PROCEDIMIENTO DE HOMOLOGACIÓN DE DISPOSITIVOS CRIPTOGRÁFICOS PARA LA PLATAFORMA DE GENERACIÓN DE CERTIFICADOS DIGITALES DE ENTIDAD FINAL DE CLASE III EMITIDOS POR EL RENIEC

1. Preliminares

   En el contexto del presente documento, un dispositivo criptográfico es un smartcard (con interfaz de contacto y/o proximidad) y/o token (con interfaz USB) con capacidad de realizar operaciones criptográficas. Un dispositivo criptográfico homologado, puede ser utilizado por la *plataforma de generación de certificados digitales del RENIEC* (en adelante la Plataforma), para generar certificados digitales de persona jurídica de clase III emitidos por la ECEP-RENIEC.

   Posterior a esta generación, el dispositivo criptográfico estará en la capacidad de realizar operaciones de firma digital con un software de generación de firma digital acreditado por la AAC en el marco de la IOFE.

2. Propósito

   El propósito de la homologación de un dispositivo criptográfico es:

   i. Integrar el dispositivo en la Plataforma.
   ii. Realizar las pruebas de regresión para el mantenimiento evolutivo de la Plataforma.

3. Vigencia

   El periodo de vigencia de la homologación es temporal. A un dispositivo criptográfico que satisface determinados requisitos normativos y técnicos, se le concede la condición de *homologado* para una determinada versión de la Plataforma. La vigencia depende, entre otros, principalmente de los siguientes factores:

   i. Evolución tecnológica de los estándares de seguridad para los dispositivos criptográficos
   ii. Soporte técnico del dispositivo criptográfico
   iii. Soporte y vigencia de los sistemas operativos de usuario final
   iv. Actualizaciones de seguridad de los navegadores web
   v. Vigencia tecnológica de los componentes de seguridad que subyacen a la Plataforma

   El RENIEC puede agregar, suprimir y/o modificar estos factores, en concordancia con la evolución tecnológica de los mismos, y en el momento que sea pertinente, sin necesidad de comunicación previa.

4. Requisitos

   Si una Entidad pública o empresa (en adelante la Organización) considera necesario que el área técnica especializada del RENIEC evalúe si un dispositivo criptográfico satisface los requisitos normativos y técnicos, la Organización deberá solicitar al RENIEC, mediante la Ficha IV, la evaluación del dispositivo, adjuntando lo siguiente:

   i. Un (01) dispositivo criptográfico del modelo a homologar

ii. El código o número de certificación de seguridad FIPS 140-2 y/o Common Criteria
iii. El brochure técnico del dispositivo criptográfico emitido por el fabricante
iv. El software (Middleware) del dispositivo criptográfico
v. La guía de usuario del dispositivo criptográfico

Realizada la evaluación del dispositivo criptográfico, se entregará un reporte de cumplimiento de los requisitos técnicos/funcionales (Ficha III).

5. Mantenimiento evolutivo

A efectos de que el dispositivo criptográfico homologado mantenga esta condición en las futuras versiones de la plataforma, se recomienda que, la Organización no solicite la devolución del dispositivo, mientras considere necesario que el referido modelo continúe homologado en las versiones posteriores de la Plataforma.

6. Procedimiento

El procedimiento de homologación consta de las etapas descritas en la siguiente Ilustración, y son realizadas de acuerdo a lo establecido en las Fichas I y II:

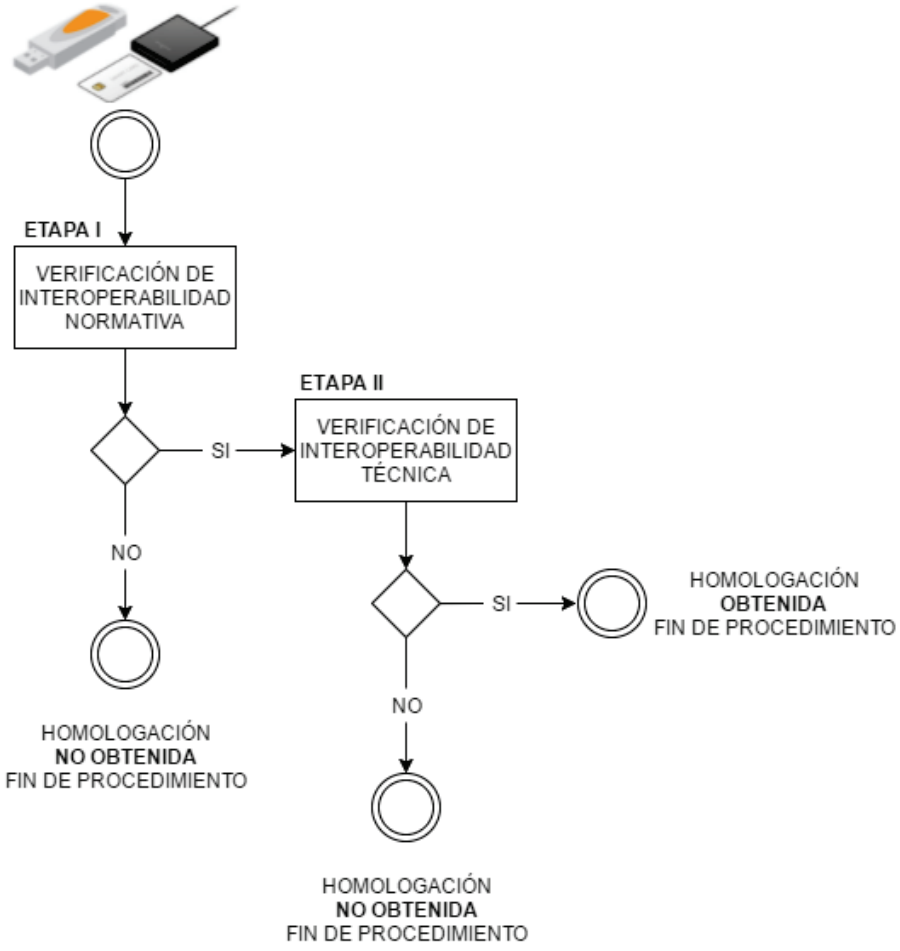

Ilustración 1 - Etapas de la homologación de dispositivos criptográficos en una determinada versión de la plataforma de generación de certificados digitales emitidos por el RENIEC

Nota: En el caso de que el RENIEC necesite realizar alguna consulta técnica en referencia al dispositivo, y esta no sea atendida oportunamente por la Organización, el procedimiento continuará conforme al flujo antes descrito.

FICHA I

ETAPA I - INTEROPERABILIDAD NORMATIVA (IOFE)

CERTIFICACIONES DE SEGURIDAD REQUERIDAS PARA LOS DISPOSITIVOS CRIPTOGRÁFICOS (TOKEN & SMART CARD) PARA SER UTILIZADOS EN APLICACIONES DE GENERACIÓN DE FIRMA DIGITAL

Requisitos mínimos obligatorios para la utilización de dispositivos criptográficos que almacenan llaves privadas y certificados digitales de clase III para aplicaciones de generación de firma digital, emitidos por la ECEP-RENIEC para entidades finales en el marco de la IOFE.

La evaluación del dispositivo requiere de las verificaciones normativas, en particular, las que se refieren a las certificaciones de seguridad de acuerdo a las Guías de Acreditación de la Autoridad Administrativa Competente (INDECOPI). Normativamente, el dispositivo debe contar con una de las siguientes certificaciones como mínimo:

FIPS 140-2	Nivel 1
Common Criteria	EAL4+

1 . Certificaciones de seguridad

Para esta verificación, es necesario identificar y proveer las certificaciones indicadas anteriormente que satisface el referido dispositivo, suministrando el(los) número(s) o código(s) de certificación de seguridad del producto.

A continuación, se describe un ejemplo por cada certificación de seguridad que debe ser proveída.

