CESAR ROBERTO ROSALES MAQUERA
Sub Director de Servicios de Certificación Digital
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
Firmado digitalmente por: ROSALES MAQUERA Cesar Roberto FAU 20295613620 soft
Motivo: En señal de conformidad
Fecha: 17/07/2024 18:07:17-0500

HÉCTOR EDUARDO SARAVIA MARTÍNEZ
Director de Certificación y Servicios Digitales
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
Firmado digitalmente por: SARAVIA MARTINEZ Hector Eduardo FAU 20295613620 hard
Motivo: En señal de conformidad
Fecha: 17/07/2024 18:12:47-0500

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

ENTIDAD DE CERTIFICACIÓN PARA EL ESTADO PERUANO

ECEP-RENIEC

Código: DA-DCSD/SDSCD-001		
OID: 1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0		
Versión: 4.0	**Año:** 2024	
Elaborado por: Sub Dirección de Servicios de Certificación Digital	**Revisado por:** Sub Director de Servicios de Certificación Digital	**Aprobado por:** Director de Certificación y Servicios Digitales

FIRMA DIGITAL
Firmado digitalmente por: RAMIREZ SALAZAR Alejandro Javier FIR 43520433 hard
Motivo: En señal de conformidad
Fecha: 17/07/2024 13:22:42-0500

FIRMA DIGITAL
Firmado digitalmente por: GALLO MONTANI Alfredo Rafael FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 17/07/2024 14:59:22-0500

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	18/05/2017	Elaboración y Aprobación	GRCD/SGCID	Aprobado
1.1	06/11/2017	Actualización	GRCD/SGCID	Aprobado
1.2	14/11/2017	Se recoge observaciones del evaluador de INDECOPI.	GRCD/SGCID	Aprobado
1.3	07/12/2018	Actualización	GRCD/SGCID	Aprobado
2.0	03/04/2019	Actualización de perfiles de entidad final y aplicación del régimen excepcional, Decreto Legislativo N° 1370, incorporación de la cuarta disposición complementaria, transitoria y final de la Ley Nº 27269, Ley de Firmas y Certificados Digitales.	GRCD/SGCID	Aprobado
2.1	12/07/2019	Actualización de perfiles de entidad final y aplicación del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital	GRCD/SGCID	Aprobado
3.0	21/02/2022	Incorporación de Nivel 1 de la jerarquía PKI, ampliación del régimen excepcional para el accionar de la SUNAT como EREP, aprobación del nuevo ROF del RENIEC, incorporación de perfiles de certificados correspondientes a nueva instancia de EC de nivel 3 Clase 2, segunda generación.	DCSD/SDSCD	Aprobado
3.1	20/07/2022	Incorporación de perfiles de certificados correspondientes a nueva instancia de EC de nivel 3 Clase 1, segunda generación.	DCSD/SDSCD	Aprobado
3.2	23/01/2023	Incorporación de la ECERNEP a cargo de la SGTD-PCM, ampliación del régimen excepcional para el accionar de la SUNAT como EREP y retiro de perfiles de certificados gestionados por la ECERNEP.	DCSD/SDSCD	Aprobado
4.0	17/07/2024	Actualización . Se retira menciones de EREP-SUNAT y de Certificado Digital Tributario por disposición de la AAC – INDECOPI.	DCSD/SDSCD	Aprobado

ÍNDICE

1. INTRODUCCIÓN 12
1.1. Visión general 12
1.2. Nombre e identificación del documento 12
1.3. Participantes 12
1.3.1. Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) 13
1.3.2. Entidades de Certificación para el Estado Peruano (ECEP) 13
1.3.3. Entidades de Registro o Verificación para el Estado Peruano (EREP) 13
1.3.4. Entidades Prestadoras de Servicios de Valor Añadido (PSVA) 14
1.3.5. Titulares y suscriptores 14
1.3.6. Terceros que confían 14
1.3.7. Otros participantes 14
1.4. Uso de un certificado digital 14
1.4.1. Usos apropiados de los certificados digitales 14
1.4.2. Usos prohibidos del certificado 15
1.5. Administración de la CPS 15
1.5.1. Organización que administra el documento 15
1.5.2. Persona de contacto 15
1.5.3. Persona que determina la conformidad de la CPS con la CP 15
1.5.4. Procedimiento de aprobación de la CPS 15
1.6. Definiciones, abreviaturas y acrónimos 15
2. RESPONSABILIDADES DEL REPOSITORIO Y SU PUBLICACIÓN 17
2.1. Repositorios 17
2.2. Actualización 17
2.3. Frecuencia de publicación 17
2.4. Control de acceso a los repositorios 18
3. IDENTIFICACIÓN Y AUTENTICACIÓN 19
3.1. Convención de nombres 19
3.1.1. Tipos de nombres 19
3.1.2. Necesidad de nombres significativos 19
3.1.3. Anonimato o seudónimo de los suscriptores 19
3.1.4. Reglas de interpretación de diferentes modalidades de nombres 19
3.1.5. Unicidad de Nombres 20
3.1.6. Reconocimiento, autenticación y rol de las marcas registradas 21

3.2. Validación inicial de la identidad 21
3.2.1. Método para probar posesión de la llave privada 21
3.2.2. Autenticación de identidad de personas jurídicas 21
3.2.3. Autenticación de identidad de personas naturales 21
3.2.4. Información no verificada del suscriptor 21
3.2.5. Validación de autoridad para efectuar la solicitud 22
3.2.6. Criterios de interoperabilidad 22
3.3. Identificación y autenticación para solicitudes de reemisión con renovación de llaves 22
3.3.1. Solicitudes rutinarias de renovación de llaves 22
3.3.2. Renovación de llaves luego de la cancelación 22
3.4. Identificación y autenticación para solicitudes de cancelación 22
4. CICLO DE VIDA DEL CERTIFICADO DIGITAL: REQUISITOS OPERACIONALES 23
4.1. Solicitud de certificado digital 23
4.1.1. Personas habilitadas para presentar una solicitud de certificado 23
4.1.2. Proceso de registro de solicitud y responsabilidades 23
4.2. Procesamiento de la solicitud de certificado 23
4.2.1. Identificación y autenticación 23
4.2.2. Aprobación o rechazo de las solicitudes de certificado 23
4.2.3. Tiempo límite para el procesamiento de las solicitudes 24
4.3. Emisión del certificado 24
4.3.1. Acciones durante la emisión del certificado 24
4.3.2. Notificación al suscriptor respecto a la emisión de un certificado 24
4.4. Aceptación del certificado 24
4.4.1. Conducta constitutiva de aceptación del certificado 24
4.4.2. Publicación del certificado por parte de la ECEP 24
4.4.3. Notificación de la EC a otras entidades sobre la emisión de un certificado 24
4.5. Uso del par de llaves y del certificado 24
4.5.1. Uso de la llave privada y del certificado por parte del suscriptor 24
4.5.2. Uso de la llave pública y del certificado por el tercero que confía 25
4.6. Renovación del certificado 25
4.6.1. Circunstancias para la renovación de los certificados 25
4.6.2. Personas habilitadas para presentar una solicitud de renovación 25
4.6.3. Procesamiento de solicitudes de renovación 26

4.6.4. Notificación al suscriptor sobre la emisión de un nuevo certificado 26
4.6.5. Conducta constitutiva de aceptación de renovación de certificados 26
4.6.6. Publicación del certificado por parte de la EC 26
4.6.7. Notificación de la EC a otras entidades sobre la renovación de un certificado 26
4.7. Reemisión de certificado digital con renovación de llaves 26
4.7.1. Criterios para la renovación de llaves de un certificado 26
4.7.2. Solicitantes de renovación de llaves de un certificado 26
4.7.3. Procesamiento de solicitudes de renovación de llaves de un certificado 26
4.7.4. Notificación al suscriptor sobre la re-emisión de un nuevo certificado 26
4.7.5. Conducta constitutiva de aceptación de certificados con renovación de llaves 26
4.7.6. Publicación del certificado con renovación de llaves 26
4.7.7. Notificación de la EC a otras entidades sobre la re-emisión de un certificado 26
4.8. Modificación del certificado 26
4.8.1. Criterios para la modificación de un certificado 26
4.8.2. Personas habilitadas para la solicitar la modificación de un certificado 27
4.8.3. Procesamiento de la solicitud de modificación de un certificado 27
4.8.4. Notificación al suscriptor sobre la modificación de un certificado 27
4.8.5. Conducta constitutiva de aceptación de modificación de certificados 27
4.8.6. Publicación del certificado modificado por parte de la EC 27
4.9. Cancelación y suspensión de certificados digitales 27
4.9.1. Motivos de cancelación 27
4.9.2. Personas habilitadas para solicitar la cancelación de un certificado 28
4.9.3. Procesamiento de la solicitud de cancelación de un certificado 28
4.9.4. Periodo de gracia de la solicitud de cancelación de un certificado 28
4.9.5. Tiempo dentro del cual se debe procesar una solicitud de cancelación 28
4.9.6. Requisitos para la verificación de cancelación por los terceros que confían 28
4.9.7. Frecuencia de publicación de la Lista de Certificados Cancelados (CRL) 29
4.9.8. Periodo máximo de latencia para las CRL 29
4.9.9. Disponibilidad en línea para verificar la información respecto a la cancelación 29
4.9.10. Necesidad de verificación del estado del certificado mediante OCSP 29
4.9.11. Otras formas de publicar la cancelación 29
4.9.12. Requisitos especiales para el caso de compromiso de llave privada 30
4.9.13. Circunstancias para una suspensión 30
4.9.14. Personas habilitadas para solicitar una suspensión 30

4.9.15. Procedimiento para solicitar una suspensión 30
4.9.16. Límite del periodo de suspensión 30
4.10. Servicios de monitoreo de estado del certificado 30
4.10.1. Características operacionales 30
4.10.2. Disponibilidad del servicio 30
4.10.3. Servicios opcionales 30
4.11. Finalización de la suscripción al servicio de certificación 30
4.12. Custodia y recuperación de llaves 31
4.12.1. Condiciones y procedimientos para custodia y recuperación de llaves privadas 31
4.12.2. Condiciones y procedimientos para custodia y recuperación de llaves de sesión 31
5. CONTROLES NO TECNICOS DE SEGURIDAD 32
5.1. Controles físicos 32
5.1.1. Ubicación y construcción del local 32
5.1.2. Acceso físico 32
5.1.3. Energía y aire acondicionado 32
5.1.4. Exposición al agua 33
5.1.5. Previsión y protección contra fuego 33
5.1.6. Almacenamiento de material 33
5.1.7. Eliminación de residuos 33
5.1.8. Copia de seguridad externa 33
5.2. Controles procedimentales 33
5.2.1. Roles de confianza 33
5.2.2. Número de personas requeridas por labor 34
5.2.3. Identificación y autenticación para cada rol 34
5.2.4. Roles que requieren separación de funciones 34
5.3. Controles de personal 34
5.3.1. Requisitos de experiencia, capacidades y autorización 34
5.3.2. Procedimiento para verificación de antecedentes 34
5.3.3. Requisitos de capacitación 35
5.3.4. Requisitos y frecuencia de re-capacitación 35
5.3.5. Frecuencia y secuencia de rotación de las funciones 35
5.3.6. Sanciones por acciones no autorizadas 35
5.3.7. Requisitos para contratistas 36
5.3.8. Documentación suministrada al personal 36

5.4. Procedimientos de registro de eventos 36
5.4.1. Tipos de eventos registrados 36
5.4.2. Frecuencia de procesamiento del registro de eventos 37
5.4.3. Periodo de conservación del registro de eventos 37
5.4.4. Protección del registro de eventos 37
5.4.5. Procedimiento de copia de respaldo del registro de eventos 37
5.4.6. Sistema de realización de auditoría (Interna vs. Externa) 37
5.4.7. Notificación al sujeto que causa el evento 37
5.4.8. Evaluación de la vulnerabilidad 37
5.5. Archivo 38
5.5.1. Tipos de información archivada 38
5.5.2. Periodo de conservación del archivo 38
5.5.3. Protección del archivo 38
5.5.4. Procedimientos para copia de seguridad del archivo 38
5.5.5. Requisitos de fecha y hora de los registros 38
5.5.6. Sistema de archivo (interno vs. externo) 38
5.5.7. Procedimientos para obtener y verificar la información archivada 38
5.6. Cambio de llaves 39
5.7. Recuperación frente al compromiso y desastre 39
5.7.1. Procedimiento para el manejo de incidentes y compromiso 39
5.7.2. Corrupción de los datos, software y/o recursos computacionales 39
5.7.3. Procedimiento en caso de compromiso de llave privada 39
5.7.4. Capacidad de continuidad de las operaciones luego de un desastre 40
5.8. Terminación de la ECEP-RENIEC 40
6. CONTROLES TÉCNICOS DE SEGURIDAD 41
6.1. Generación e instalación del par de llaves 41
6.1.1. Generación del par de llaves 41
6.1.2. Entrega de la llave privada al suscriptor 41
6.1.3. Entrega de la llave pública al emisor del certificado digital 42
6.1.4. Entrega de la llave pública al tercero que confía 42
6.1.5. Tamaño de llaves 42
6.1.6. Parámetros de generación de llave pública y verificación de calidad 42
6.1.7. Propósito de uso de la llave (extensión *KeyUsage* X.509 v3) 43

6.2. Controles de ingeniería para protección de la llave privada y módulo criptográfico 43
6.2.1. Estándares y controles para el módulo criptográfico 43
6.2.2. Control multipersonal (k de m) de la llave privada 43
6.2.3. Custodia de la llave privada 43
6.2.4. Respaldo de la llave privada 43
6.2.5. Archivo de la llave privada 44
6.2.6. Transferencia de la llave privada hacia o desde un módulo criptográfico 44
6.2.7. Almacenamiento de la llave privada en un módulo criptográfico 44
6.2.8. Método de activación de la llave privada 44
6.2.9. Método de desactivación de la llave privada 44
6.2.10. Método de destrucción de la llave privada 45
6.2.11. Clasificación del módulo criptográfico 45
6.3. Otros aspectos de la gestión del par de llaves 45
6.3.1. Archivo de la llave pública 45
6.3.2. Periodo operacional del par de llaves y periodo de uso de llaves 45
6.4. Datos de activación 46
6.4.1. Generación e instalación de los datos de activación 46
6.4.2. Protección de los datos de activación 46
6.4.3. Otros aspectos de los datos de activación 46
6.5. Controles de seguridad computacional 46
6.5.1. Requisitos técnicos específicos de seguridad computacional 46
6.5.2. Evaluación de la seguridad computacional 46
6.6. Controles técnicos del ciclo de vida 47
6.6.1. Controles para el desarrollo de sistemas 47
6.6.2. Controles de gestión de seguridad 47
6.6.3. Controles de seguridad del ciclo de vida 47
6.7. Controles de seguridad de red 47
6.8. Fecha y Hora 48
7. PERFILES DE CERTIFICADOS, CRL y OCSP 49
7.1. Perfil de los certificados 49
7.1.1. Versión de certificados digitales 49
7.1.2. Extensiones de certificados digitales 49
7.1.3. Identificador de objeto de certificados digitales 51

7.1.4. Sintaxis y semántica de los calificadores de la política 51
7.1.5. Procesamiento de semantica para la extensión crítica de politicas de certificados51
7.2. Perfil de la CRL 51
7.2.1. Números de versión 51
7.2.2. CRL y extensiones de entrada CRL 51
7.3. Perfil de OCSP 52
7.3.1. Números de versión 52
7.3.2. Extensiones OCSP 52
8. AUDITORÍAS DE CONFORMIDAD Y OTRAS EVALUACIONES 53
8.1. Frecuencia y circunstancias de evaluación 53
8.2. Identidad/Calificaciones de auditores 53
8.3. Relación del auditor con la entidad auditada 53
8.4. Elementos cubiertos por la evaluación 53
8.5. Acciones a ser tomadas frente a deficiencias 53
8.6. Publicación de resultados 53
9. OTRAS MATERIAS DE NEGOCIO Y LEGALES 54
9.1. Tarifas 54
9.1.1. Tarifas para la emisión o renovación de certificados 54
9.1.2. Tarifas de acceso a certificados 54
9.1.3. Tarifas para información sobre cancelación o estado 54
9.1.4. Tarifas para otros servicios 54
9.1.5. Políticas de reembolso 54
9.2. Responsabilidad Financiera 54
9.2.1. Cobertura de seguro 54
9.2.2. Otros activos 55
9.2.3. Cobertura de seguro o garantía para entidades finales 55
9.3. Confidencialidad de información del negocio 55
9.3.1. Alcances de la información confidencial 55
9.3.2. Información no contenida dentro del rubro de información confidencial 55
9.3.3. Responsabilidad de protección de la información confidencial 56
9.4. Privacidad de la información personal 56
9.4.1. Plan de privacidad 56
9.4.2. Información tratada como privada 56
9.4.3. Información no considerada privada 57

