Registro un token nuevo con certificación FIPS 140 nivel 2 o superior, registra su número de serie y la recepción, y el Oficial de Registro inicializa el token y genera su clave en presencia del Responsable de la AR, sin que este conozca su contraseña.

6.2. Protección de la clave privada y controles sobre los dispositivos criptográficos

Según el punto 6.2 de la Política.

6.2.11. Requisitos de los dispositivos criptográficos

Según el punto 6.2.11 de la Política.

Procedimiento de mantenimiento del listado de dispositivos admitidos

- **Frecuencia, oportunidad y urgencia:** revisión mensual del estado de los certificados CMVP y ante cada nueva versión de iOS o cambio de estado publicado por el NIST. Planificado. Urgencia alta ante un cambio de estado.
- **Roles:** Responsable de Seguridad; Responsable de la AC; Administrador de sistemas; Responsable de Soporte Técnico.
- **Acción que lo pone en marcha:** la revisión periódica, la publicación de una nueva versión de iOS, un cambio de estado de un certificado CMVP o el conocimiento de una vulnerabilidad en el módulo criptográfico de un dispositivo admitido.
- **Tareas:**
    1. El Responsable de Seguridad verifica en el sitio del NIST el estado de los certificados de los módulos admitidos y las versiones de iOS que cubren.
    2. **Nueva versión de iOS cubierta por un certificado ACTIVO:** el Responsable de Seguridad propone su inclusión; el Responsable de la AC la aprueba; el Administrador de sistemas actualiza el listado en la AR y en el repositorio.
    3. **Nueva versión de iOS no cubierta por un certificado ACTIVO:** la AR rechaza las solicitudes nuevas desde esa versión. La aplicación AdES informa al

solicitante que debe esperar la certificación de esa versión. Los certificados emitidos en versiones anteriores admitidas siguen vigentes.

4. **Paso de un módulo a HISTÓRICO:** se excluye del listado para nuevas emisiones; se notifica a los suscriptores afectados que deben renovar en un dispositivo admitido antes de que se cumplan tres (3) años de la reclasificación; y la AR programa la revocación de los certificados que sigan vigentes a esa fecha.
5. **Vulnerabilidad que permita extraer la clave o usarla sin la autenticación del titular:** el Responsable de la AC suspende de inmediato las emisiones para los modelos o versiones afectados; evalúa con el Responsable de Seguridad si los certificados emitidos deben revocarse; si corresponde, los revoca con aviso previo a los suscriptores, sustituye gratuitamente los certificados según el punto 9.1 de la Política, e informa al Ente Licenciante.
6. Cada cambio se registra y el listado publicado indica su fecha de actualización.

- **Resultado:** listado de dispositivos admitidos actualizado y aplicado por la AR.

6.3. Otros aspectos de administración de claves

Según el punto 6.3 de la Política.

6.4. Datos de activación

Según el punto 6.4 de la Política. El procedimiento de distribución y custodia de las credenciales de activación de la clave de la AC está en el Anexo A.

6.5. Controles de seguridad informática

Según el punto 6.5 de la Política. En particular:

- Los servidores de la AC, de la AR y de los servicios de estado ejecutan sistemas operativos endurecidos según guías reconocidas, con solo los servicios necesarios.
- Los parches críticos se aplican dentro de las setenta y dos (72) horas, previa prueba en el ambiente de prueba.
- Las comunicaciones entre la aplicación AdES y la AR usan TLS 1.2 o superior, con verificación del certificado del servidor por la aplicación.
- Las bases de datos de la AR cifran los legajos con claves gestionadas en el HSM.
- Los accesos administrativos usan cuentas nominativas, doble factor y estaciones dedicadas.

6.6. Controles técnicos del ciclo de vida de los sistemas

Según el punto 6.6 de la Política.

Procedimiento de aprobación de versiones de la aplicación AdES

- **Frecuencia, oportunidad y urgencia:** ante cada nueva versión. Planificado. Urgencia según la naturaleza del cambio.
- **Roles:** equipo de desarrollo de Jacobs Comercial S.R.L.; Responsable de Seguridad; Responsable de la AC.

- **Acción que lo pone en marcha:** el equipo de desarrollo propone una nueva versión.
- **Tareas:**
    1. El equipo de desarrollo documenta los cambios e indica si afectan la generación de claves, la captura de rostro, la atestación, la firma o la comunicación con la AR.
    2. Si los afectan, el Responsable de Seguridad revisa el código de esos componentes y el resultado de las pruebas, y aprueba o rechaza la versión antes de su envío a la tienda.
    3. Publicada la versión, el Responsable de la AC decide si actualiza la versión mínima exigida por la AR. Ante correcciones de seguridad, la versión mínima se actualiza de inmediato.
    4. Cada versión aprobada y su código fuente se conservan.
- **Resultado:** versión aprobada y, en su caso, versión mínima actualizada.

6.7. Controles de seguridad de red

Según el punto 6.7 de la Política. Las zonas de red son: Internet; zona de servicios públicos (repositorio, OCSP, interfaz de la AR para la aplicación AdES); red interna de la AR; y red aislada de la AC. Las reglas de los firewalls se revisan cada seis (6) meses, junto con los análisis de seguridad de red.

