Proveedor de Certificados PROCERT ITFB, C. A.
Declaración sobre la Implantación y Uso de Procesos KYC

Fecha	Junio, 2026
Edición	1
Versión	1
Elaborado por	Gerencia General junio 2026
Aprobado	Alta Dirección junio 2026
Descripción	Declaración sobre la Implantación y Uso de Procesos KYC
Vigente	Si

1. Título**:** Declaración sobre la Implantación y Uso de Procesos KYC

2. Código**:** AC-D-00__.

3. Introducción: El presente documento contiene la Declaración sobre la Implantación y Uso de Procesos KYC de Proveedor de Certificados PROCERT ITFB, C.A. y tiene como objeto principal informar sobre la base de los mejores principios y prácticas de gestión, orientadas a la mejora continua de los procesos de generación de certificados electrónicos por parte de PROCERT, en cumplimiento de principios éticos, valores, los requisitos impuestos por la Ley de Mensajes de Datos y Firmas Electrónica y su Reglamento, las normas de la Superintendencia de Servicios de Certificación Electrónica y los lineamientos del CA Browser Forum

4. Objetivo**:** El objetivo del presente documento de la Declaración sobre la Implantación y Uso de Procesos KYC, se constituye en el establecimiento de las mejores prácticas, procesos y normas orientadas al cumplimiento de la regulación aplicable y vigente dentro y fuera de la República Bolivariana de Venezuela en materia de prevención de actividades que se traduzcan en la facilitación de prevención de legitimación de capitales o de financiamiento del terrorismo y de armas de destrucción masiva; así como el debido proceso de conocer a las personas políticamente expuesta (PEP y es aplicable clientes, empleados y proveedores, asegurando el cumplimiento de estándares regulatorios, mitigación de riesgos y preservación de la integridad del ecosistema de certificación digital.

5. Alcance: El presente Documento de la Declaración sobre la Implantación y Uso de Procesos KYC de Proveedor de Certificados PROCERT ITFB, C.A, aplica a la Alta Dirección, Personal que labora bajo dependencia y por contratación tercerizada y proveedores de bienes y servicios de Proveedor de Certificados PROCERT ITFB, C.A. y para todo proceso asociados a la generación de certificados, gestión de adquisiciones de bienes, servicios e insumos requeridos para la operación regular de PROCERT y para el manejo y administración de personal interno y contratados de PROCERT; todo ello en cumplimiento de las normas vigentes y aplicables de prevención de legitimación de capitales o de financiamiento del terrorismo y de armas de destrucción masiva; así como el debido proceso de conocer a las personas políticamente expuesta (PEP).

6. Principios rectores: A los fines de dar cumplimiento a la Declaración sobre la Implantación y Uso de Procesos KYC de Proveedor de Certificados PROCERT ITFB, C.A, se han establecido una serie de principios rectores, los cuales se indican a continuación:

    6.1. Aplicación de los procesos y validación KYC*:* PROCERT ITFB, C.A, implementa procesos KYC bajo los siguientes principios:

        - Verificación de identidad confiable
        - Trazabilidad y auditabilidad
        - Enfoque basado en riesgo (Risk-Based Approach)
        - Cumplimiento normativo (CA/B Forum, AML, GDPR o equivalentes)
        - Seguridad y protección de datos personales

6.2. Procesos KYC para Clientes

6.2.1. Identificación inicial

- Recolección de datos:
  - Nombre legal completo
  - Identificación oficial (pasaporte o cédula de identidad, En el extranjero el ID nacional)
  - Registro de Información Fiscal (RIF) o documento de registro fiscal en el exterior.
  - Información de la organización (si aplica)
- Validación contra:
  - Registros oficiales
  - Bases de datos gubernamentales y comerciales
  - Listas de sanciones (OFAC, UE, ONU)

6.2.2. Verificación

- Verificación documental
- Validación de dominio y control organizacional (para certificados TLS/Code Signing)
- Verificación de existencia legal de la entidad.

6.2.3. Evaluación de riesgo

- Clasificación del cliente según:
- Tipo de organización (pública, privada, ONG, Asociación Civil, etc.)
- Tipo de certificado solicitado
- Actividad económica
- Aplicación de medidas reforzadas (EDD) en caso de alto riesgo.

6.2.4. Aprobación y registro

- Registro seguro de evidencia KYC
- Conservación conforme a políticas de retención y almacenamiento por 10 años.

6.2.5. Monitoreo continuo

- Revalidación periódica.
- Revisión ante eventos relevantes (revocación, cambios corporativos)

6.3. Procesos KYC para Empleados

6.3.1. Verificación previa a la contratación

- Validación de identidad
- Cumplir con el registro del formato KYC para trabajadores
- Mantener y actualizar formato KYC para trabajadores
- Verificación de antecedentes:
  - Académicos
  - Laborales

6.3.2. Clasificación por rol

- Asignación basada en nivel de acceso:
  - Acceso a HSM
  - Sistemas PKI
  - Procesos de emisión/revocación
  - Procesos de Autoridad de Registro

- Procesos de Seguridad de la información.

6.3.3. Control de acceso
- Aplicación de principio de mínimo privilegio
- Autenticación fuerte (MFA)
- Registro y monitoreo de actividades.
- SOC y NOC
- Registros de Logs.