9.4.4. Responsabilidad de protección de la información privada 57
9.4.5. Notificación y consentimiento para el uso de información 57
9.4.6. Divulgación con motivo de un proceso judicial o administrativo 58
9.4.7. Otras circunstancias para divulgación de información 58
9.5. Derechos de propiedad intelectual 58
9.6. Representaciones y garantías 58
9.6.1. Representaciones y garantías de la EC 58
9.6.2. Representaciones y garantías de la ER 59
9.6.3. Representaciones y garantías de los suscriptores 59
9.6.4. Representaciones y garantías de los terceros que confían 60
9.6.5. Representaciones y garantías de otros participantes 61
9.7. Exención de garantías 61
9.8. Limitaciones a la responsabilidad 61
9.9. Indemnizaciones 61
9.10. Término y terminación 61
9.10.1. Término 61
9.10.2. Terminación 62
9.10.3. Efecto de terminación y supervivencia 62
9.11. Notificaciones y comunicaciones individuales con los participantes 62
9.12. Enmendaduras 62
9.12.1. Procedimiento para enmendaduras 62
9.12.2. Mecanismos y periodos de notificación 62
9.12.3. Circunstancias bajo las cuales debe ser cambiado el OID 62
9.13. Procedimiento sobre resolución de disputas 63
9.14. Ley aplicable 63
9.15. Conformidad con la ley aplicable 63
9.16. Cláusulas misceláneas 63
9.16.1. Acuerdo Íntegro 63
9.16.2. Subrogación 64
9.16.3. Divisibilidad 64
9.16.4. Ejecución (tarifas de abogados y cláusulas de derechos) 64
9.16.5. Fuerza Mayor 64
9.17. Otras cláusulas 64
Anexo 1 - Definiciones, abreviaturas y acrónimos 65

Anexo 2 – Perfiles de Certificado Digital de la ECEP-RENIEC 78

1. INTRODUCCIÓN

1.1. Visión general

El RENIEC se ha acreditado ante la Autoridad Administrativa Competente (en adelante AAC) de la Infraestructura Oficial de Firma Electrónica (en adelante IOFE) como ECEP. La ECEP del RENIEC (en adelante ECEP-RENIEC) opera como una entidad de certificación subordinada a la jerarquía PKI denominada "ECERNEP PERU CA Root 3" bajo el nivel de seguridad establecido como "medio" en la Guía de Acreditación de Entidades de Certificación EC. Una ilustración de la jerarquía "ECERNEP PERU CA Root 3" se presenta en la siguiente figura:

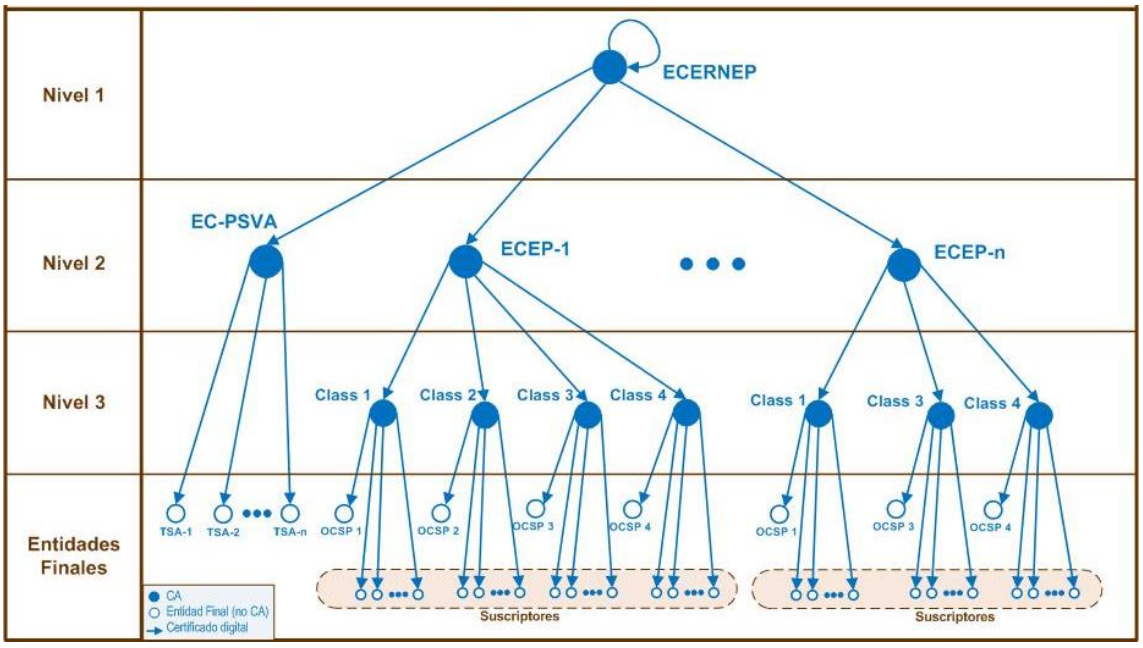

Figura 1: Diagrama de la jerarquía ECERNEP PERÚ CA ROOT 3

El presente documento denominado Declaración de Prácticas de Certificación (en adelante CPS) establece de qué manera la ECEP-RENIEC implementa los procedimientos y controles para cumplir con los requerimientos establecidos en la Política General de Certificación (CP) Versión 4.0, identificada con el código OID 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000, de la jerarquía PKI "ECERNEP PERU CA Root 3".

1.2. Nombre e identificación del documento

- **Nombre:** Declaración de Prácticas de Certificación de la ECEP-RENIEC
- **Versión:** 3.2
- **OID:** 1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0
- **Website:** http://www.reniec.gob.pe/repository/
- **Fecha de elaboración:** 18/05/2017
- **Fecha de última modificación:** 24/01/2023
- **Lugar:** Lima, Perú

1.3. Participantes

La comunidad de usuarios, está formada por personas naturales y jurídicas del Estado Peruano que obtienen y utilizan certificados digitales emitidos.

1.3.1. Entidad de Certificación Nacional para el Estado Peruano (ECERNEP)[1]

La ECERNEP es la encargada de administrar el certificado digital raíz, denominado "ECERNEP PERÚ CA ROOT 3". Asimismo, tiene como función emitir y cancelar o revocar los certificados digitales destinados a PSCs subordinados. El certificado digital raíz de la ECERNEP es autofirmado y es el inicio de la cadena de confianza de todos los participantes de la jerarquía.

Asimismo, la ECERNEP administra el certificado digital denominado EC-PSVA, que ha sido emitido subordinado a la ECERNEP y es utilizado para emitir certificados digitales para las Entidades Públicas acreditadas ante la AAC como PSVA en la modalidad de Autoridad de Sellado de Tiempo (TSA).

1.3.2. Entidades de Certificación para el Estado Peruano (ECEP)

Las ECEP son Entidades de Certificación subordinadas a la ECERNEP que han sido acreditadas por la AAC y tienen como función principal gestionar el ciclo de vida de los certificados digitales de Entidades Finales.

La ECEP-RENIEC, en su rol de Prestador de Servicios de Certificación, cuenta con un certificado digital de Nivel 2 emitido por la ECERNEP que opera en modo *offline* y cuatro (04) certificados digitales de Nivel 3 (también llamados Clases), que operan en modo *online*, los que en su conjunto posibilitan la emisión de los certificados digitales a entidades finales (titulares y suscriptores).

Clase	Descripción
Class 1	Certificados digitales para usos específicos
Class 2	Certificados digitales para Ciudadanos (contenidos en el DNI electrónico)
Class 3	Certificados digitales para Trabajadores de la Administración Pública
Class 4	Certificados digitales para Sistemas de Información

Tabla 1: Certificados digitales de nivel 3 de la ECEP-RENIEC

1.3.3. Entidades de Registro o Verificación para el Estado Peruano (EREP)

La función principal de una EREP es la verificación de la identidad de los solicitantes que realizan solicitudes de emisión y cancelación (o cualquier otro servicio que brinde la ECEP asociada) de certificados digitales. La EREP debe realizar el levantamiento de datos y la comprobación de la información brindada por el solicitante. Asimismo, debe aprobar o rechazar la emisión o cancelación de certificados digitales, comunicando a la respectiva Entidad de Certificación con la que se encuentra asociada, de acuerdo a lo estipulado en su correspondiente Declaración de Prácticas de Registro (en adelante RPS).

La ECEP-RENIEC opera en asociación con las siguientes entidades de Registro:

[1] Por Decreto Supremo Nº 029-2021-PCM el RENIEC transfiere la ECERNEP a la Presidencia del Consejo de Ministros a través de la ex SEGDI, hoy Secretaría de Gobierno y Transformación Digital - SGTD. A su vez, mediante Decreto Supremo Nº 156-2022-PCM del 30 de diciembre de 2022 se modifica la Octava Disposición Complementaria Final del Reglamento de la Ley de firmas y Certificados Digitales ampliando el plazo por el que dicha entidad puede prestar sus servicios como ECERNEP sin encontrarse acreditada ante el INDECOPI.

- EREP-RENIEC, acreditada para emitir certificados digitales de persona natural a los ciudadanos peruanos (contenidos en dispositivos móviles bajo la Class 1 y en el DNIe bajo la Class 2) y para emitir certificados digitales de persona jurídica, tanto a los trabajadores de la Administración Pública bajo la Class 3 como a los sistemas de información de la Administración Pública bajo la Class 4 (certificados de agente automatizado).

1.3.4. Entidades Prestadoras de Servicios de Valor Añadido (PSVA)

Una entidad prestadora de servicios de valor añadido es aquella que brinda servicios bajo cualquiera de las siguientes modalidades:

- Sistema de Intermediación Digital (SID)
- Sistema de creación de firma remota
- Autoridad de Sellado de Tiempo (TSA)
- Sistema de preservación digital

Las entidades PSVA deben acreditarse ante la AAC y deben desarrollar su correspondiente Declaración de Prácticas. El RENIEC opera en la actualidad como Prestador de Servicios de Valor Añadido bajo la modalidad de autoridad de sellado de tiempo.

1.3.5. Titulares y suscriptores

Las Entidades Finales pueden ser personas naturales o personas jurídicas. Las personas naturales se constituyen siempre en titulares y suscriptores del certificado digital, mientras que las personas jurídicas, dependiendo del tipo de certificado digital, se constituyen en titular o en titular y suscriptor.

1.3.6. Terceros que confían

Los terceros que confían pueden ser personas naturales, jurídicas, equipos, servicios o cualquier otro ente diferente al suscriptor que decide aceptar y confiar en un certificado digital emitido por la ECEP-RENIEC y, por lo tanto, en las firmas digitales y mensajes cifrados correspondientes.

1.3.7. Otros participantes

Se considera como otros participantes a aquellas entidades que proveen servicios de soporte a las operaciones del proceso de certificación digital. En la eventualidad que la ECEP-RENIEC requiera la tercerización de algún servicio debe suscribirse un acuerdo de tercerización que cuente con las cláusulas específicas relacionadas con la seguridad de la información y la protección de los datos personales de acuerdo a la normativa y legislación del Estado Peruano.

1.4. Uso de un certificado digital

1.4.1. Usos apropiados de los certificados digitales

Los certificados digitales de la ECEP-RENIEC son utilizados para:

- De Nivel 2 (ECEP-RENIEC *offline*): usados exclusivamente para la emisión de certificados digitales de Nivel 3.

- De Nivel 3 (Classes de la ECEP-RENIEC): usados exclusivamente para la emisión de certificados digitales de entidad final a titulares y suscriptores.
- Firmar las listas de certificados revocados (CRL) que corresponden a cada nivel, tal como se indica en el numeral 4.9.7 Frecuencia de publicación de la Lista de Certificados Cancelados (CRL).

Los certificados de Entidad Final, emitidos por la ECEP-RENIEC, podrán ser utilizados únicamente para los propósitos indicados en las extensiones *keyUsage (KU) y extendedKeyUsage (EKU)*, según lo indicado en el numeral **7.1.1 Certificado Digital de Entidad Final.**

1.4.2. Usos prohibidos del certificado

Los certificados de la ECEP-RENIEC y los emitidos por ella (certificados de Entidad Final), no pueden ser utilizados en situaciones diferentes a las descritas en el numeral **1.4.1 Usos apropiados de los certificados digitales** del presente documento, de acuerdo a lo señalado en el RFC 3647.

1.5. Administración de la CPS

1.5.1. Organización que administra el documento

La organización encargada de la administración (elaboración, registro, mantenimiento y actualización) de este documento es:

- **Nombre:** Registro Nacional de Identificación y Estado Civil - RENIEC.
- **Dirección de correo:** identidaddigital@reniec.gob.pe
- **Dirección:** Jr. Bolivia 109, Centro Cívico - Cercado de Lima.
- **Número de teléfono:** 01-3152700

1.5.2. Persona de contacto

- **Contacto:** Sub Director de Servicios de Certificación Digital.
- **Dirección de correo electrónico:** identidaddigital@reniec.gob.pe
- **Dirección:** Jr. Bolivia 109, Centro Cívico, Cercado de Lima
- **Número de teléfono:** 01-3152700

1.5.3. Persona que determina la conformidad de la CPS con la CP

Según lo dispuesto en el Reglamento de la Ley de Firmas y Certificados Digitales, la AAC es la responsable de revisar la presente Declaración de Prácticas de Certificación y verificar que cumple con la normativa vigente.

1.5.4. Procedimiento de aprobación de la CPS

El presente documento en su versión primera, así como sus modificaciones son propuestos por la ECEP-RENIEC a la AAC, a quien corresponde su aprobación mediante sus procedimientos, según lo dispuesto en el Reglamento de la Ley de Firmas y Certificados Digitales.

1.6. Definiciones, abreviaturas y acrónimos

Ver Anexo 1.

2. RESPONSABILIDADES DEL REPOSITORIO Y SU PUBLICACIÓN

2.1. Repositorios

La ECEP-RENIEC gestiona repositorios, accesibles desde Internet, con la siguiente información:

- Directorio de certificados digitales de ECEP *offline* (Nivel 2) y ECEP *online* (Nivel 3).
- Lista de Certificados Cancelados (CRL) Nivel 2 y Nivel 3, según lo indicado en el numeral 4.9.7 Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)
- Declaración de Prácticas de Certificación (CPS) de la ECEP-RENIEC, que también se encuentra indicada en la extensión *"CertificatePolicy"* de cada certificado digital de entidad final[2].
- Política y Plan de Privacidad
- Políticas de Seguridad

Estos repositorios se encuentran accesibles en la Web, específicamente en:

- http://www.reniec.gob.pe/repository/
- http://www.reniec.gob.pe/crt/
- https://pki.reniec.gob.pe/repositorio/
- http://crl.reniec.gob.pe/

Cabe resaltar que la ECEP-RENIEC no publica los certificados digitales de entidad final emitidos, a excepción de los correspondientes a la PSVA-TSA-RENIEC.

2.2. Actualización

La ECEP-RENIEC actualiza la información de sus repositorios cuando corresponda, en función a la frecuencia establecida en el numeral 2.3 **Frecuencia de publicación**. Asimismo, los mantiene una disponibilidad mínima de 99% anual, con un tiempo programado de inactividad máximo de 0.5% anual.

2.3. Frecuencia de publicación

La ECEP-RENIEC gestiona y actualiza sus repositorios conforme a la siguiente frecuencia:

- Directorio de certificados digitales de ECEP *offline* (Nivel 1), ECEP *offline* (Nivel 2) y ECEP *online* (Nivel 3): Actualizado cada vez que se emite un nuevo certificado digital de cualquiera de los dos niveles mencionados.
- Listas de certificados digitales cancelados: Actualizado con la emisión de una nueva CRL, según lo indicado en el numeral 4.9.7 del presente documento.
- Repositorio de la Declaración de Prácticas de Certificación (CPS) de la ECEP-RENIEC: Actualizado cada vez que la AAC aprueba una nueva versión.
- Políticas de Privacidad: Actualizado cada vez que la AAC aprueba una nueva versión.
- Políticas de Seguridad: Actualizado cada vez que la AAC aprueba una nueva versión.

[2] Cfr. la sección 6.1.d) de ETSI EN 319 411-1.

2.4. Control de acceso a los repositorios

La ECEP-RENIEC no limita el acceso de lectura a la información en sus repositorios, pero establece controles físicos y lógicos para impedir que de forma no autorizada se puedan añadir, modificar o borrar registros del Repositorio, de modo tal que:

- Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad e integridad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

Los repositorios de la ECEP-RENIEC son administrados, publicados y gestionados por la propia organización.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Convención de nombres

3.1.1. Tipos de nombres

La estructura *DistinguishedName* (ITU-T X.501) en los campos *IssuerDN* y *SubjectDN* es utilizado por la ECEP-RENIEC para identificar de forma única y plena a los titulares de los certificados digitales.
Asi mismo se tiene configurada la opción "Enforce unique SubjectDN" en el Software de Gestion de Certificados Digitales para que los SubjectDN de entidad final (titular y suscriptor) no se repitan.

3.1.2. Necesidad de nombres significativos

El campo *SubjectDN* de los certificados digitales administrados por la ECEP-RENIEC (Nivel 1 y Nivel 2) es significativo en la medida que registra el nombre oficial de la Entidad emisora (Registro Nacional de Identificación y Estado Civil). Los certificados digitales Nivel 3, por su parte, que registran un nombre único definido para cada una de las clases y el nombre del RENIEC.

En los certificados digitales emitidos por la ECEP-RENIEC a entidades finales, el campo *SubjectDN* contiene los datos del suscriptor (nombre completo, número de documento de identidad, nombre de la entidad a la que pertenece), según corresponda a cada Clase.

En el caso de certificados emitidos a sistemas de información y no a personas naturales (Class 4), la ECEP-RENIEC verifica la unicidad de los nombres designados a estos.

3.1.3. Anonimato o seudónimo de los suscriptores

La ECEP-RENIEC no emite ningún certificado digital anónimo; pero sí se permite el uso de seudónimos, únicamente para el caso de certificados emitidos a Agentes Automatizados.