1. Certificación FIPS.

   La certificación es dada conjuntamente: Hardware + Firmware + Application

Certificación de seguridad FIPS 140-2	
Módulo criptográfico	**iKey 4000 USB Token (Level 3)**
Certificado Nº	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm#943
Diploma Nº (Certificado único)	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt943.pdf
Security Policy	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp943.pdf

2. Certificación Common Criteria.

   La certificación es dada por separado: Hardware & (Firmware + Application)

Certificación de seguridad Common Criteria		
Dispositivo criptográfico		**Link**
Hardware: (EAL5+) Microcontrolador ST19WR66I	Reporte de certificación 2006/18	https://www.commoncriteriaportal.org/files/epfiles/2006_18en.pdf
	Security Target	https://www.commoncriteriaportal.org/files/epfiles/cible2006_18en.pdf
Firmware + Application: (EAL4+) Touch&Sign2048	Reporte de certificación BSI-DSZ-CC-0422-2008	https://www.commoncriteriaportal.org/files/epfiles/20080527_0422a.pdf
	Security Target	https://www.commoncriteriaportal.org/files/epfiles/20080527_0422b.pdf

FICHA II

ETAPA II - INTEROPERABILIDAD TÉCNICA (RENIEC)

REQUISITOS TECNICOS PARA LOS DISPOSITIVOS CRIPTOGRÁFICOS (TOKEN & SMART CARD) PARA LA GENERACIÓN DE CERTIFICADOS DIGITALES DE CLASE III PARA ENTIDADES FINALES EMITIDOS POR LA ECEP-RENIEC

1. Requisitos mínimos obligatorios para la generación de llaves y certificados digitales de la clase III para entidades finales emitidos por la ECEP-RENIEC.

Algoritmos de hash	1	SHA-2
Algoritmos de firma	2	RSAwithSHA2
Formato de certificados	3	X.509 v3
Estándares	4 5 6	ISO 7816 1, 2, 3, 4 Smart card: Tamaño conforme al ISO 7810 (ID-1) Smart card: Driver (compatible con PC/SC)
Sistema operativo	7	MS Windows 7, 8 & 10 (32/64 bits)
Conectividad	8	Token: (USB 2.0)
Memoria mínima disponible para el usuario	9	16 Kb
Funciones criptográficas (en el chip)	10 11 12 13 14 15 16	Generación de llaves RSA de 2048 bits Generación de Firma Digital Verificación de Firma Digital Operación de resumen (Hashing) Importación de cadenas de certificados digitales Uso de PIN como la credencial de autorización a las operaciones criptográficas en el dispositivo Almacenamiento seguro de llaves privadas protegidas con PINes
Middleware para PC	17 18	Librerías PKCS#11 v2.20 o superior para Windows Microsoft Minidriver
Funcionalidades del middleware para PC	19 20	Estándar PKCS#10: Generación y firma de la solicitud de certificado (CSR) Estándar PKCS#11: Generación de llaves RSA e importación de la cadena de certificados del RENIEC (usuario final, intermedios & raíz) (*)
Interfaces de acceso para uso	21	Posterior a la generación de certificados digitales en el dispositivo, el acceso a los mismos debe ser posible a través de las interfaces: PKCS#11 y MSCAPI

(*) En el caso que el (token/smartcard) solamente tenga la capacidad de permitir la importación del certificado de usuario final en el dispositivo, y no los certificados digitales de autoridades; la Entidad/Institución o usuario final, será responsable del despliegue en su plataforma de los certificados intermedios y/o raíz del RENIEC.

2. Requisitos para el uso (posterior a la generación de certificados digitales por el RENIEC) de los dispositivos criptográficos por la Entidad Pública.

   De ser requerido por la Entidad/Institución, ésta deberá agregar a los requisitos mínimos obligatorios anteriores (numeral 1.) los requisitos que exigen sus Casos de Uso y sus Sistemas de Información.