6.3.4. Monitoreo continuo
- Evaluaciones periódicas
- Revisión de comportamiento anómalo
- Revalidación de controles internos

6.4. Procesos KYC para Proveedores y Terceros

6.4.1. Due diligence inicial
- Verificación legal de la entidad
- Identificación de beneficiarios finales (UBO)
- Evaluación de reputación y cumplimiento.
- Cumplir con el registro del formato KYC para proveedores
- Mantener y actualizar formato KYC para proveedores

6.4.2. Evaluación de riesgos
- Clasificación según:
  - Tipo de servicio (crítico/no crítico)
  - Acceso a información sensible
  - Ubicación geográfica
  - Empresa en listas de cumplimiento
  - Cumplimiento gubernamental

6.4.2. Contratación
- Inclusión de cláusulas de:
  - Seguridad de la información
  - Protección de datos
  - Cumplimiento de estándares (ej. WebTrust, ISO 27001)
  - Confidencialidad de la información.
  - Cumplimiento normativo
  - Contratista independiente.
  -

6.4.3. Monitoreo continuo
- Evaluaciones periódicas
- Validación de Auditorías (internas o externas)
- Revisión de incidentes de seguridad
- Cumplimiento normativo y de permisos.

6.5. Gestión de la Información y Protección de Datos
- La información KYC será:
  - Almacenada de forma segura (cifrado, control de accesos)
  - Accesible únicamente a personal autorizado
- Cumplimiento con normativas de privacidad aplicables
- Eliminación segura tras expiración del periodo de retención
- Entregada solo bajo requerimiento judicial firma.

6.6. Auditoría y Cumplimiento
- Revisión periódica de procesos KYC
- Auditorías independientes (WebTrust y SUSCERTE))
- Mantenimiento de registros para inspección regulatoria
- Gestión de no conformidades y mejora continua

6.7. Gobernanza
- Se creó en la organización y se mantiene un responsable de cumplimiento (Compliance Officer)
- Existen políticas internas de establecimientos de funciones y roles por cargo y área, donde se definen las responsabilidades y funciones de forma clara.
- Descripción de puestos de trabajo para los distintos cargos.
- Procedimientos documentados para cambios en la PKI y controles de versiones del software de PROCERT
- Reporte periódico a dirección sobre riesgos y controles KYC
- Establecimiento de un Comité de Seguridad.

7. Actores sujetos al cumplimiento de la política**.** El presente Documento de la Declaración sobre la Implantación y Uso de Procesos KYC es emitido en cumplimiento de las normas legales vigentes y aplicables en materia de prevención de legitimación de capitales o de financiamiento del terrorismo y de armas de destrucción masiva; así como el debido proceso de conocer a las personas políticamente expuesta (PEP) y se constituye en norma de obligatorio cumplimiento y sujeción por parte de los actores que se indican a continuación:

- Alta Dirección de PROCERT.
- Empleados de PROCERT.
- Proveedores de PROCERT.
- Clientes de PROCERT

8. Mecanismo para el desarrollo, ajuste y aprobación**.**

8.1. Mecanismo de desarrollo del documento***:*** El presente Documento de la Declaración sobre la Implantación y Uso de Procesos KYC se encuentra desarrollado sobre la base de la normativa de prevención de legitimación de capitales o de financiamiento del terrorismo y de armas de destrucción masiva; así como el debido proceso de conocer a las personas políticamente expuesta (PEP)**.**

8.2. Mecanismo para ajuste del documento**:** Los cambios en la Resolución No. 18-12-01de fecha 4 de diciembre de 2018, contentiva de las “Normas Generales sobre los Sistemas de Pago y Proveedores no Bancarios de Servicios de Pago que Operan en el País”, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela No. 41.547 de fecha 17 de diciembre de 2018; de las normas de prevención de legitimación de capitales y financiamiento al terrorismo dictadas por la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), que contemplen cambios sustanciales en los procesos de seguridad y operación, los cuales incluyan variación de los procedimientos y actividades de PROCERT producirán una revisión del presente documento, con el fin de ajustar los procesos y procedimientos a los estándares y normativa aplicable y aprobada por la legislación vigente o el ejecutivo nacional. Todo ajuste a la presente Declaración sobre la Implantación y Uso de Procesos KYC,

será producto del trabajo del equipo técnico y legal de PROCERT y requerirá contar para su implantación, con la aprobación de Alta Dirección.

8.3. Mecanismo para aprobación de los ajustes al documento**:** Todo ajuste o modificación de la Declaración sobre la Implantación y Uso de Procesos KYC deberá contar con la aprobación de la Alta Dirección de PROCERT, ser documentada y constar por escrito, señalando el número de edición y revisión, fecha de elaboración, fecha de aprobación y la firma del representante de la Alta Dirección que aprueba el ajuste o modificación.

9. Marco legal y normativo**.**
   - Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento.
   - Normativa de la SUSCERTE.
   - Normativa PROCERT.
   - Norma ISO 9000:2005.
   - Norma ISO/IEC 9594-8.
   - Norma ISO/TR 10013:2001.
   - Norma ISO/IEC 27001:2006.
   - Resolución No. 18-12-01de fecha 4 de diciembre de 2018, contentiva de las "Normas Generales sobre los Sistemas de Pago y Proveedores no Bancarios de Servicios de Pago que Operan en el País", publicada en la Gaceta Oficial de la República Bolivariana de Venezuela No. 41.547 de fecha 17 de diciembre de 2018.
   - Normas de prevención de legitimación de capitales y financiamiento al terrorismo dictadas por la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN).

10. Funciones y responsabilidades dentro de la AC PROCERT**:** Las funciones y responsabilidades de los distintos niveles de PROCERT, respecto al manejo, control y resguardo del presente documento, se encuentran definidos en el Documento de la Política para el Establecimiento de Funciones y Responsabilidades.

11. Revisión, aprobación y modificación**:** Los procesos asociados a la revisión, aprobación, modificación o ajuste de la documentación de PROCERT, serán regulados por el Documento de la Política de Documentación y Gestión Documental y será ejecutada cada seis (6) meses.