3.1.4. Reglas de interpretación de diferentes modalidades de nombres

El certificado digital de Nivel 2 de la ECEP-RENIEC utiliza el siguiente *SubjectDN:*:

	Atributo	Valor
Subject Distinguished Name	**CN**	ECEP-RENIEC
	SN	--[3]
	GIVENNAME	--
	O	Registro Nacional de Identificación y Estado Civil
	OU	--
	ST	--
	L	--
	C	PE
	SERIALNUMBER	--
SubjectAltName		--

Tabla 2: Valor de los campos del SubjectDN del certificado digital de la ECEP-RENIEC offline

[3] Para la tabla 2, 3 y 4, el símbolo "--" indica que el valor para el SubjectDN no es requerido al momento de firmar las CA por la Sub CA inmediata.

Los certificados digitales de Nivel 3 de la ECEP-RENIEC CA Class {1,2,3,4} utilizan el siguiente *SubjectDN*:

	Atributo	Valor
Subject Distinguished Name	**CN**	ECEP-RENIEC CA Class {1,2,3,4}
	SN	--
	GIVENNAME	--
	O	Registro Nacional de Identificación y Estado Civil
	OU	--
	ST	--
	L	--
	C	PE
	SERIALNUMBER	--
SubjectAltName		--

Tabla 3 – Valor de los campos de los *SubjectDN* de los certificados digitales de nivel 3 de la ECEP-RENIEC CA Class {1,2,3,4} *online*

Los certificados digitales Nivel 3 de segunda generación de la ECEP-RENIEC CA Class {1,2} II utilizan el siguiente *SubjectDN*:

	Atributo	Valor
Subject Distinguished Name	**CN**	ECEP-RENIEC CA Class {1,2} II
	SN	--
	GIVENNAME	--
	O	Registro Nacional de Identificación y Estado Civil
	OU	--
	ST	--
	L	--
	C	PE
	SERIALNUMBER	--
SubjectAltName		--

Tabla 4 – Valor de los campos de los *SubjectDN* de los certificados digitales de nivel 3 de segunda generación de la ECEP-RENIEC CA Class {1, 2} II online

El valor del campo IssuerDN de los certificados Nivel 3 de la ECEP-RENIEC es igual al SubjectDN del certificado digital Nivel 2, que se muestra en la Tabla 3.

Por su parte, los campos del *SubjectDN, **IssuerDN*** y la extensión ***SubjectAltName*** de cada tipo de certificado digital de Entidad Final, se encuentran descritos en el Anexo 2.

3.1.5. Unicidad de Nombres

La ECEP-RENIEC garantiza que el *SubjectDN* de los certificados digitales que emite es único no sólo durante el periodo de vigencia del certificado, sino durante la entera existencia de la jerarquía de certificación digital.

Las EREP asociadas a la ECEP-RENIEC establecen en su RPS la forma en que se evita la reasignación de un mismo nombre a entidades o certificados diferentes. Las EREP asociadas

a la ECEP-RENIEC deben rechazar las solicitudes de certificados cuando se evidencie el conflicto de nombres.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

No aplica

3.2. Validación inicial de la identidad

3.2.1. Método para probar posesión de la llave privada

La ECEP-RENIEC genera y administra sus propias llaves para los certificados de Nivel 2 y Nivel 3.

Las Entidades Finales solicitantes de un certificado digital que generen sus propias llaves utilizando módulos criptográficos que cumplen los requisitos descritos en el numeral **6.2.11 Clasificación del módulo criptográfico** demuestran la posesión de su llave privada mediante el envío de un *Certificate Signing Request* en formato PKCS#10.

Sin embargo, no se requiere una prueba de posesión en el caso donde la generación de llaves de Entidades Finales se encuentre bajo el control directo de la ECEP-RENIEC o una EREP asociada.

3.2.2. Autenticación de identidad de personas jurídicas

El RENIEC como entidad de la Administración Pública que administra a la ECEP-RENIEC se identifica por su razón social y su número de RUC. Además, se encuentra comprendida dentro de las entidades referidas en el Artículo I del Título Preliminar de la Ley 27444 – Ley del Procedimiento Administrativo General, consideradas hábiles para que se les emita certificados digitales de ECEP por parte de la ECERNEP, previa acreditación ante la AAC.

- Nombre de la entidad: Registro Nacional de Identificación y Estado Civil
- Siglas: RENIEC
- RUC: 20295613620

Las EREP asociadas a la ECEP-RENIEC incluyen en su RPS los procedimientos de autenticación de la identidad de personas jurídicas según lo indicado en el numeral **3.2.1, Método para probar posesión de la llave privada,** y en el presente numeral.

3.2.3. Autenticación de identidad de personas naturales

Para la emisión de certificados digitales de Entidad Final a personas naturales, la EREP correspondiente, asociada a la ECEP-RENIEC, realiza la verificación de identidad del solicitante usando el Registro Único de Identificación de Personas Naturales del RENIEC y mediante la comprobación de su Documento Nacional de Identidad vigente. Para incrementar la seguridad en el procedimiento de verificación se hace uso de los servicios biométricos del RENIEC.

En el caso de tratarse de solicitantes extranjeros, las EREP asociadas a la ECEP-RENIEC realizan la verificación con carné de extranjería y el registro oficial de extranjeros.

3.2.4. Información no verificada del suscriptor

Toda la información contenida en un certificado digital de Entidad Final es verificada por las EREP durante el proceso de autenticación de la identidad.

3.2.5. Validación de autoridad para efectuar la solicitud

Las EREP asociadas a la ECEP-RENIEC verifican la autoridad que posee el solicitante para requerir un tipo o clase específico de certificado digital para Entidad Final conforme se establece en sus RPS.

3.2.6. Criterios de interoperabilidad

La interoperabilidad de los certificados digitales emitidos por la ECEP-RENIEC es obtenida debido a que se cumple con el estándar X509v3 de acuerdo a lo indicado en el **numeral 7.1 Perfil de los certificados.**

3.3. Identificación y autenticación para solicitudes de reemisión con renovación de llaves

Este servicio no es brindado por la ECEP-RENIEC.

3.3.1. Solicitudes rutinarias de renovación de llaves
No aplica.

3.3.2. Renovación de llaves luego de la cancelación
No aplica.

3.4. Identificación y autenticación para solicitudes de cancelación

Las EREP acreditadas asociadas a la ECEP-RENIEC verifican y procesan las solicitudes de cancelación de los certificados digitales de Entidad Final emitidos por ésta, conforme se precisa en sus RPS u otros documentos.

En el caso que la ECEP-RENIEC requiera cancelar sus certificados *online*, procederá a cancelarlos directamente y dejará constancia del hecho en un acta. En el caso que la ECEP-RENIEC requiera cancelar su certificado *offline*, efectuará la solicitud a la ECERNEP.

4. CICLO DE VIDA DEL CERTIFICADO DIGITAL: REQUISITOS OPERACIONALES

4.1. Solicitud de certificado digital

4.1.1. Personas habilitadas para presentar una solicitud de certificado

La ECEP-RENIEC solicita la emisión o cancelación de sus certificados de Nivel 2 como PSC a la ECERNEP únicamente a través de su representante legal o apoderado.

La solicitud de certificados digitales de Entidad Final (titulares y suscriptores) que emite la ECEP-RENIEC se realiza a través de las EREP asociadas conforme se encuentra establecido en sus RPS.

4.1.2. Proceso de registro de solicitud y responsabilidades

Es atribución de las EREP asociadas a la ECEP-RENIEC solicitar los documentos y datos necesarios para identificar al solicitante del certificado digital de Entidad Final, conforme se establece en sus RPS.

La ECEP-RENIEC informa a los suscriptores y titulares sobre los términos y limitaciones aplicables a los certificados digitales que emite y sobre las obligaciones que deben cumplir de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas empleando los mismos. La entrega de dicha información es asumida por las EREP, como parte de su asociación con la ECEP-RENIEC.

4.2. Procesamiento de la solicitud de certificado

4.2.1. Identificación y autenticación

Las EREP asociadas a la ECEP-RENIEC realizan la identificación y autenticación al solicitante de certificados de Entidad Final, conforme se encuentra descrito en sus RPS y, con lo establecido en los numerales **3.2.2 Autenticación de identidad de personas jurídicas** y **3.2.3 Autenticación de identidad de personas naturales**.

4.2.2. Aprobación o rechazo de las solicitudes de certificado

Las EREP asociadas tienen la potestad y obligación de rechazar las solicitudes de los certificados digitales que emite la ECEP-RENIEC en los siguientes casos.

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles
- Si el resultado de la verificación de identidad del titular o suscriptor fue negativo
- Si el representante legal de la persona jurídica no cuenta con un poder vigente
- Si la solicitud de firma de certificado (CSR) no es compatible con PKCS#10 o los datos consignados no son correctos.
- Si la longitud de la llave es menor a 2048 bits.

Las EREP asociadas deben comunicar a la ECEP-RENIEC la aprobación de la solicitud para la emisión del certificado digital debiendo contar previamente con los contratos firmados por los solicitantes donde constan las responsabilidades de la EREP, de la ECEP-RENIEC, de los suscriptores y de los titulares de los certificados. Los contratos cumplen con los contenidos indicados en la CP de la ECERNEP.

4.2.3. Tiempo límite para el procesamiento de las solicitudes

La ECEP-RENIEC procesa la solicitud de emisión del certificado digital de Entidad Final (titulares y suscriptores) dentro de un periodo no mayor a un (01) día.

4.3. Emisión del certificado

4.3.1. Acciones durante la emisión del certificado

La emisión de certificados de la ECEP-RENIEC de Nivel 2 y Nivel 3 se realiza en una ceremonia de llaves, utilizando un módulo criptográfico con las características indicadas en el numeral **6.1.1 Generación del par de llaves**

La ECEP-RENIEC emitirá un certificado digital siempre que reciba una petición (CSR) válida en formato PKCS#10 según lo indicado en el numeral **4.1, Solicitud de certificado digital** y se asegure que el par de llaves se haya generado de manera correcta y que la llave pública guarde relación con la llave privada.

4.3.2. Notificación al suscriptor respecto a la emisión de un certificado

La notificación al suscriptor es responsabilidad de la EREP a través de medios telemáticos.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de aceptación del certificado

La firma del contrato aludido en el numeral **4.2.2 Aprobación o rechazo de las solicitudes de certificado**, por parte de los solicitantes o el empleo que se haga del certificado digital constituyen tácitamente la aceptación del certificado digital emitido por la ECEP-RENIEC.

4.4.2. Publicación del certificado por parte de la ECEP

Los certificados digitales de la ECEP *offline* Nivel 2 y ECEP *online* Nivel 3 son publicados por la ECEP-RENIEC en su repositorio de certificados emitidos, de acuerdo a lo indicado en el numeral **2. RESPONSABILIDADES DEL REPOSITORIO Y SU PUBLICACIÓN.** La ECEP-RENIEC no publica los certificados digitales de entidad final emitidos.

4.4.3. Notificación de la EC a otras entidades sobre la emisión de un certificado

La ECEP-RENIEC no informa a terceros sobre los certificados digitales de entidad final que emite. Sin embargo, actualiza el repositorio correspondiente cada vez que se emite un nuevo certificado de la ECEP *offline* Nivel 2 y/o ECEP *online* Nivel 3, de acuerdo a lo indicado en el numeral **2. RESPONSABILIDADES DEL REPOSITORIO Y SU PUBLICACIÓN.**

4.5. Uso del par de llaves y del certificado

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

El uso de la llave privada, correspondiente a la llave pública del certificado digital, está permitido luego de que el suscriptor haya aceptado los términos y condiciones establecidos

en los contratos aludido en el numeral **4.2.2 Aprobación o rechazo de las solicitudes de certificado**.

La ECEP-RENIEC requiere del suscriptor y titular, lo siguiente:

- Emplear el certificado de acuerdo con lo establecido en la CPS de la ECEP-RENIEC y en el contrato del suscriptor.
- Ser razonablemente diligente en la custodia de su llave privada, con el fin de evitar usos no autorizados.
- Notificar a la EREP asociada, sin retrasos injustificables los motivos indicados a continuación (la notificación puede realizarse de manera presencial, acercándose a las oficinas de la EREP o mediante medios telemáticos que éstas pongan a disposición):
  - La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su llave privada (computador, token criptográfico o tarjeta inteligente).
  - El compromiso potencial de su llave privada.
  - La pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

4.5.2. Uso de la llave pública y del certificado por el tercero que confía

Los terceros que confían, deben usar la llave pública contenida en los certificados para realizar únicamente las validaciones indicadas en las extensiones *KeyUsage (KU) y ExtendedKeyUsage (EKU)*, tal como se expone en el numeral, **6.1.7 Propósito de uso de la llave (extensión *KeyUsage* X.509 v3) ,** del presente documento.

El tercero que confía está obligado a:

- Utilizar software de validación acreditado dentro de la IOFE, para asegurarse que realice la verificación adecuada de los valores consignados en las extensiones *KeyUsage* y *ExtendedKeyUsage.*
- Denunciar situaciones que supongan el compromiso de la llave privada de un suscriptor.
- No comprometer intencionalmente la seguridad de la jerarquía ECERNEP PERÚ CA Root 3.
- No monitorear, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la ECEP-RENIEC sin su autorización por escrito.
- Denunciar vía identidaddigital@reniec.gob.pe cualquier situación en la que la ECEP-RENIEC deba revocar un certificado, siempre y cuando se tengan pruebas fehacientes del compromiso de la llave privada o de su uso ilegal.

4.6. Renovación del certificado

La ECEP-RENIEC no brinda este servicio.

4.6.1. Circunstancias para la renovación de los certificados
No aplica.

4.6.2. Personas habilitadas para presentar una solicitud de renovación
No aplica.

4.6.3. Procesamiento de solicitudes de renovación
No aplica.

4.6.4. Notificación al suscriptor sobre la emisión de un nuevo certificado
No aplica.

4.6.5. Conducta constitutiva de aceptación de renovación de certificados
No aplica.

4.6.6. Publicación del certificado por parte de la EC
No aplica.

4.6.7. Notificación de la EC a otras entidades sobre la renovación de un certificado
No aplica.

4.7. Reemisión de certificado digital con renovación de llaves

La ECEP-RENIEC no brinda este servicio.

4.7.1. Criterios para la renovación de llaves de un certificado
No aplica.

4.7.2. Solicitantes de renovación de llaves de un certificado
No aplica.

4.7.3. Procesamiento de solicitudes de renovación de llaves de un certificado
No aplica.

4.7.4. Notificación al suscriptor sobre la re-emisión de un nuevo certificado
No aplica.

4.7.5. Conducta constitutiva de aceptación de certificados con renovación de llaves
No aplica.

4.7.6. Publicación del certificado con renovación de llaves
No aplica.

4.7.7. Notificación de la EC a otras entidades sobre la re-emisión de un certificado
No aplica.

4.8. Modificación del certificado

La ECEP-RENIEC no brinda este servicio.

4.8.1. Criterios para la modificación de un certificado

No aplica.

4.8.2. Personas habilitadas para la solicitar la modificación de un certificado
No aplica.

4.8.3. Procesamiento de la solicitud de modificación de un certificado
No aplica.

4.8.4. Notificación al suscriptor sobre la modificación de un certificado
No aplica.

4.8.5. Conducta constitutiva de aceptación de modificación de certificados
No aplica.

4.8.6. Publicación del certificado modificado por parte de la EC
No aplica.

4.9. Cancelación y suspensión de certificados digitales

La cancelación de un certificado digital conlleva la cancelación de todos los certificados digitales subordinados, ya que la validez de dichos certificados no podrá seguir siendo verificada.

4.9.1. Motivos de cancelación
La ECEP-RENIEC cancelará sus certificados de Nivel 2 o Nivel 3, por la ocurrencia de alguno de los siguientes motivos:

- Por exposición, puesta en peligro o uso indebido de la llave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la llave privada.
- Cuando la información contenida en el certificado digital ya no resulte correcta

Así también, la ECEP-RENIEC ejecuta la cancelación de certificados de las Entidades Finales mediando la aprobación de solicitud ante las EREP asociadas o al tomarse conocimiento de la ocurrencia de alguna de los siguientes motivos:

- Por exposición, puesta en peligro o uso indebido de la llave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la llave privada.
- Cancelación de las facultades de representación y/o poderes de sus representantes legales o apoderados (al tratarse de certificados de persona jurídica).
- Cuando la información contenida en el certificado digital ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- A solicitud expresa del suscriptor.

La revocación supone la cancelación de oficio de los certificados de Entidad Final por parte de la ECEP-RENIEC, tal como se indica en el Art. 19º del Reglamento de la Ley de Certificados

Digitales. La ECEP-RENIEC procede a cancelar los certificados de oficio bajo las siguientes circunstancias:

- Cuando el suscriptor incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando se tenga evidencia de cualquiera de los motivos de cancelación descritos líneas arriba

4.9.2. Personas habilitadas para solicitar la cancelación de un certificado

La solicitud de cancelación de certificado de Entidad Final debe presentarse ante las EREP asociadas a la ECEP-RENIEC. De acuerdo a lo estipulado por la Ley, las personas que pueden solicitar la cancelación de un certificado digital son:

- El titular o suscriptor del certificado.
- La ECEP-RENIEC.
- La autoridad administrativa o judicial a través de una resolución que ordene la cancelación del certificado.
- Un tercero que tenga pruebas fehacientes de alguno de los supuestos indicados en los numerales 1 y 2 del artículo 10 de la Ley N° 27269- Ley de Firmas y Certificados Digitales.