   Por ejemplo, si la Entidad/Institución contempla utilizar smart cards o tokens criptográficos con certificados digitales en sistemas operativos Linux, la entidad pública debería exigir al proveedor o fabricante, entre otros, los requisitos adicionales siguientes:

Sistema operativo compatible	• Linux (Distribución y versión)
Estándares	• Smart card - Driver (PC/SC Lite)
API criptográfico compatible	• Dependencias (SharedObject.so) que implementan el estándar PKCS#11, para Linux (Distribución y versión)
Interfaces de acceso para su uso	• Posterior a la generación de certificados digitales en el dispositivo, el acceso a los mismos deben ser posible a través de la interfaz PKCS#11

FICHA III

REPORTE DE EVALUACION DE DISPOSITIVO CRITOGRÁFICO PARA GENERACIÓN DE CERTIFICADOS DIGITALES DE CLASE III PARA ENTIDADES FINALES EMITIDOS POR LA ECEP-RENIEC					
REPORTE N°		**FECHA**		**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

PRESENTACIÓN	
1. Token	
USB	
2. Smart Card	
Contacto	
Proximidad	
Dual	

DATOS DEL PRODUCTO		
Marca		
Modelo		
Número de serie lógico		
Número de serie físico		
¿Cuenta con drivers?		
¿Cuenta con manuales?		

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager		Versión del Manager	
Librería PKCS#11		Fecha de despliegue	

2. EVALUACIÓN

ETAPA I	**INTEROPERABILIDAD NORMATIVA**		
FIPS 140-2	Nivel		
	URL Nivel		
	URL Certificado		
Common Criteria	Nivel		
	URL HW		
	URL FW		
	URL APP		

ETAPA II	**INTEROPERABILIDAD TÉCNICA**
Generación de par de llaves RSA de 2048 bits	
Generación de CSR	
Importación de certificado de entidad final (usuario)	
Importación de certificados digitales de autoridades (intermedia y raíz)	
¿La librería PKCS#11 funciona en modo standalone?	

Nota: El certificado generado pertenece a la jerarquía de certificación SHA1 de la ECEP-RENIEC

3. VERIFICACIÓN DE GENERACIÓN DE FIRMA DIGITAL

Prueba satisfactoria de generación de firma digital con el software ReFirma 1.4.7 acreditado por la AAC	

4. CONCLUSIÓN

¿Cumple los requisitos mínimos?	

5. OBSERVACIONES Y COMENTARIOS

Nota: En el contexto de este documento, el acrónimo PIN (Personal Identification Number) se utiliza para referirse a una secuencia de caracteres alfanuméricos

FICHA IV

Asunto: Solicitud de homologación de dispositivo criptográfico para ser utilizado en la generación de certificados digitales de clase III por la ECEP-RENIEC

Sub Gerente de Certificación e Identidad Digital

Registro Nacional de Identificación y Estado Civil

Presente.

Es grato dirigirme a Usted, y en relación con el asunto en referencia, conforme lo indica el procedimiento de homologación de dispositivos criptográficos para ser utilizados en la plataforma de generación de certificados digitales de clase III de la ECEP-RENIEC, para solicitar la evaluación de un dispositivo criptográfico, y verificar la conformidad de los requisitos normativos y técnicos mínimos con la finalidad de proceder a su uso por parte de nuestra Organización (Entidad/Empresa)_____

En ese sentido se remite adjunto lo siguiente:

- 01 Dispositivo criptográfico

Presentación:	
Marca:	
Modelo:	
Serie física y/o lógica:	

- 01 CD ROM conteniendo

Código o Número de certificación de seguridad FIPS 140-2 y/o Common Criteria
Brochure técnico del dispositivo emitido por el fabricante
Software (Middleware) del dispositivo
Guía del usuario del dispositivo

- Datos del Especialista técnico de la Organización
  (Quién será el responsable de las coordinaciones y/o comunicaciones que se requieran durante el proceso de homologación)

Nombre:	
Email:	
Teléfono:	

Atentamente.

_____

Nombres y Apellidos del Representante de la Organización

Organización