6.8. Certificación de fecha y hora

No aplica.

6.9. Servicio de emisión de sello de competencia o atributo

No aplica.

7. Perfiles de certificados y de listas de certificados revocados

Según la sección 7 de la Política. Antes de poner en producción cualquier cambio en el software de la AC, se emiten certificados y CRL de prueba en el ambiente de prueba y se verifica su conformidad con los perfiles con una herramienta de análisis de certificados.

8. Auditoría de cumplimiento y otras evaluaciones

Según la sección 8 de la Política.

Procedimiento de auditoría interna

- **Frecuencia, oportunidad y urgencia:** anual, desde la fecha de la última auditoría, y ante cambios relevantes. Planificado. Urgencia baja, salvo situación excepcional.
- **Roles:** Auditor interno; Responsable de la AC; Responsable de la AR; Responsable de Seguridad; roles auditados.

- **Acción que lo pone en marcha:** haber transcurrido un año desde la última auditoría interna, o decisión del Responsable de la AC.
- **Tareas:**
    1. El Auditor interno planifica la auditoría sobre los temas de la sección 8 de la Política, incluida una muestra de legajos de emisiones remotas, presenciales y de personas jurídicas, y de revocaciones.
    2. Ejecuta la auditoría y elabora un informe que entrega a los roles auditados, con copia al Responsable de la AC.
    3. Los roles auditados responden por escrito y proponen acciones correctivas.
    4. El Responsable de la AC aprueba el plan de acción de no conformidades, con plazos, y lo eleva a la Gerencia.
    5. Si corresponde, se aplican sanciones según el punto 5.3.f.
    6. El Auditor interno verifica la ejecución del plan.
- **Resultado:** informe de auditoría interna, respuesta de los auditados, plan de acción y, en su caso, sanciones.

Jacobs Comercial S.R.L. facilita a los auditores del Ente Licenciante el acceso a las instalaciones, registros, legajos y personal, incluido el código fuente de la aplicación AdES y de la AR.

9. Aspectos legales y administrativos

9.1. Aranceles

Según el punto 9.1 de la Política.

Procedimiento de asignación de planes

- **Frecuencia, oportunidad y urgencia:** en cada solicitud, en cada compra o renovación y en cada firma con plan de prueba. Numerosas veces por día. Urgencia alta.
- **Roles:** solicitante o suscriptor; aplicación AdES; sistema de la AR CENTRAL; área comercial; Responsable de la AR.
- **Acción que lo pone en marcha:** el solicitante elige un plan, la App Store informa una compra, renovación, vencimiento o reembolso, el área comercial registra un pago directo, o se aprueba un convenio o una exención.
- **Tareas:**
    1. **Prueba:** al emitirse el primer certificado de una persona, el sistema de la AR le asigna cinco (5) firmas de prueba, por única vez por CUIL o CUIT. Antes de cada firma con este plan, la aplicación pide a la AR que descuente una firma; la AR no recibe el documento ni su huella.
    2. **Planes de persona humana:** se contratan con la App Store desde la aplicación AdES. La AR verifica la transacción firmada por Apple y asigna o extiende el plan. Las renovaciones, vencimientos y reembolsos los informa Apple a la AR, que actualiza el plan.
    3. **Persona jurídica:** el área comercial registra el pago con la factura de Jacobs Comercial S.R.L. y el período, y la AR asigna el plan.

4. **Convenios:** el área comercial valida la matrícula del solicitante con la entidad del convenio y la AR asigna el plan bonificado.
5. **Sector Público:** el Responsable de la AR verifica la condición de la entidad y aprueba la exención.
6. Ningún cambio de plan modifica el estado de los certificados.

- **Resultado:** plan asignado a la persona y registrado.

9.2. a 9.11.

Según los puntos 9.2 a 9.11 de la Política. Las responsabilidades de los roles que gestionan información confidencial se detallan en el punto 5.2 de este Manual y en el Plan de Seguridad.

9.12. Gestión del ciclo de vida del documento

Según el punto 9.12 de la Política. Este Manual se revisa junto con la Política. Los cambios en el Anexo A se presentan al Ente Licenciante como documento reservado.

9.13. a 9.17.

Según los puntos 9.13 a 9.17 de la Política.

Procedimiento de atención de reclamos

- **Frecuencia, oportunidad y urgencia:** ante cada reclamo. Poco frecuente. Urgencia media.
- **Roles:** reclamante; Responsable de Soporte Técnico; Responsable de la AC.
- **Acción que lo pone en marcha:** recepción de un reclamo escrito en reclamos@advancedelectronicsignature.com o en el domicilio de Jacobs Comercial S.R.L.
- **Tareas:**
    1. El Responsable de Soporte Técnico registra el reclamo y acusa recibo dentro de las cuarenta y ocho (48) horas.
    2. El Responsable de la AC labra el acta y sigue el procedimiento del punto 9.13 de la Política.
    3. La resolución se notifica al reclamante con la indicación de que puede recurrir a la Autoridad de Aplicación.
- **Resultado:** reclamo resuelto y archivado.