4.9.3. Procesamiento de la solicitud de cancelación de un certificado

La ECEP-RENIEC gestiona la cancelación de los certificados digitales de Nivel 2 (ECEP-RENIEC *offline)* y de Nivel 3 (Clases de la ECEP-RENIEC) sin notificación previa a los suscriptores o terceros que confían, pero sí notifica a la AAC mediante un Oficio.

Además, efectúa la cancelación de los certificados digitales de Entidad Final mediante el procesamiento de las solicitudes recibidas de las EREP asociadas bajo las circunstancias y procedimientos especificados en sus RPS, en conformidad con lo establecido en el numeral **4.9 Cancelación y suspensión de certificados digitales**.

La ECEP-RENIEC puede cancelar de oficio los certificados que ha emitido según los motivos indicados en el numeral **4.9.1 Motivos de cancelación**.

La identificación y autenticación del solicitante de la cancelación de los certificados digitales se realiza según lo indicado en la RPS de la EREP acreditada.

4.9.4. Periodo de gracia de la solicitud de cancelación de un certificado

La ECEP-RENIEC realiza la cancelación de certificados sin mediar un periodo de gracia, bastando la aprobación de la solicitud por parte de las EREP asociadas y no siendo necesaria una confirmación del solicitante.

4.9.5. Tiempo dentro del cual se debe procesar una solicitud de cancelación

La solicitud de cancelación es procesada dentro de las 24 horas (01 día calendario) siguientes a la aprobación de la solicitud por parte de las EREP asociadas.

4.9.6. Requisitos para la verificación de cancelación por los terceros que confían

Una vez realizada la cancelación de un certificado digital, la ECEP-RENIEC registra la cancelación en la CRL respectiva, haciendo posible de esta manera que todos los interesados puedan verificar el estado del certificado. La frecuencia de publicación de la CRL se realiza conforme a lo indicado en el numeral **2.3 Frecuencia de publicación**

Adicionalmente, la ECEP-RENIEC dispone de servicios de consulta de estado de certificado en línea *(Online Certificate Status Protocol - OCSP)* únicamente para los certificados digitales de entidad final, donde se reflejan las cancelaciones de manera inmediata.

La integridad y autenticidad de la información de estado del certificado es asegurada mediante la firma digital de la CRL y de la respuesta OCSP por parte de la ECEP-RENIEC.

4.9.7. Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)

La ECEP-RENIEC emite la CRL Nivel 2, donde se listan los certificados cancelados de Nivel 3 (Clases de la ECEP-RENIEC) que fuesen firmados por su certificado EC Nivel 2 con frecuencia de publicación de 6 meses (incluso si ningún certificado ha sido cancelado) o, ante la ocurrencia de una cancelación, dentro del periodo máximo de latencia establecido en el numeral **4.9.8, Periodo máximo de latencia para las CRL.**

La ECEP-RENIEC también emite las CRLs Nivel 3, una por cada Clase de certificados, donde se listan los certificados cancelados de Entidad Final que fuesen firmados por sus certificados de ECs de clases correspondientes con frecuencia de publicación de 24 horas (incluso si ningún certificado ha sido cancelado), dentro del periodo máximo de latencia establecido en el numeral **4.9.8, Periodo máximo de latencia para las CRL.**

4.9.8. Periodo máximo de latencia para las CRL
La latencia máxima de las CRLs administradas por la ECEP-RENIEC se presenta en la siguiente tabla:

CRL	Certificados digitales cancelados	Emisora	Frecuencia de publicación	Máxima Latencia
Nivel 2	Nivel 3	EC Nivel 2	6 meses	24 horas
Nivel 3	Entidad final	ECs de clases	24 horas	1 hora

Tabla 5 – Frecuencia de publicación y máxima latencia de CRLs

4.9.9. Disponibilidad en línea para verificar la información respecto a la cancelación
La ECEP-RENIEC brinda el servicio de verificación en línea de estado de certificados (OCSP) para los certificados de Entidad Final. La ruta de acceso al servicio se encuentra en la extensión *Authority Information Access (AIA)* de los certificados digitales de entidad final.

4.9.10. Necesidad de verificación del estado del certificado mediante OCSP
No es obligatorio realizar la verificación en línea (vía OCSP) del estado del certificado al momento de la generación de la firma digital; los suscriptores pueden utilizar únicamente la CRL de la ECEP-RENIEC. Sin embargo, sí es recomendable que los terceros que confían usen los servicios OCSP para efectuar la verificación de firmas digitales.

4.9.11. Otras formas de publicar la cancelación

No aplica.

4.9.12. Requisitos especiales para el caso de compromiso de llave privada

En caso que una llave privada administrada por la ECEP-RENIEC de las asociadas a los certificados digitales de clases de la ECEP-RENIEC *online* se vea comprometida, se procede a cancelar de inmediato todos los certificados emitidos de la clase correspondiente de acuerdo a la legislación vigente y lo estipulado en el numeral **4.9.1 Motivos de cancelación,** comunicando dicha acción a la AAC, todos los suscriptores, titulares y terceros que confían, en un plazo máximo de 24 horas

4.9.13. Circunstancias para una suspensión

No aplica.

4.9.14. Personas habilitadas para solicitar una suspensión

No aplica.

4.9.15. Procedimiento para solicitar una suspensión

No aplica.

4.9.16. Límite del periodo de suspensión

No aplica

4.10. Servicios de monitoreo de estado del certificado

4.10.1. Características operacionales

La ECEP-RENIEC brinda, de forma irrestricta, el servicio de verificación del estado de los certificados mediante la publicación de la Lista de Certificados Cancelados (CRL) y el servicio de verificación en línea (OCSP), que son firmados digitalmente y cuentan con registro de hora y fecha.

4.10.2. Disponibilidad del servicio

La ECEP-RENIEC brinda los servicios de CRL y OCSP, con un tiempo mínimo de disponibilidad del 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3. Servicios opcionales

No aplica.

4.11. Finalización de la suscripción al servicio de certificación

La ECEP-RENIEC finaliza la suscripción al servicio de certificación de las siguientes formas:

- Al cancelarse los certificados digitales de Nivel 2 (ECEP-RENIEC *offline*) antes de la fecha de expiración.
- Al expirar el certificado digital de Nivel 2 (ECEP-RENIEC *offline*).

En caso el INDECOPI revoque o varíe el estado de acreditación de la ECEP-RENIEC o de alguna de las EREP asociadas, corresponderá a las EREP notificar a sus suscriptores.

Una Entidad Final finaliza la suscripción al servicio de certificación de las siguientes formas:

- Al cancelarse el certificado digital antes de la fecha de expiración.
- Al expirar el certificado digital.

4.12. Custodia y recuperación de llaves

4.12.1. Condiciones y procedimientos para custodia y recuperación de llaves privadas

La ECEP-RENIEC almacena las llaves privadas de su certificado digital de Nivel 1 *(offline)*, de sus certificados digitales de Nivel 2 *(offline)* y de sus certificados digitales de Nivel 3 *(online)* en módulos criptográficos que cumplen con lo indicado en el numeral **6.2.11 Clasificación del módulo criptográfico.**

4.12.2. Condiciones y procedimientos para custodia y recuperación de llaves de sesión

No aplica.

5. CONTROLES NO TECNICOS DE SEGURIDAD

La ECEP-RENIEC mantiene controles de seguridad físicos para impedir y prevenir el acceso a personas no autorizadas a sus instalaciones mediante la aplicación de controles según los estándares NTP-ISO/IEC 27001 (ISO/IEC 27001) y NTP-ISO/IEC 17799 (ISO/IEC 27002).

5.1. Controles físicos

5.1.1. Ubicación y construcción del local

Las instalaciones de la ECEP-RENIEC cuentan con las siguientes características físicas:

- Perímetro cerrado, puerta sólida, piso y techo de concreto,
- Personal de seguridad que sólo permite el ingreso a personas autorizadas.
- Zonas de alta seguridad con activos críticos restringidas con acceso biométrico
- Medidas de prevención ante desastres naturales (, por ejemplo, terremotos) y ante desastres accidentales creados por el hombre (aniego, incendios, explosiones, disturbios civiles).
- Ambientes separados para:
    - Área Operacional: Contiene los equipos y servidores computacionales necesarios para la operación de la ECEP-RENIEC *online*, gestión de certificados de entidad final, repositorios y servicios de verificación de estado de certificado.
    - Área Restringida: Contiene la información confidencial y crítica con acceso solamente al personal autorizado mediante verificación biométrica doble (dos personas). En esta área se resguardan los módulos criptográficos que contienen las llaves privadas de la ECEP-RENIEC *offline*.

5.1.2. Acceso físico

Las instalaciones de la ECEP-RENIEC se encuentran protegidas a través de procedimientos que permiten el ingreso solamente a personal autorizado mediante verificación biométrica. Asimismo, cuenta con video vigilancia 24 horas al día, 7 días a la semana (24x7).

Solamente se permite el ingreso a personal ajeno a las instalaciones de la ECEP-RENIEC en casos de auditoría, soporte, mantenimiento o para su limpieza. El visitante pasa por un proceso de verificación de identidad mediante su documento oficial de identidad o fotocheck de la entidad a la que pertenece. Luego, ingresa escoltado por personal de la ECEP-RENIEC y se registra la fecha, hora y motivo de visita.

En condiciones normales, las áreas restringida y operacional se encuentran desocupadas, es decir, sin personal.

5.1.3. Energía y aire acondicionado

Las instalaciones de la ECEP-RENIEC cuentan con sistemas de energía eléctrica de respaldo para asegurar la continuidad del fluido eléctrico. Además, se cuenta con sistemas de aire acondicionado de precisión capaces de controlar la temperatura y humedad relativa, brindando condiciones ambientales óptimas para el área operacional.

Los equipos resguardados en el área restringida se encuentran sin energía para proteger las llaves privadas de los certificados de la ECEP-RENIEC *offline* de Nivel 2.

En caso se requiera activar o utilizar los componentes tecnológicos de la ECEP-RENIEC *offline* de Nivel 2, estos son llevados a un área segura con energía eléctrica, previa autorización y coordinación con el responsable de la custodia del módulo criptográfico correspondiente.

5.1.4. Exposición al agua

El área operacional se encuentra protegida mediante pintura impermeabilizante. Además, se cuenta con mecanismos y sensores de aniego y humedad para prevenir inundaciones y otros daños por exposición al agua.

5.1.5. Previsión y protección contra fuego

Las instalaciones de la ECEP-RENIEC cuentan con puerta sólida, detectores de humo y extintores. El área operacional cuenta con un sistema de extinción no contaminante ni tóxico especializado para *data center*, de manera que se prevenga cualquier daño a los equipos sin afectar al medio ambiente ni la salud de las personas.

5.1.6. Almacenamiento de material

Se almacena dentro de una caja fuerte metálica:

- El módulo criptográfico que contiene las llaves de los certificados digitales de la ECEP-RENIEC *offline* de Nivel 2.
- Información crítica o sensible del sistema, así como los documentos que evidencian la realización de la Ceremonia de Llaves, tanto de la ECEP-RENIEC *offline* como de la ECEP-RENIEC *online.*

5.1.7. Eliminación de residuos

La información que se requiere eliminar, es destruida física o lógicamente a fin de evitar la posibilidad de su recuperación.

5.1.8. Copia de seguridad externa

Se realizan copias externas de respaldo de la información con una frecuencia de siete (07) días, como parte del cumplimiento del documento técnico de Copias de Seguridad con el código DT- DCSD/SDSCD-017.

5.2. Controles procedimentales

5.2.1. Roles de confianza

Los trabajadores designados para gestionar la infraestructura de la ECEP-RENIEC son considerados como “personas de confianza”. Los roles se designan de manera oficial incluyendo sus funciones y responsabilidades, mediante un contrato de trabajo, orden de servicio u otro, según corresponda.

5.2.2. Número de personas requeridas por labor

El uso de las llaves privadas de la ECEP-RENIEC *offline*, necesitan por lo menos la presencia de tres personas, según se establece en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada).**

Las demás labores de la ECEP-RENIEC, requieren por lo menos la presencia de una persona.

5.2.3. Identificación y autenticación para cada rol

En caso de trabajadores nuevos, el área de recursos humanos del RENIEC realiza la confirmación de identidad del personal que inicia labores en las instalaciones de la ECEP-RENIEC. Por otro lado, en caso de proveedores o visitas, se identifican mediante su documento de identidad o fotocheck de la entidad en la que trabajan.

Existe control de acceso biométrico para los roles que implican el ingreso al área operacional o al área restringida, tal como se indica en el numeral **5.1.2 Acceso físico.**

5.2.4. Roles que requieren separación de funciones

Las ECEP-RENIEC define los roles que requieren separación de funciones, sin que esto sea excluyente, para las siguientes actividades:

- Generación, emisión o destrucción de par de llaves y certificados digitales.
- Acceso y gestión de los repositorios y bases de datos con información crítica.
- Auditoría interna.

En general, las personas que se encargan de la implementación de una función, no tienen el rol de realización de la auditoría de conformidad, evaluación o revisión de dicha implementación.

5.3. Controles de personal

5.3.1. Requisitos de experiencia, capacidades y autorización

La ECEP-RENIEC define la experiencia y capacidades necesarias para cada rol de confianza, de acuerdo a lo indicado en el numeral **5.2.1 Roles de confianza**.

5.3.2. Procedimiento para verificación de antecedentes

Se verifica la documentación entregada por el personal aspirante, tomándose como referencia lo establecido en el Reglamento Interno de Trabajo del RENIEC. El área competente, realiza las siguientes verificaciones:

- Verificación de la identidad.
- Confirmación de las referencias.
- Confirmación de empleos anteriores.
- Revisión de referencias profesionales.
- Confirmación y verificación de grados académicos obtenidos.
- Verificación de antecedentes penales y policiales.
- Verificación de antecedentes financieros, crediticios o similares permitidos.

Corresponde al contratista que presta servicios en la entidad, realizar la verificación de los antecedentes de sus empleados, conforme a sus procedimientos.

5.3.3. Requisitos de capacitación

Se imparte una capacitación al inicio de funciones (inducción) y una actualización anual, si corresponde, en los siguientes aspectos:

- Uso y operación del hardware y software de la ECEP-RENIEC.
- Aspectos relevantes de la Política General de Certificación de la ECERNEP, Declaración de Prácticas de Certificación de la ECERNEP, Declaración de Prácticas de Certificación de la ECEP-RENIEC, Política de Seguridad, Plan de Privacidad, Política de Privacidad y otra Documentación de la ECEP-RENIEC.
- Marco regulatorio de la prestación de los servicios de certificación digital.
- Procedimientos en caso de contingencias.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos de seguridad para cada rol específico.

Además, se imparten capacitaciones sobre temas especializados, según se considere pertinente o al implementar un nuevo servicio de la ECEP-RENIEC.

5.3.4. Requisitos y frecuencia de re-capacitación

Las capacitaciones especializadas se imparten al personal encargado cuando se realizan cambios significativos, por ejemplo, actualizaciones de hardware y software, cambio de los sistemas y/o procedimientos de seguridad.

Se realizan capacitaciones con una frecuencia que asegure el adecuado nivel de conocimiento del personal y eficiencia para realizar sus labores. De igual manera, cada vez que se sustituya o rote al personal encargado.

5.3.5. Frecuencia y secuencia de rotación de las funciones

La rotación de funciones se realizará, en caso que, el personal de la ECEP-RENIEC cese sus funciones o por descanso físico vacacional, las cuales se encuentran establecidas en un documento.

5.3.6. Sanciones por acciones no autorizadas

Se toman acciones administrativas y disciplinarias apropiadas contra el personal, independientemente de la modalidad de contratación, que ejecute acciones no autorizadas dentro de sus funciones o que viole las normas de seguridad, según lo indique el reglamento interno del RENIEC.

Se consideran acciones no autorizadas las que contravengan, de manera negligente o malintencionada a la Política General de Certificación de la ECERNEP, la Declaración de Prácticas de la ECERNEP, la Declaración de Prácticas de la ECEP-RENIEC, la Política de Seguridad, la Política de Privacidad y Plan de Privacidad, así como a los documentos normativos de alcance al personal de la entidad.

5.3.7. Requisitos para contratistas

En caso se estime conveniente el empleo de contratistas que al interior de las instalaciones de la ECEP-RENIEC, éstos y sus empleados estarán sujetos a lo establecido en el numeral **5.3, Controles de personal** del presente documento en lo que resulte aplicable, en los mismos criterios de funciones y seguridad aplicados a empleados de la ECEP-RENIEC con cargos o roles similares. El contrato, orden de servicio u otro similar, especificará las sanciones y reparaciones para las acciones indebidas llevadas a cabo por los contratistas y sus empleados.

5.3.8. Documentación suministrada al personal

La ECEP-RENIEC suministra al personal, de acuerdo al cargo o rol, la documentación necesaria y suficiente para desempeñar sus funciones. Aquellos documentos confidenciales o con información crítica, son entregados considerando la clasificación de dicha información. Como mínimo, se suministra al personal, los siguientes documentos:

- Declaración de funciones y autorizaciones.
- Manuales para los equipos y software que deba operar.
- Declaración de prácticas, política de seguridad y otra documentación relevante en relación a sus funciones.
- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a situaciones de contingencia.

5.4. Procedimientos de registro de eventos

5.4.1. Tipos de eventos registrados

La ECEP-RENIEC mantiene un registro de auditoría de los siguientes eventos (incluyendo fecha y hora):

- Encendido y apagado de los sistemas.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema de certificación o equipos que manejen información de la Entidad.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de acceso a los registros o bases de datos del sistema de certificación
- Acceso físico a las áreas operacional y restringida.
- Eventos relacionados con el ciclo de vida de sus certificados digitales.
- Modificaciones en la CPS de la ECEP-RENIEC.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Intentos de intrusión física a la infraestructura de la ECEP-RENIEC.

Los relojes del sistema computacional se sincronizan mediante el uso del protocolo NTP para un registro exacto de la hora de los eventos.

5.4.2. Frecuencia de procesamiento del registro de eventos

Se realiza la revisión de registros de auditoría una vez al mes, como medida de prevención. Además, los registros de auditoría son revisados ante la presencia de una alerta o incidente.

5.4.3. Periodo de conservación del registro de eventos

La conservación del registro de eventos es por un periodo mínimo de diez (10) años.

5.4.4. Protección del registro de eventos

Los registros de eventos, tanto físicos como electrónicos, son considerados activos de información por lo que se encuentran sujetos a controles físicos y lógicos, de manera que se previene el acceso no autorizado y se garantiza su conservación.

La destrucción de un archivo de auditoría solo se lleva a cabo con la autorización de la AAC o cuando ha transcurrido un periodo mínimo de 10 años, como se indica en el numeral **5.4.3 Periodo de conservación del registro de eventos.**

5.4.5. Procedimiento de copia de respaldo del registro de eventos

La ECEP-RENIEC realiza copias semanales de respaldo del registro de eventos, las cuales se archivan fuera de sus instalaciones principales.

5.4.6. Sistema de realización de auditoría (Interna vs. Externa)

Las auditorías internas de la ECEP-RENIEC se llevan a cabo una vez cada tres (03) meses y las externas se realizan una vez al año o cuando la AAC lo requiera.

5.4.7. Notificación al sujeto que causa el evento

Ante la ocurrencia de un evento, personal de la ECEP-RENIEC comunica el hecho al Oficial de Seguridad de Información para que proceda con las acciones pertinentes en función a su gravedad.

En los casos, en que se establezca que el evento es de índole accidental y puede volver a ocurrir, se notifica al autor del evento (sujeto que causa el evento).

5.4.8. Evaluación de la vulnerabilidad

La ECEP-RENIEC cuenta con equipos criptográficos de hardware y software que cumplen con altos estándares de seguridad, tales como Common Criteria EAL4+ y FIPS 140-2 nivel 3, los cuales han sido evaluados ante vulnerabilidades por los fabricantes. Adicionalmente, la ECEP-RENIEC realiza análisis de vulnerabilidades y de *ethical hacking* en sus demás componentes y servicios de manera preventiva para reforzar la seguridad. Este servicio puede ser realizado por su propio personal o por un proveedor externo contratado para dicho fin.

5.5. Archivo

5.5.1. Tipos de información archivada

La ECEP-RENIEC gestiona el archivo de la siguiente información:

- CPS de la ECEP-RENIEC.
- Todos los certificados digitales emitidos o cancelados.
- Resolución de acreditación como ECEP-RENIEC ante la AAC.
- Todos los certificados digitales emitidos (Nivel 1, Nivel 2, Nivel 3 y entidades finales)
- CRL vigente.
- Registros de eventos, por el periodo de tiempo indicado en el numeral **5.4.3 Periodo de conservación del registro de eventos**

5.5.2. Periodo de conservación del archivo

Los archivos son mantenidos como mínimo por un período de diez (10) años.

5.5.3. Protección del archivo

Los archivos físicos están protegidos y supervisados para evitar el empleo inadecuado, revelación o copia de información. Los archivos de mayor relevancia, se resguardan en una caja fuerte con llave física y contraseña que se encuentra en un área restringida con control de acceso biométrico.

Los archivos lógicos de mayor relevancia, se encuentran firmados digitalmente.

5.5.4. Procedimientos para copia de seguridad del archivo

Se cuenta con procedimientos aprobados para realizar las copias de seguridad de los registros de eventos y la base de datos.

5.5.5. Requisitos de fecha y hora de los registros

Los datos archivados contienen fecha y hora del instante en que se generan. La información de hora y fecha son obtenidas mediante el protocolo NTP o Time Stamping.

5.5.6. Sistema de archivo (interno vs. externo)

Se realizan al menos dos copias de seguridad de los sistemas de la ECEP-RENIEC, gestionadas una internamente y la otra externamente, en lugar físicamente separado de las instalaciones principales.

5.5.7. Procedimientos para obtener y verificar la información archivada

La ECEP-RENIEC archiva la información clasificándola e indicando a la persona responsable. Se cuenta con un procedimiento aprobado para el acceso a la información de acuerdo a su clasificación.

5.6. Cambio de llaves

El procedimiento de cambio de llaves de la ECEP-RENIEC es el mismo procedimiento que debe realizarse para la emisión por primera vez y se realiza en fecha próxima a la expiración de sus certificados Nivel 2 o Nivel 3, en casos de cancelación de cualquiera de ellos o en caso de verse afectada la seguridad de los algoritmos criptográficos en uso.

En cualquiera de los casos expuestos, las llaves de los certificados de la ECEP-RENIEC que están siendo reemplazadas, no se usarán para emitir nuevos certificados, sino solamente para firmar las CRL correspondientes hasta la fecha de expiración del último certificado subordinado emitido utilizando dichas llaves.

5.7. Recuperación frente al compromiso y desastre

5.7.1. Procedimiento para el manejo de incidentes y compromiso

La ECEP-RENIEC cuenta con un procedimiento documentado para la gestión de contingencias en caso de falla o interrupción de algún servicio, el cual es evaluado en una auditoría. En el procedimiento se establecen mecanismos de comunicación, registro y respuesta ante incidentes, indicando la acción que ha de emprenderse. Los incidentes son comunicados, tan pronto se haya tomado conocimiento, al Oficial de Seguridad de Información de la ECEP-RENIEC.

De ser el caso, se generan reportes mensuales de incidente que permiten cuantificar y monitorear los tipos, cantidad y costos de los incidentes en la seguridad de la información.

Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (civil o criminal), se recolecta, mantiene y presenta la evidencia al oficial de seguridad de la información a fin de cumplir con la legislación vigente.

5.7.2. Corrupción de los datos, software y/o recursos computacionales

Se encuentran identificadas fuentes alternativas de recursos computacionales, software y datos para su uso en los casos de adulteraciones o fallas dentro del procedimiento documentado para la gestión de contingencias.

En caso de compromiso real o potencial de las llaves privadas de la ECEP-RENIEC, se procede según el numeral **5.7.3 Procedimiento en caso de compromiso de llave privada.**

5.7.3. Procedimiento en caso de compromiso de llave privada

En caso que, alguna de las llaves privadas de la ECEP-RENIEC resultase comprometida de manera real o potencial, el certificado digital asociado será inmediatamente cancelado, notificándose el hecho a la ECERNEP y la AAC. Todos los certificados digitales subordinados emitidos en el periodo comprendido entre el compromiso de la llave y la cancelación del certificado dejarán de ser válidos, lo cual se comunicará a los suscriptores afectados, a través de la EREP en la que realizaron sus trámites.

5.7.4. Capacidad de continuidad de las operaciones luego de un desastre

La ECEP-RENIEC cuenta con un procedimiento, conocido por su personal, probado como mínimo una (01) vez al año y aprobado para garantizar la continuidad de las operaciones en caso de desastres, haciendo posible la continuidad de las siguientes actividades:

- Recepción de solicitudes de cancelación de certificados digitales
- Cancelación de certificados digitales.
- Generación y publicación del directorio de certificados digitales de Nivel 2 y Nivel 3 y de las listas de certificados cancelados (CRL).

5.8. Terminación de la ECEP-RENIEC

En caso que la ECEP-RENIEC finalice sus actividades informará, mediante un oficio, a la ECERNEP, EREP asociadas y a la AAC, así como a los titulares, suscriptores y terceros que confían sobre el cese de sus operaciones con una anticipación mínima de treinta (30) días calendario.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. Generación e instalación del par de llaves

6.1.1. Generación del par de llaves

La ECEP-RENIEC genera sus propias pares de llaves utilizando módulos criptográficos HSM que cumplen con los requisitos descritos en el numeral **6.2.1 Estándares y controles para el módulo criptográfico.** Este procedimiento se realiza mediante una ceremonia de llaves que se efectúa en un entorno físicamente asegurado por personal en roles fiables bajo, como mínimo, control dual[4] y elementos de conocimiento dividido[5].

RENIEC dispone de un procedimiento documentado para la ceremonia de llaves de la ECEP-RENIEC, que indica, al menos, lo siguiente[6]:

- Los roles que participan en la ceremonia (internos y externos a la organización).
- Las funciones que asume cada rol y en qué fases.
- Las obligaciones de los roles antes y después de la ceremonia, según corresponda.
- La aprobación para la realización de la ceremonia.
- El hardware criptográfico y los materiales de activación necesarios para la ceremonia.
- Los pasos específicos que realizar durante la ceremonia.
- Los requisitos de seguridad física específicos para la localización de la ceremonia.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de la ceremonia.
- Los requisitos de evidencias a recoger en relación con la ceremonia.
- Las desviaciones del guion de la ceremonia.

La ECEP-RENIEC produce un acta firmada[7] que demuestra que la ceremonia ha tenido lugar de acuerdo con el procedimiento establecido, y que se ha garantizado la integridad y confidencialidad del par de llaves.

La generación de llaves de Entidad Final debe hacerse por parte de los propios suscriptores, la ECEP-RENIEC o por la EREP, utilizando módulos criptográficos que cumplan los requisitos descritos en la sección **6.2.11 Clasificación del módulo criptográfico.**

6.1.2. Entrega de la llave privada al suscriptor

Las Entidades Finales solicitantes de un certificado digital a través de la EREP-RENIEC de Persona Natural y la EREP-RENIEC de Persona Jurídica, generan sus propios pares de llaves utilizando módulos criptográficos que cumplen los requisitos descritos en el numeral **6.2.11 Clasificación del módulo criptográfico**; por lo tanto, no es necesario realizar ninguna entrega de sus llaves privadas. La ECEP-RENIEC *offline* de Nivel 2 y Nivel 3 y el PSVA-RENIEC-TSA generan, asimismo, sus propios pares de llaves en ceremonias de llaves.

[4] ETSI EN 319 411-1:2016, sección 6.5.1.a); CICA WebTrust for CA 2.0, sección 4.1.
[5] CICA WebTrust for CA 2.0, sección 4.1; CA/Browser Forum Baseline Requirements 1.4.4, sección 6.1.1.1.
[6] ETSI EN 319 411-1:2016, sección 6.5.1.f); CICA WebTrust for CA 2.0, sección 4.1.
[7] ETSI EN 319 411-1:2016, sección 6.5.1.g). CICA WebTrust for CA 2.0, sección 4.1.

En general, en caso que la ECEP-RENIEC o las EREP generen las llaves privadas del suscriptor, deben proveer canales seguros por separado para la emisión de la llave y de los códigos de activación de dichas llaves, de tal manera que se asegure la confidencialidad del titular y/o suscriptor.

6.1.3. Entrega de la llave pública al emisor del certificado digital

Las instancias de entidad de certificación de la ECEP-RENIEC del Nivel 2 y Nivel 3 y el PSVA-TSA-RENIEC entregan sus llaves públicas a las instancias superiores en la jerarquía PKI como emisoras de sus certificados digitales mediante el envío de un CSR en formato PKCS#10.

Las Entidades Finales solicitantes, a través de la EREP-RENIEC de Persona Natural o Persona Jurídica, generan su propio par de llaves y la llave pública correspondiente es remitida a la ECEP-RENIEC, para emitir su certificado, mediante el envío de un CSR en formato PKCS#10.

En caso que la ECEP-RENIEC genere el par de llaves del suscriptor, ya no será necesario solicitar la llave llave pública pues ya cuenta con ella.

6.1.4. Entrega de la llave pública al tercero que confía

Los certificados digitales de la ECEP-RENIEC son remitidos a la AAC para que sean consignados en la lista (TSL) de los PSC de confianza de la IOFE.

Además, la ECEP-RENIEC publica en los repositorios correspondientes (ver numeral **2.1 Repositorios**) sus certificados digitales que incluyen la llave pública correspondiente.

6.1.5. Tamaño de llaves

El algoritmo y el tamaño de las llaves asociadas a los certificados digitales emitidos para la ECEP-RENIEC en sus instancias de entidad de certificación de Nivel 1 y Nivel 2 (que operan *offline)* y de Nivel 3 (que opera *online)* y las que corresponden a los certificados digitales que la ECEP-RENIEC *online* emite a las Entidades Finales, tienen las siguientes características:

Nivel de la jerarquía PKI	Algoritmo de Firma	Tamaño de llaves RSA
ECEP-RENIEC *offline*	sha512WithRSAEncryption	4096 bits
ECEP-RENIEC *online*	sha512WithRSAEncryption	4096 bits
Entidades finales	sha256WithRSAEncryption	2048 bits

Tabla 6 - Algoritmo de firma y tamaño de llave

6.1.6. Parámetros de generación de llave pública y verificación de calidad

Las llaves públicas correspondientes a los certificados de la ECEP-RENIEC se generan como parte del par de llaves en un módulo criptográfico seguro y certificado, con lo que se garantiza la generación de llaves de calidad conforme a los parámetros establecidos en el numeral 6.1.5 Tamaño de llaves. Las auditorías de conformidad verificarán la calidad de las llaves públicas que emite la ECEP-RENIEC.

Además, se verifica que la llave pública contenida en el CSR de los suscriptores cumpla con los siguientes parámetros de calidad:

- Tamaño de llave: 2048 bits
- Algoritmo de generación: RSA

6.1.7. Propósito de uso de la llave (extensión *KeyUsage* X.509 v3)

Los usos admitidos de la llave para los certificados digitales están diferenciados por el valor de las extensiones *KeyUsage (KU)* y *ExtendedKeyUsage (EKU)*. El contenido de dichas extensiones, para cada tipo de certificado, se puede consultar en el Anexo 2 del presente documento.

6.2. Controles de ingeniería para protección de la llave privada y módulo criptográfico

6.2.1. Estándares y controles para el módulo criptográfico

Los módulos criptográficos de la ECEP-RENIEC, se encuentran certificados y operan conforme a Common Criteria EAL4+, perfiles de protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda[8]; o según el estándar FIPS 140-2 nivel 3.

6.2.2. Control multipersonal (k de m) de la llave privada

El acceso a los módulos criptográficos que contienen las llaves de la ECEP-RENIEC se encuentra protegido por un algoritmo criptográfico que distribuye la credencial de acceso en cinco (05) partes y que requiere un quórum de tres (03) de ellas para poder realizar cualquier operación.

La ECEP-RENIEC distribuye cada parte en una smartcard y se la entrega a una persona, llamada “custodio” y es el único autorizado para poder utilizarla, ingresando el PIN de acceso.

6.2.3. Custodia de la llave privada

La ECEP-RENIEC custodia sus propias llaves privadas, incluyendo las llaves privadas asociadas a los certificados que firman las respuestas OCSP, que son propiedad de la ECEP-RENIEC.

Además, a solicitud del suscriptor, la ECEP-RENIEC podrá almacenar y custodiar el original, copia o backup de las llaves privadas de los certificados digitales que emite para entidades finales de los perfiles de CIFRADO.

6.2.4. Respaldo de la llave privada

La ECEP-RENIEC realiza copia de respaldo (*backup*) de sus llaves privadas, aplicando el mismo nivel de protección establecido para las llaves privadas originales.

[8] Cfr. sección 6.5.2 de ETSI EN 319 411-1. Estos perfiles de protección actualizan las antiguas especificaciones CEN CWA 14167, partes 2 a 5, referenciados en el Anexo 11 de la Guía de Acreditación.

6.2.5. Archivo de la llave privada

La ECEP-RENIEC archiva sus propias llaves privadas en módulos criptográficos que cumplen lo indicado en el numeral **6.2.1 Estándares y controles para el módulo criptográfico**; en ningún caso archiva o respalda llaves privadas de las Entidades Finales.

6.2.6. Transferencia de la llave privada hacia o desde un módulo criptográfico

Se realiza al menos una copia de respaldo (ver numeral 6.2.4) de las llaves privadas de la ECEP-RENIEC *offline.* Para ello se siguen métodos y procedimientos y se utilizan algoritmos de cifrados aprobados en conformidad con la certificación FIPS 140-2 nivel 3 del módulo criptográfico HSM donde éstas se generaron u otro estándar de los indicados en el numeral **6.2.1 Estándares y controles para el módulo criptográfico**, de este documento. Estas llaves son ilegibles fuera del HSM y están protegidas por controles de seguridad de igual nivel que los establecidos para éste. Ante el mal funcionamiento del dispositivo criptográfico HSM original, la restauración de las llaves privadas a un nuevo dispositivo criptográfico HSM se dará bajo las mismas consideraciones y también lo establecido en el documento Gestión de Llaves de la ECEP-RENIEC.

Bajo los procedimientos señalados en el presente numeral se requiere de la cantidad de personas para la activación de los módulos criptográficos HSM indicada en el numeral **6.2.2, Control multipersonal (k de m) de la llave privada**, y la presencia del Oficial de Seguridad de Información de la ECEP-RENIEC.

6.2.7. Almacenamiento de la llave privada en un módulo criptográfico

Las llaves privadas de la ECEP-RENIEC han sido generadas y se mantienen en módulos criptográficos HSM certificados que operan bajo el estándar FIPS 140-2 nivel 3 u otro estándar de los indicados en el numeral **6.2.1 Estándares y controles para el módulo criptográfico**, de este documento.

6.2.8. Método de activación de la llave privada

- Llaves privadas de la ECEP-RENIEC *offline*: El método de activación sigue lo establecido en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada.** Adicionalmente, al encontrarse en un área restringida, para realiza la activación se requiere primero acceder físicamente al módulo criptográfico que las contiene, el cual se encuentra protegido dentro de una caja fuerte con llave física y contraseña dentro de un área con control biométrico.
- Llaves privadas de la ECEP-RENIEC *online:* Se encuentran activadas y operando dentro del área operacional de la ECEP-RENIEC.
- Llaves privadas de Entidades Finales: Las credenciales de uso y activación de las llaves privadas de los titulares y suscriptores se encuentran bajo control y dominio exclusivo de sus propietarios, en ningún caso de la ECEP-RENIEC.

6.2.9. Método de desactivación de la llave privada

La llave privada de la ECEP-RENIEC *offline* de Nivel 2 se activa solamente para la firma periódica de las CRLs de los certificados de la ECEP-RENIEC *online* y para la firma de los certificados digitales subordinados.

La desactivación de las llaves privadas de Nivel 3 de la ECEP-RENIEC *online* ocurre al momento del apagado de los módulos criptográficos que las contienen, los que se encuentran en el área operacional de la ECEP-RENIEC.

En el caso de Entidades Finales la desactivación de sus llaves privadas es responsabilidad del suscriptor. Para ello, se recomienda primero realizar la cancelación de los certificados digitales y luego eliminar las llaves mediante el mecanismo especificado por el fabricante de los dispositivos criptográficos que las almacenan.

6.2.10. Método de destrucción de la llave privada

En caso se requiera la destrucción de las llaves privadas de la ECEP-RENIEC, primero se realiza el procedimiento de cancelación del certificado digital (ver numeral **3.4, Identificación y autenticación para solicitudes de cancelación**), y luego se destruyen las llaves privadas de los módulos criptográficos que las contienen, incluyendo las copias de respaldo. El procedimiento se realiza según lo indicado por el fabricante del módulo criptográfico, de manera que copias recuperables no se mantengan en el dispositivo criptográfico o en zonas de memoria o de disco.

6.2.11. Clasificación del módulo criptográfico

Los módulos criptográficos de la ECEP-RENIEC cumplen con la certificación de seguridad indicada en el numeral **6.2.1 Estándares y controles para el módulo criptográfico**, de este documento.

Asimismo, los módulos criptográficos usados por los titulares y suscriptores deben cumplir con la certificación FIPS 140-2 nivel de seguridad 1 como mínimo o equivalente, según lo indicado por la AAC.

6.3. Otros aspectos de la gestión del par de llaves

6.3.1. Archivo de la llave pública

Las llaves públicas junto con los certificados digitales correspondientes a la ECEP-RENIEC Nivel 2 y Nivel 3 forman parte de los datos archivados por la ECEP-RENIEC.

6.3.2. Periodo operacional del par de llaves y periodo de uso de llaves

El periodo operacional y periodo de uso del par de llaves de los certificados emitidos por la ECEP-RENIEC, se encuentra establecido por el intervalo comprendido entre los campos "*notBefore*" y “notAfter” del certificado digital, según se indica en el numeral **7.1 Perfil de los certificados**.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

La ECEP-RENIEC realiza la generación de los datos de activación según lo indicado en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada**.

6.4.2. Protección de los datos de activación

La ECEP-RENIEC protege los datos de activación mediante lo indicado en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada.**

6.4.3. Otros aspectos de los datos de activación

La ECEP-RENIEC no cambia los datos de activación de sus módulos criptográficos, lo que haces es realizar el cambio de PIN a las smartcards que contienen los datos de activación cuando se transfieren de un custodio a otro o cuando se tenga la sospecha de una vulnerabilidad real o potencial.

6.5. Controles de seguridad computacional

6.5.1. Requisitos técnicos específicos de seguridad computacional

la ECEP-RENIEC cumple con lo estipulado en los siguientes estándares de seguridad computacional:

- ISO/IEC 27001:2013, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, o el estándar internacional ISO/IEC 27001.
- ISO/IEC 17799, Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, o el estándar internacional ISO/IEC 27002.
- ISO/IEC 15408 “Information technology - Security techniques - Evaluation criteria for IT security”.

El RENIEC dispone de una certificación ISO/IEC 27001:2013 para los sistemas de información que dan soporte a los servicios de certificación digital.

6.5.2. Evaluación de la seguridad computacional

Las evaluaciones en los módulos criptográficos utilizados por la ECEP RENIEC han sido realizadas por laboratorios autorizados en otorgar las siguientes certificaciones internacionales de seguridad:

- ISO/IEC 15408 “Information technology -- Security techniques - Evaluation criteria for IT security”.
- ISO/IEC 27001:2005 “Information technology -Security techniques - Information security management systems - Requirements”.
- FIPS PUB 140-2 – “Security Requirements for Cryptographic Modules”

Además, los equipos de cómputo y módulos criptográficos de la ECEP-RENIEC, cumplen con los siguientes controles de seguridad computacionales en todos los componentes de hardware y/o software de manera permanente:

- Autenticación de acceso.
- Almacenamiento y respaldo (copias backup) de los registros de actividad (logs).

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles para el desarrollo de sistemas

El módulo criptográfico de la ECE-RENIEC *offline* que se utiliza para la emisión y cancelación de certificados digitales cuenta con certificación de seguridad FIPS 140-2 nivel 3. El sistema criptográfico que incluye este módulo no recibe cambios o actualizaciones ni se ponen en línea.

El software que utiliza la ECEP-RENIEC para la emisión y cancelación de certificados digitales es una versión enterprise que cuenta con certificación de seguridad *Common Criteria* EAL4+.

6.6.2. Controles de gestión de seguridad

Los controles para prevenir o detectar la modificación no autorizada del software o hardware de la ECEP-RENIEC forman parte de los controles del sistema de gestión de la seguridad de la información bajo el que opera el proceso de certificación digital de la institución.

6.6.3. Controles de seguridad del ciclo de vida

Los controles de seguridad establecidos para la ECEP-RENIEC son revisados a través de auditorías que se desarrollan periódicamente según lo señalado en el numeral **5.4.6 Sistema de realización de auditoría (Interna vs. Externa).**

6.7. Controles de seguridad de red

Los módulos criptográficos de la ECEP-RENIEC que operan *offline* se encuentran normalmente sin energía y no se conectan a la red.

Los equipos de la ECEP-RENIEC y los módulos criptográficos de la ECEP-RENIEC se encuentran protegidos contra ataques, accesos no autorizados o alteración de datos. Además, los servicios y puertos que no se requieren, se encuentran desactivados.

La ECEP-RENIEC trabaja con redes segregadas, con segmentos de red aislados de otras áreas de trabajo del RENIEC.

La red tiene las siguientes características:

- Protegida por controles, tales como, firewalls, sistemas de detección de intrusos, antivirus y DMZ.

- Los datos sensibles que son transmitidos a través de redes públicas o no confiables, se protegen mediante canal seguro (SSL/TLS).
- Se controla el acceso de los usuarios a través de políticas de seguridad de red.
- Los componentes de la red local se mantienen en un ambiente físicamente seguro con control biométrico y sus configuraciones son revisadas.

6.8. Fecha y Hora

El servidor que almacena los repositorios de certificados digitales emitidos y CRL de la ECEP-RENIEC están sincronizados con un servidor confiable de tiempo (NTP).

Para el caso de archivos, se admiten servicios de sellado de hora y tiempo según la norma *ISO/IEC 18014-1 "Information technology -- Security techniques-- Time-stamping Services -- Part 1: Framework"* o la norma ETSI EN 319 421[9]. Para tal efecto debe emplearse una fuente confiable de tiempo y el Prestador de Servicio de Valor Añadido de sellos de tiempo deberá encontrarse acreditado por la AAC.

[9] Esta norma es la actualización del RFC 3628 y especificación ETSI TS 102 023.

7. PERFILES DE CERTIFICADOS, CRL y OCSP

7.1. Perfil de los certificados

El detalle de los perfiles de los certificados digitales que emite la ECEP-RENIEC se encuentra en el Anexo 2.

7.1.1. Versión de certificados digitales

Los certificados digitales que emite la ECEP-RENIEC cumplen con el estándar X509 versión 3.

7.1.2. Extensiones de certificados digitales

Los certificados emitidos por la ECEP-RENIEC cuentan, como mínimo, con los siguientes campos y extensiones de acuerdo a lo indicado en el numeral 4.1 del RFC 5280 y el numeral 7.2 de la recomendación ITU-T X.509:

	Descripción
Version	Indica el número de versión X.509 que aplica al certificado digital.
Serial Number	Número entero, mayor a cero (0), aleatorio, no secuencial de al menos 8 bytes para las entidades finales. En cualquier caso, una CA no debe emitir dos certificados digitales con el mismo número de serie.
Signature Algorithm	Algoritmo de firma con el que fue emitido el certificado digital subordinado.
Issuer	*SubjectDN* del PSC emisor
Validity	Campo que contiene el intervalo de tiempo en que el PSC garantiza que se mantendrá la información sobre el estado del certificado. El campo se representa por dos fechas: notBefore, la fecha y hora (en formato UTC) a partir de la cual el certificado digital es válido; y notAfter, la fecha y hora (en formato UTC) en que finaliza la validez del certificado (expiración).
Subject	*SubjectDN* del certificado digital
Subject Public Key Info	Campo que contiene el algoritmo de llave pública y la llave pública propiamente dicha. El algoritmo de llave debe ser RSA de 4096 bits para las CAs y 2048 bits para las entidades finales.
	EXTENSIONES
Authority Key Identifier	Esta extensión provee un medio (al software de validación) para identificar a la llave pública correspondiente a la llave privada utilizada para firmar este certificado digital. El valor de esta extensión debe estar compuesta del resumen hash SHA-1 (160 bits) de la llave pública del emisor.
Subject Key Identifier	Esta extensión provee un medio (al software de validación) para identificar a la llave pública correspondiente a este certificado digital. El valor de esta extensión debe estar compuesta del resumen hash SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info.
Key Usage	Propósitos y usos permitidos de la llave pública contenida en el certificado digital. Campo crítico. KeyUsage ::= BIT STRING { digitalSignature (0), nonRepudiation (1), -- recent editions of X.509 have -- renamed this bit to contentCommitment keyEncipherment (2), dataEncipherment (3), keyAgreement (4), keyCertSign (5), cRLSign (6), encipherOnly (7), decipherOnly (8) }

	Los bits keyCertSign (5) y cRLSign(6) solo deben ser utilizados en certificados de CA, nunca en certificados de entidad final.
Certificate Policies	Indica el OID, nombre y URL de acceso a las políticas aplicables al certificado digital y el OID correspondiente al tipo de certificados según el árbol de OID's definido por el PSC.
Subject Alternative Name	Extensión que contiene uno o más nombres adicionales del suscriptor del certificado. SubjectAltName ::= GeneralNames GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName GeneralName ::= CHOICE { otherName [0] OtherName, rfc822Name [1] IA5String, dNSName [2] IA5String, x400Address [3] ORAddress, directoryName [4] Name, ediPartyName [5] EDIPartyName, uniformResourceIdentifier [6] IA5String, iPAddress [7] OCTET STRING, registeredID [8] OBJECT IDENTIFIER } Las CAs puede incluir el email del suscriptor en rfc822Name[1] (ejemplo@dominio) cuando KeyUsage contenga el bit nonRepudiation (1). Las EC deben incluir el DNS en dNSName[2], al emitir certificados de entidad final de tipo SSL.
Basic Constraints	Indica si el certificado digital es de CA o no (entidad final) y cuántos niveles inferiores de certificados digitales de CA subordinadas se puede emitir. La extensión es una secuencia de dos valores: BasicConstraints ::= SEQUENCE { cA BOOLEAN DEFAULT FALSE, pathLenConstraint INTEGER (0…MAX) OPTIONAL cA toma el valor TRUE cuando el certificado es de CA y el valor FALSE, cuando el certificado es de entidad final. pathLenConstraint no debe estar presente si se trata de un certificado de entidad final.
Extended Key Usage	Extensión que indica propósitos y usos de la llave pública, adicionales a los indicados en la extensión KeyUsage.
CRL Distribution Points	Extensión que identifica cómo se obtiene la información de la Lista de Certificados Cancelados (CRL). Las CAs deben incluir la(s) URL(s) de acceso a la CRL. La CRL debe ser emitida por la misma CA que emite los certificados.
Authority Information Access	Indica un método de acceso a información del emisor del certificado. La extensión puede contener dos métodos de acceso: caIssuers, que debe contener la URL de acceso al certificado de la CA emisor y ocsp, que debe contener la URL del OCSP Responder, si fuera implementado por el PSC. El OCSP responder es opcional para cualquier PSC, pero, de existir, debe indicarse su URL de acceso en esta extensión.

Tabla 7 - Extensiones mínimas de los certificados digitales emitidos por la ECEP-RENIEC

El detalle de las extensiones utilizadas en los certificados digitales que emite la ECEP-RENIEC se muestra en el Anexo 2.

7.1.3.Identificador de objeto de certificados digitales

a) Identificadores de objeto de algoritmo, según RFC 3279 y RFC5280 (antes RFC 3280).
b) Identificadores de politica de certificados digitales, de acuerdo al Anexo 1 de la Guía de Acreditación para Entidades de Certificación Digital.

En el certificado digital de Nivel 2 de la ECEP-RENIEC *offline,* se consigna el identificador de objetos comodín "anyPolicy", ello para efectos de interoperabilidad en conformidad con en el RFC 5280.

En los certificados del PSVA-TSA-RENIEC se incluye un OID identificador de objeto de la política de certificados digitales, además del OID correspondiente a la política ETSI EN 319-411-1.

Los certificados digitales emitidos por la ECEP-RENIEC a entidades finales (titulares y suscriptores) cuentan con identificadores de objeto OID que provienen del PEN otorgado por IANA a RENIEC. En cada certificado digital se encuentran, en la extensión "*CertificatePolicy",* al menos los siguientes OID:

- OID de la Política General de Certificación de la ECERNEP[10]
- OID de la Declaración de Prácticas de Certificación Digital de la ECEP-RENIEC
- OID del tipo de certificado digital, según el árbol de OID de la ECEP-RENIEC
- OID de aquellas políticas de línea base a las que se adhieran a efectos de interoperabilidad, como ETSI EN 319 411-1.

7.1.4. Sintaxis y semántica de los calificadores de la política

Los calificadores de políticas estan establecidas conforme al RFC 5280 (antes RFC3280): *cPSuri* y *explicitText.* Puede encontrarse un identificador, o ambos, según se requiera.

7.1.5. Procesamiento de semantica para la extensión crítica de politicas de certificados

No aplica porque, en ningún caso, la extensión de Política de certificados (CertificatePolicy) está marcada como crítica. Revisar Anexo 2

7.2. Perfil de la CRL

7.2.1. Números de versión

Las CRLs emitidas por la ECEP-RENIEC cumplen con lo especificado en el numeral *5.* del RFC 5280 para el perfil de CRL en su versión 2.

7.2.2. CRL y extensiones de entrada CRL

No aplica.

[10] La presente declaración de prácticas cumple con los requisitos y controles establecidos en la Política General de Certificación de la ECERNEP Versión 4.0, identificada con el código OID 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.

7.3. Perfil de OCSP

7.3.1.Números de versión

La ECEP-RENIEC implementa el servicio OCSP que permite la verificación de estado de certificado en línea para certificados de Entidad Final (titular y suscriptor), según lo estipulado en el RFC 6960 (anterior RFC2560) "*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*".

Los certificados digitales emitidos por la ECEP-RENIEC que firman las respuestas OCSP cumplen con lo especificado en el RFC 5280 *"PKIX Certificate and CRL Profile"*, para el perfil de certificados en su versión 3 (X.509 v3).

7.3.2.Extensiones OCSP

El detalle de las extensiones en el certificado digital del OCSP, de acuerdo al RFC 6960, se encuentra en el Anexo 2.

8. AUDITORÍAS DE CONFORMIDAD Y OTRAS EVALUACIONES

8.1. Frecuencia y circunstancias de evaluación

La ECEP-RENIEC está sujeta a una auditoría o evaluación de conformidad, según lo regulado por la AAC.

El resultado de estas auditorías o evaluaciones de conformidad se publica por la ECEP-RENIEC en la dirección https://pki.reniec.gob.pe/acreditaciones/

8.2. Identidad/Calificaciones de auditores

Las personas que llevan a cabo la auditoria o evaluación de conformidad son designados por la AAC, de acuerdo a su normativa. Es potestad de la AAC evaluar y reconocer a un auditor como personal calificado.

8.3. Relación del auditor con la entidad auditada

La ECEP-RENIEC verifica que no exista ninguna relación entre la entidad y el auditor que pueda derivar en conflicto de intereses, de acuerdo a la normativa legal vigente sobre el tema.

8.4. Elementos cubiertos por la evaluación

Las auditorías o evaluaciones de conformidad verifican, como mínimo, los siguientes aspectos considerados como críticos:

- Alineación de la CPS de la ECEP-RENIEC a la CP DE LA ECERNEP[11] y a las Guías de Acreditación de la IOFE.
- Revisión de la vigencia de la certificación ISO/IEC 27001:2013

8.5. Acciones a ser tomadas frente a deficiencias

La ECEP-RENIEC toma acciones frente a los hallazgos encontrados por los auditores.

8.6. Publicación de resultados

La AAC publica los resultados de las auditorías o evaluaciones de conformidad realizadas dentro de la IOFE.

[11] La presente declaración de prácticas cumple con los requisitos y controles establecidos en la Política General de Certificación de la ECERNEP Versión 4.0, identificada con el código OID 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.

9. OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1. Tarifas

Las tarifas por la prestación de los servicios de certificación digital que brinda la ECEP-RENIEC se encuentran establecidas en el Texto Único de Procedimientos Administrativos del RENIEC (TUPA). Alternativamente, se puede dar la prestación de servicios a través de la suscripción de convenios donde se establecen las prestaciones y contraprestaciones del caso.

9.1.1. Tarifas para la emisión o renovación de certificados

La emisión de certificados digitales está supeditada al pago previo de la tarifa respectiva establecida en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC. Esta tasa es un tributo que grava la emisión del certificado digital, en cumplimiento al Art. 36.1 de la Ley 27444, Ley del Procedimiento Administrativo General, siendo el trato a los administrados regulado por dicho texto sin requerirse que en el contrato o acuerdo de prestación se establezca costo o pago por la tarifa.

9.1.2. Tarifas de acceso a certificados

La ECEP-RENIEC brinda el servicio de acceso a certificados digitales considerando únicamente la tarifa establecida en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC para la emisión de certificados. No aplica ninguna tasa por el empleo de los certificados digitales, ni por el acceso a los repositorios descritos en el numeral **2.1 Repositorios.**

9.1.3. Tarifas para información sobre cancelación o estado

La ECEP-RENIEC no aplica ninguna tarifa por la información sobre cancelación o estado de los certificados digitales.

9.1.4. Tarifas para otros servicios

Todas las tarifas respectivas por la prestación del servicio de certificación digital se encuentran establecidas en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC.

9.1.5. Políticas de reembolso

Es política del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano, reembolsar al solicitante la tarifa respectiva por la emisión del certificado digital, en caso su solicitud no hubiese sido atendida por responsabilidad atribuible a la ECEP-RENIEC.

La política de reembolso del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital, se encuentra establecida en el contrato o acuerdo, de darse el caso.

9.2. Responsabilidad Financiera

9.2.1.Cobertura de seguro

La ECEP-RENIEC cuenta con una Póliza de Seguros de Responsabilidad Civil contra terceros, la que es de aplicación bajo todos los ámbitos de las operaciones que desarrolla la entidad en conformidad con los roles y funciones que le han sido atribuidos bajo el marco legal

regulatorio vigente, cumpliéndose de este modo con la obligación señalada en el artículo 27° del Reglamento de la Ley de Firmas y Certificados Digitales.

9.2.2.Otros activos

La ECEP-RENIEC, para la prestación del servicio de certificación digital a su cargo, cuenta con el respaldo económico del RENIEC.

9.2.3.Cobertura de seguro o garantía para entidades finales

La ECEP-RENIEC en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano no otorga seguro o garantía para entidades finales.

9.3. Confidencialidad de información del negocio

9.3.1.Alcances de la información confidencial

La ECEP-RENIEC declara expresamente como información confidencial, que no podrá ser divulgada a terceros y que se mantendrá con carácter reservado excepto en aquellos supuestos previstos legalmente, la siguiente:

- Las llaves privadas de la ECEP-RENIEC.
- Material o información reservada de la ECEP-RENIEC, incluyendo información que versa sobre derechos de propiedad intelectual.
- Información reservada de los titulares y/o suscriptores, y de ser el caso, de los terceros que confían.
- La información del negocio suministrada por los suscriptores y otras personas con las que la ECEP-RENIEC tiene el deber de guardar secreto establecido de modo convencional.
- Información que pueda permitir a terceros no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores, titulares y los terceros que confían.
- Información que pueda permitir a terceros no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- La causa que motivó la cancelación del certificado digital.
- Información personal provista por los titulares y/o suscriptores que no sea la autorizada para estar contenida en los certificados digitales y en la Lista de Certificados Cancelados.
- Toda información relativa a las operaciones internas que lleve a cabo la ECEP-RENIEC.
- Toda información clasificada como "confidencial".
- Otra mencionada en la “Política de Seguridad”, el “Plan de Privacidad” y el “Plan de Seguridad”.

9.3.2.Información no contenida dentro del rubro de información confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La información contenida en la Política de Certificación y en la Declaración de Prácticas de Certificación aprobadas por la AAC.
- La información contenida en la Política y Plan de Privacidad aprobadas por la AAC.
- La información contenida en la Política de Seguridad aprobada por la AAC.

- La lista de certificados digitales cancelados (CRL)
- Toda otra información identificada como "pública"

El acceso a la información no considerada confidencial es permitido sin perjuicio de que la ECEP-RENIEC aplique los controles de seguridad pertinentes con el fin de proteger la autenticidad e integridad de los documentos y que impida que personas no autorizadas puedan añadir, modificar o suprimir contenidos.

9.3.3.Responsabilidad de protección de la información confidencial

El personal de la ECEP-RENIEC, personal contratado por el RENIEC, y cualquiera que se relacione con alguna actividad de la ECEP-RENIEC, está obligado a guardar secreto sobre la información clasificada como "confidencial".

9.4. Privacidad de la información personal

9.4.1.Plan de privacidad

De conformidad con lo establecido en la Ley N° 29733 – Ley de Protección de Datos Personales, se considera como datos personales, toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

La ECEP-RENIEC asegura a los titulares y/o suscriptores el adecuado tratamiento de sus datos personales, los cuales serán tratados para los fines propios de la prestación del servicio de certificación digital o para otros propósitos relacionados con dichos servicios, y que permitan otorgar confianza al tercero que confía, pudiendo él verificar el estado del certificado digital emitido por la ECEP-RENIEC.

La ECEP-RENIEC conjuntamente con la EREP-RENIEC ha desarrollado un “Plan de Privacidad”, el cual recoge los principios de la Ley antes indicada.

El referido “Plan de Privacidad” establece, entre otros aspectos, las directrices que deben cumplir los colaboradores de la ECERNEP, ECEP-RENIEC y EREP-RENIEC, y terceros que presten sus servicios como contratistas, así como las directrices respecto de la recolección de datos personales, uso y tratamiento de los mismos, transferencia de la información, mecanismos de acceso a la información personal y las medidas de seguridad destinadas a garantizar la integridad y confidencialidad de la información.

El “Plan de Privacidad” es catalogado como información pública y es publicado en el repositorio de la ECEP-RENIEC.

Las sanciones que la ECEP-RENIEC aplicará al personal involucrado en la prestación del servicio de certificación digital son las establecidas por el RENIEC.

9.4.2.Información tratada como privada

La ECEP-RENIEC declara expresamente como información personal de carácter privado, a toda aquella información que no se encuentre contenida en los certificados digitales, la lista CRL ni la respuesta OCSP.

La información personal considerada como privada es protegida contra pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

9.4.3.Información no considerada privada

La información que la ECEP-RENIEC considera no privada es aquella que se incluye en los certificados digitales, en la CRL o la respuesta OCSP. Se detalla, pero no se limita a:

- Certificados digitales emitidos o en trámite de emisión.
- Datos de identificación que figuran en el certificado digital del suscriptor y que sirven para autenticar a aquel.
- Usos y límites de uso de los certificados digitales.

Por consiguiente, la información que se hará pública es la siguiente:

- Listas de certificados digitales cancelados (CRL).
- Datos de identificación que figuran en el certificado digital del suscriptor, como: nombre completo, número del Documento Nacional de Identidad, Carné de Extranjería y Registro Único de Contribuyente (RUC), entre otros.
- Usos y límites de uso de los certificados digitales.
- El periodo de validez del certificado digital, así como la fecha de emisión y la fecha de caducidad del certificado digital.
- El número de serie del certificado.

9.4.4.Responsabilidad de protección de la información privada

La ECEP-RENIEC, consciente de la importancia de la protección de los datos personales, cumple con los principios y las disposiciones establecidas en la Ley N° 29733, Ley de Protección de Datos Personales y su reglamento.

En tal sentido, ha implementado medidas de índole organizativo y técnico orientadas a garantizar la protección y privacidad de los datos personales, así como de la información confidencial que gestiona.

Las medidas implementadas por la ECEP-RENIEC se encuentran detalladas en la “Política de Seguridad”, en la “Política de Privacidad” y en el “Plan de Privacidad”.

9.4.5.Notificación y consentimiento para el uso de información

En los formatos de solicitud de emisión y cancelación de certificados digitales se especifican los datos personales de los titulares y/o suscriptores que son recolectados.

De conformidad con lo dispuesto en el numeral 1 del Artículo 14[12]de la Ley N° 29733, Ley de Protección de Datos Personales, la ECEP-RENIEC está exceptuada de solicitar el consentimiento al titular de los datos para el tratamiento de sus datos personales.

[12] **Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales**
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.

9.4.6.Divulgación con motivo de un proceso judicial o administrativo

Los datos personales de carácter privado o la información confidencial del titular y/o suscriptor de un certificado digital, serán revelados o comunicados cuando una orden judicial o resolución administrativa emitida por la autoridad competente y de acuerdo a ley así lo exijan. De igual manera, cuando ésto sea autorizado de manera expresa por el titular y/o suscriptor.

9.4.7.Otras circunstancias para divulgación de información

La ECEP-RENIEC, dentro del marco de colaboración del sector público, podrá comunicar o ceder a otros organismos del Estado los datos personales de los titulares y/o suscriptores.

Asimismo, dentro del marco de la IOFE, los datos personales podrán ser transferidos a otras entidades de certificación.

En todo caso, la cesión o transferencia de datos personales se realizará de acuerdo a la Ley N° 29733, Ley de Protección de Datos Personales, y en lo que fuese aplicable, en el caso de las entidades de la Administración Pública, según lo señalado en el artículo 55 del Reglamento de la Ley de Firmas y Certificados Digitales.

Cabe resaltar que, en todos los casos, la entidad receptora debe garantizar a la ECEP-RENIEC la confidencialidad de la información transferida.

9.5. Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual, incluyendo los referidos a certificados, repositorios de la ECEP-RENIEC, identificadores OID, la Política General de Certificación Versión 4.0, identificada con el código OID 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000, la presente Declaración de Prácticas de Certificación, Política de Seguridad, así como cualquier otro documento de gestión de la ECEP-RENIEC en formato físico o electrónico son propiedad del RENIEC y de uso exclusivo de la ECEP-RENIEC.

Los documentos de la ECEP-RENIEC publicados en los repositorios de libre acceso son de carácter público y por lo tanto se permite su reproducción, distribución y comunicación, más no su transformación o alteración. Se prohíbe la reproducción, distribución, comunicación, transformación o alteración de los documentos de gestión de la ECEP-RENIEC que tienen el carácter de interno o reservado sin la autorización expresa del RENIEC.

Las llaves privadas y las llaves públicas son propiedad del titular y/o suscriptor del certificado digital, independientemente del medio físico que se emplee para su almacenamiento.

9.6. Representaciones y garantías

9.6.1.Representaciones y garantías de la EC

Son obligaciones de la ECEP-RENIEC:

1. Emitir y cancelar el certificado digital previa evaluación y aprobación de la solicitud.
2. Cancelar el certificado digital al suscitarse alguna de las causales señaladas en el contrato.

3. Incluir la información pertinente del certificado digital cancelado en la Lista de Certificados Digitales Cancelados (CRL).
4. Mantener la confidencialidad de la información relativa al titular y/o suscriptor, limitando su empleo a las necesidades propias del servicio de certificación, salvo por orden judicial o mandato de autoridad competente amparados por la Ley, o a pedido del titular y/o suscriptor.
5. Mantener actualizado el repositorio con los certificados digitales emitidos y la CRL.
6. Proceder a la entrega del certificado digital al titular y/o suscriptor conforme a las condiciones definidas en el presente documento.
7. En general, es obligación de la ECEP-RENIEC cumplir con todas las obligaciones establecidas en el artículo 26° del D.S N° 052-2008-PCM.

En ese sentido, la ECEP-RENIEC asumirá responsabilidad por la emisión, cancelación y consulta del estado del certificado digital. No obstante, no será responsable por:

1. Los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del titular y/o suscriptor.
2. Cualquier violación a la confidencialidad que en el uso de datos personales pudiera incurrir el propio titular y/o suscriptor.
3. La utilización incorrecta del certificado digital y de las llaves, así como de cualquier daño indirecto que pueda resultar de la utilización del certificado digital o de la información almacenada en el procesador del dispositivo criptográfico.
4. Los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado digital.
5. El contenido de aquellos documentos firmados digitalmente por el titular y/o suscriptor.
6. La falta de diligencia o cuidado del suscritor en la protección de su contraseña o PIN de acceso a su llave privada.

9.6.2.Representaciones y garantías de la ER

No aplica a la ECEP-RENIEC.

9.6.3.Representaciones y garantías de los suscriptores

Para la ECEP-RENIEC, la entidad solicitante (persona jurídica) se constituirá en el titular del certificado digital, en el caso de certificados digitales de persona jurídica y será su representante legal debidamente acreditado quien suscribirá la solicitud correspondiente, procediéndose al registro o verificación de su identidad, siendo quien asuma las obligaciones de suscriptor del certificado digital en aplicación del Art. 14° del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por D.S 052-2008-PCM.

Asimismo, en el caso de certificados digitales de persona natural, será la persona natural quien asuma los roles de titular y suscriptor, procediéndose de la misma manera al registro o verificación de su identidad y asumiendo las obligaciones como suscriptor del certificado digital en aplicación del Art. 14° del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por D.S 052-2008-PCM.

Conforme se encuentran detalladas en el correspondiente contrato o acuerdo de prestación de servicios, las obligaciones del Titular y Suscriptor son:

1. Entregar información veraz bajo su responsabilidad.

2. Actualizar la información proporcionada a la ECEP-RENIEC cuando estos ya no resulten exactos o son incorrectos.
3. Custodiar su contraseña o clave de identificación personal (PIN[13]) de acceso a su llave privada de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
4. Observar las condiciones establecidas por la ECEP-RENIEC para la utilización del certificado digital y la generación de firmas digitales.
5. Realizar un uso debido y correcto del certificado digital.
6. Notificar de inmediato a la ECEP-RENIEC en caso de que detecte que se ha incluido información incorrecta o inexacta en el certificado digital.
7. Solicitar inmediatamente a la ECEP-RENIEC la cancelación de su certificado digital en caso de tener conocimiento o sospecha de la ocurrencia de alguna de las siguientes circunstancias:
   a) Exposición, puesta en peligro o uso indebido de la llave privada o de la contraseña o PIN de acceso a su llave privada. El compromiso de la llave privada puede darse, entre otras causas, por pérdida, robo o conocimiento por terceros de la clave personal de acceso.
   b) Deterioro, alteración o cualquier otro hecho u acto que afecte la llave privada o la contraseña o PIN de acceso a su llave privada.
8. Solicitar de inmediato a la ECEP-RENIEC la cancelación del certificado cuando:
   a) La información contenida en el certificado digital ya no resulte correcta.
   b) El titular y suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la ECEP-RENIEC.

Asimismo, el titular y suscriptor del certificado asumirá las responsabilidades, a que hubiese lugar, por los daños y perjuicios que pudiese causar por aportar datos falsos, incompletos o inexactos, así como, es de su exclusiva responsabilidad el uso indebido, incorrecto o no acorde a los fines para el que fue extendido el certificado. A tal efecto, la ECEP-RENIEC está excluida de toda responsabilidad.

9.6.4.Representaciones y garantías de los terceros que confían

Es obligación de los Terceros que Confían en los certificados digitales emitidos por la ECEP-RENIEC:

1. Verificar la validez de los certificados digitales en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o haya sido cancelado.
2. No usar los certificados digitales fuera de los términos establecidos en el marco de la IOFE.
3. Limitar la fiabilidad de los certificados digitales a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados digitales y la Política de General de Certificación de la ECERNEP[14] y la Declaración de Prácticas de la ECEP-RENIEC.
4. Dar lectura al presente documento.

[13] Corresponde al término en inglés *Personal Identification Number* (PIN).

[14] La presente declaración de prácticas cumple con los requisitos y controles establecidos en la Política General de Certificación de la ECERNEP Versión 4.0, identificada con el código OID 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.

5. Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía, y aceptar y sujetarse a las mismas.

9.6.5.Representaciones y garantías de otros participantes

Es responsabilidad de la ECEP-RENIEC mantener disponibles los repositorios mencionados en el numeral **2.1 Repositorios**, tal como se indica en el numeral **2.4 Control de acceso a los repositorios.**

9.7. Exención de garantías

La ECEP-RENIEC está exenta del pago de indemnización alguna en caso que el hecho o circunstancia acaecida no sea consecuencia de lo declarado en el numeral **9.9 Indemnizaciones** del presente documento.

9.8. Limitaciones a la responsabilidad

La ECEP-RENIEC no será en ningún caso responsable cuando se encuentra en alguna de las siguientes circunstancias:

- Estado de guerra, desastre natural o cualquier otra causa de fuerza mayor, incluida el funcionamiento defectuoso de los servicios de las redes telemáticas de los ISP (Proveedores de Internet), fluido eléctrico o equipos informáticos de terceros.
- Por el uso que se pueda realizar de los certificados digitales, en especial por el contenido de los mensajes o documentos firmados o cifrados.

9.9. Indemnizaciones

La ECEP-RENIEC dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado por el RENIEC. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la ECEP-RENIEC, cumpliendo así con lo dispuesto en el artículo 27 del Reglamento de la Ley de Firmas y Certificados Digitales.

9.10. Término y terminación

9.10.1. Término

El presente documento entra en vigencia desde el momento en que es aprobado por la AAC de la IOFE, y su periodo de vigencia es de 05 años al ser este el plazo de las acreditaciones otorgadas por la AAC de acuerdo a la legislación vigente. Esto sin perjuicio que en el trascurso de este tiempo este documento pueda ser modificado por decisión propia del RENIEC o determinación de la AAC. Se contemplará que la validez de tal documentación estará sujeta a la continuidad de la acreditación.

9.10.2. Terminación

En caso de cese de actividades de la ECEP-RENIEC, ésta informará a la AAC, así como a los titulares, suscriptores y terceros que confían según lo indicado en el numeral **5.8 Terminación de la ECEP-RENIEC.**

9.10.3. Efecto de terminación y supervivencia

Las obligaciones y restricciones que establecen en esta Declaración de Prácticas de Certificación, en referencia a auditorías, información confidencial, obligaciones y responsabilidades, nacidas bajo la vigencia del presente documento, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. Notificaciones y comunicaciones individuales con los participantes

Toda notificación o comunicación con la ECEP-RENIEC se hará mediante correo electrónico o por escrito dirigido a la dirección señalada en el numeral 1.5.2 Persona de contacto, del presente documento.

Las comunicaciones producirán sus efectos cuando se envíe el acuse de recibo o el escrito se presente a mesa de partes del RENIEC, en la dirección a la que se refiere el párrafo precedente.

9.12. Enmendaduras

9.12.1. Procedimiento para enmendaduras

En caso se actualice algún procedimiento o se requiera hacer alguna enmendadura la ECEP-RENIEC presentará a la AAC la nueva versión del documento para su respectiva aprobación y posterior publicación.

9.12.2. Mecanismos y periodos de notificación

La ECEP-RENIEC pondrá a disposición de la comunidad de usuarios, así como a otras infraestructuras que la reconocen, la nueva versión de su CPS, una vez que esta haya sido aprobada por la AAC.

La ECEP-RENIEC comunicará a los suscriptores y terceros que confían, aquellas modificaciones que impliquen cambios en los términos y condiciones básicas de la prestación de los servicios de certificación que brinda, a través de la publicación en el Portal PKI https://pki.reniec.gob.pe/, surtiendo los efectos de una notificación válidamente emitida.

9.12.3. Circunstancias bajo las cuales debe ser cambiado el OID

Solo cambios significativos en la presente CPS y en otros documentos de gestión justificarán el cambio de su OID. La operación bajo una nueva jerarquía PKI o criterios de segmentación de certificados digitales podrían justificar la emisión de otras CPS distintas a la presente, debiendo llevar en ese caso un OID distinto que permita su diferenciación y adecuada referencia.

9.13. Procedimiento sobre resolución de disputas

En caso el reclamo esté directamente relacionado con el servicio de certificación digital brindado por la ECEP-RENIEC, este se deberá dirigir a la oficina con dirección indicada en el numeral **1.5.2 Persona de contacto** del presente documento para su atención en 48 horas.

De conformidad con la Segunda Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales, el titular o suscriptor podrá, una vez agotadas las instancias en el RENIEC y si lo considera pertinente, recurrir en vía administrativa ante la AAC, la que en los casos en los que proceda tal reclamación dispondrá las medidas correctivas necesarias.

En consideración a que tanto la AAC como el RENIEC son entidades de la administración pública se procederá con sujeción a la ley N° 27444, Ley del Procedimiento Administrativo General.

9.14. Ley aplicable

Conforme al Artículo Nº47 del Reglamento de la Ley de Firmas y Certificados Digitales que designa al RENIEC como ECEP y EREP, el funcionamiento y operaciones de la ECEP-RENIEC, así como el presente documento, estarán sujetos a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificaciones.
- Guía de Acreditación de Entidades de Certificación EC.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Reglamento de la Ley de Protección de Datos Personales aprobado mediante el Decreto Supremo N° 003-2013-JUS.

Así como a las disposiciones que sobre la materia dicte el INDECOPI como Autoridad Administrativa Competente en el marco de la IOFE.

9.15. Conformidad con la ley aplicable

Es responsabilidad de la ECEP-RENIEC en la prestación de sus servicios, velar por el cumplimiento de la legislación aplicable recogida en el numeral **9.14 Ley aplicable**, del presente documento.

9.16. Cláusulas misceláneas

9.16.1. Acuerdo Íntegro

Los titulares y/o suscriptores de certificados digitales, así como los terceros que confían deben observar en su totalidad el contenido del presente documento, así como las actualizaciones que se realice sobre el mismo, las cuales estarán disponibles en la siguiente dirección: https://pki.reniec.gob.pe/repositorio/

9.16.2. Subrogación

Las funciones, deberes y derechos asignados al RENIEC, en su calidad de ECEP, no serán objeto de cesión de ningún tipo a terceros, así como ninguna tercera entidad podrá subrogarse en dicha posición jurídica, salvo por disposición legal que expresamente disponga lo contrario.

9.16.3. Divisibilidad

En el caso que alguna estipulación del contrato o acuerdo de prestación de servicios de certificación digital llegase a ser declarada inválida, nula o inexigible legalmente o por orden judicial, se entenderá por no puesta. La invalidez de alguna cláusula no afectará en nada al resto del contrato o acuerdo.

9.16.4. Ejecución (tarifas de abogados y cláusulas de derechos)

No aplica.

9.16.5. Fuerza Mayor

La ECEP-RENIEC, en ningún caso será responsable por daños o perjuicios causados por:

- Catástrofes naturales;
- Casos de guerra;
- Actos de terrorismo y/o sabotaje;
- Otros actos de fuerza mayor.

Sin perjuicio de lo expuesto, la ECEP-RENIEC, dentro de lo posible, asegurará la continuidad del negocio y recuperación ante desastres.

9.17. Otras cláusulas

No se estipula.

Anexo 1 - Definiciones, abreviaturas y acrónimos

A. Acrónimos:

- **AAC**: Autoridad Administrativa Competente
- **APEC**: Foro de Cooperación Económica Asia-Pacífico
- **CP**: Política de Certificación
- **CPS**: Declaración de Prácticas de Certificación
- **DCSD**: Dirección de Certificación y Servicios Digitales (ex GRCD o Gerencia de Registros de Certificación Digital)
- **ECEP**: Entidad de Certificación para el Estado Peruano
- **ECERNEP**: Entidad de Certificación Nacional para el Estado Peruano
- **EREP**: Entidad de Registro para el Estado Peruano
- **IANA:** Del inglés, Internet Assinged Numbers Authority
- **INACAL**: Instituto Nacional de Calidad
- **INDECOPI**: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
- **OID**: Identificador de Objeto
- **PSC**: Prestador de Servicios de Certificación Digital
- **PSVA**: Prestador de Servicios de Valor Añadido
- **RENIEC**: Registro Nacional de Identificación y Estado Civil
- **PSVAEP**: Prestador de Servicios de Valor Añadido para el Estado Peruano
- **RPS**: Declaración de Prácticas de Registro
- **SDSCD**: Sub Dirección de Servicios de Certificación Digital (ex SGCID o Sub Gerencia de Certificación e Identidad Digital y ex SGRD o Sub Gerencia de Registro Digital)
- **SID**: Sistema de Intermediación Digital
- **TUPA**: Texto Único de Procedimiento Administrativo.
- **UPS**: Uninterruptible Power Supply (Unidad de alimentación de energía ininterrumpida).
- **TI**: Tecnologías de la Información
- **TSA**: Autoridad de Sellado de Tiempo
- **TSS**: Servicio de Sellado de tiempo
- **TSU**: Unidad de Sellado de tiempo
- **UTC**: Tiempo Universal Coordinado
- **VAPS**: Declaración de Prácticas de Valor Añadido

B. Glosario / Definición de términos:

Acreditación.- Es el acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, el Reglamento y las disposiciones dictadas por ella, faculta a las entidades solicitantes a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Acuse de Recibo.- Son los procedimientos que registran la recepción y validación de la Notificación Electrónica Personal recibida en el domicilio electrónico, de modo tal que impide

rechazar el envío y da certeza al remitente de que el envío y la recepción han tenido lugar en una fecha y hora determinada a través del sello de tiempo electrónico.

Agente Automatizado.- Son los procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.

Archivo.- Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fin, y que están destinados al servicio.

Autenticación.- Es el proceso de verificar la identidad de un individuo, sistema o entidad. En el contexto de la informática y la seguridad de la información, la autenticación se refiere al proceso mediante el cual un usuario demuestra ser quien dice ser, generalmente presentando credenciales como nombres de usuario, contraseñas, certificados digitales, huellas dactilares, tokens u otros medios. La autenticación es fundamental para garantizar la seguridad y la privacidad de los sistemas informáticos, ya que ayuda a prevenir el acceso no autorizado a información sensible o datos protegidos.

Autoridad de Sellado de Tiempo.- Del inglés *Time Stamping Authority* o TSA, es la autoridad que, según la norma EN 319 421, emite sellos de tiempo. En el caso de la IOFE, el servicio de sellado de tiempo es una variante de los servicios que puede brindar un Proveedor de Servicios de Valor Añadido debidamente acreditado por la Autoridad Administrativa Competente. Bajo la IOFE la TSA no es reconocida específicamente con esta denominación como una autoridad o entidad prestadora de servicios de certificación o como una entidad prestadora de servicios de confianza.

Autoridad Administrativa Competente (AAC).- Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

Backup. Proceso de respaldo que se ejecuta sobre ciertos archivos, y que consiste en copiar un archivo original a una nueva copia en un repositorio.

Cancelación de certificado digital.- Anulación definitiva de un certificado digital a petición del suscriptor, un tercero o por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las llaves o por cualquier motivo permitido y debidamente sustentado descritos en la Declaración de Prácticas de Registro o Verificación.

Certificación Cruzada.- Es el acto por el cual una Entidad de Certificación acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la Autoridad Administrativa Competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

Certificate Signing Request: Solicitud de firma de certificado (CSR por su sigla en inglés), es un bloque de texto cifrado que es enviado a una entidad de certificación para solicitar la certificación de una llave pública.

Certificado Digital.- Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de llaves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender:

La suspensión, que consiste en inhabilitar la validez de un certificado digital por un período de tiempo establecido en el momento de la solicitud de suspensión, dicho período no puede superar la fecha de expiración del certificado digital.

La modificación de la información contenida en un certificado sin la re-emisión de sus llaves.

La re-emisión, que consiste en generar un nuevo par de llaves y un nuevo certificado, correspondiente a una nueva llave pública, pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar.

Cifrado. es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que disponga de la llave de cifrado adecuada para descodificarlo.

Código de verificación o resumen (hash).- Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:

(1) El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.

(2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.

(3) Sea improbable por medios técnicos, que se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

Criptografía Asimétrica.- Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos “llaves” diferentes, pero matemáticamente relacionadas entre sí. Una de esas llaves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (llave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (llave pública). Las llaves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la llave privada a partir de la pública es técnicamente ínfima.

Declaración de Prácticas de Certificación (CPS).- Es el documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

Declaración de prácticas de la TSA.- Declaración de las prácticas que una TSA emplea para la emisión de sellos de tiempo. En el caso de la IOFE, la denominación del documento equivalente sería la Declaración de Prácticas de Valor Añadido bajo la variante de servicios de sellado de tiempo.

Declaración de Prácticas de Registro o Verificación (RPS).- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.

Declaración de Prácticas de Prestador de Servicios de Valor Añadido (PSVA).- Documento oficialmente presentado por un Prestador de Servicios de Valor Añadido a la Autoridad Administrativa Competente, mediante el cual define las prácticas para la prestación de su servicio.

Declaración de Prácticas de Valor Añadido.- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define las prácticas y procedimientos que emplea en la prestación de sus servicios.

Depósito de Certificados.- Es el sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.

Destinatario.- Es la persona designada por el iniciador para recibir un documento electrónico, siempre y cuando no actúe a título de intermediario.

Dirección de correo electrónico.- Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

Dirección oficial de correo electrónico.- Es la dirección de correo electrónico del ciudadano, reconocido por el Gobierno Peruano para la realización confiable y segura de las notificaciones electrónicas personales requeridas en los procesos públicos.

Esta dirección recibirá los mensajes de correo electrónico que sirvan para informar al usuario acerca de cada notificación o acuse de recibo que haya sido remitida a cualquiera de sus domicilios electrónicos. A diferencia del domicilio electrónico, esta dirección centraliza todas las comunicaciones que sirven para informar al usuario que se ha realizado una actualización de los documentos almacenados en sus domicilios electrónicos. Su lectura es de uso obligatorio.

Documento.- Es cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.

Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.

Documento electrónico.- Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada

por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.

Documento Nacional de Identidad electrónico (DNIe).- El Documento Nacional de Identidad Electrónico (DNIe) es una credencial de identidad digital, emitida por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y no presencialmente la identidad de las personas.

Documento oficial de identidad.- Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:

- Documento Nacional de Identidad (DNI)
- Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país.
- Pasaporte, si se trata de personas naturales extranjeras no residentes.

Domicilio Digital.- Es uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las Entidades de la Administración Pública para efectuar comunicaciones o notificaciones.

Domicilio electrónico.- Está conformado por la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital, para la tramitación confiable y segura de las notificaciones, acuses de recibo y demás documentos requeridos en sus procedimientos. En el caso de una persona jurídica el domicilio electrónico se asocia a sus integrantes. Para estos efectos, se empleará el domicilio electrónico como equivalente funcional del domicilio habitual de las personas naturales o jurídicas.

En este domicilio se almacenarán los documentos y expedientes electrónicos correspondientes a los procedimientos y trámites realizados en el respectivo Sistema de Intermediación Digital. El acceso a este domicilio se realiza empleando un certificado digital de autenticación.

EC-PSVA: Instancia de entidad de certificación de segundo nivel dentro de la jerarquía PKI CA Root 3 gestionada por la ECERNEP a través de la cual se emiten certificados digitales para los PSVA-TSA del Estado Peruano.

Entidad de Certificación.- Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Certificación Extranjera.- Es la Entidad de Certificación que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.

Entidad de Certificación Nacional para el Estado Peruano (ECERNEP): La ECERNEP es la encargada de emitir y cancelar los certificados digitales destinados a las ECEP que se lo soliciten como entidades de certificación intermedias acreditadas bajo el marco de la Infraestructura Oficial de Firma Electrónica (en adelante IOFE). De igual maneras propone políticas y estándares

ante su Autoridad Administrativa Competente (en adelante AAC) para los prestadores de servicios de certificación del Estado Peruano.

Entidad de Certificación para el Estado Peruano (ECEP): Las ECEP son Entidades de Certificación del Estado Peruano que han sido acreditadas por la AAC y tienen como función principal gestionar el ciclo de vida de los certificados digitales de Entidades Finales.

Entidad de Registro o Verificación.- Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Entidades de Registro o Verificación para el Estado Peruano (EREP): Las EREP son prestadoras de servicios de certifición del Estado Peruano que verifican la identidad de los solicitantes que realizan solicitudes de emisión y cancelación (o cualquier otro servicio que brinde la ECEP asociada) de certificados digitales. La EREP debe realizar el levantamiento de datos y la comprobación de la información brindada por el solicitante. Asimismo, debe aprobar o rechazar la emisión, reemisión o cancelación de certificados digitales, comunicando a la respectiva Entidad de Certificación con la que se encuentra asociada, de acuerdo a lo estipulado en su correspondiente Declaración de Prácticas de Registro.

Entidades de la Administración Pública.- Es el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales de los ciudadanos y la industria.

Entidad Final.- Es el suscriptor de un certificado digital.

Entorno Digital.- Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

Estándares Técnicos Internacionales.- Son los requisitos de orden técnico y de uso internacional que deben observarse en la emisión de certificados digitales y en las prácticas de certificación.

Estándares Técnicos Nacionales.- Son los estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales -CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.

Equivalencia funcional.- Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

Gobierno Digital.- Es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

Hardware Security Module: Un módulo de seguridad basado en hardware (HSM por su sigla en inglés) es un procesador de cifrado dedicado, diseñado especialmente para la protección del ciclo de vida de llaves criptográficas como las llaves privadas dentro de la criptografía asimétrica que se usan para generar la firma digital y para emitir certificados digitales o listas CRL. El HSM permite generar y almacenar las llaves criptográficas aportando aceleración en las operaciones criptográficas.

Identidad Digital.- La identidad digital significa la representación electrónica de la identidad de una persona, entidad o dispositivo en el mundo digital. Incluye atributos únicos que permiten la identificación y diferenciación de un individuo o entidad en un entorno digital. Esto puede incluir información personal como nombres de usuario, direcciones de correo electrónico, números de identificación, certificados digitales, huellas dactilares y otra información relacionada. Es esencial para el acceso a servicios en línea, comunicaciones digitales y autenticación en plataformas digitales. Gestionarlo y protegerlo es esencial para la seguridad y la privacidad en el mundo digital.

Identificación Digital.- La identificación digital es el procedimiento de reconocimiento de una persona como distinta de otras, en el entorno digital.

Identificador de objeto (OID).- Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 | ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).

Inclusión digital.- La inclusión digital es el acceso y uso de los servicios digitales por parte de los ciudadanos a través de su identidad digital, promoviendo la ciudadanía digital.

Información. Conjunto organizado de datos procesados. La información puede encontrarse en un medio físico o digital y es considerada un activo esencial para las organizaciones.

Infraestructura Oficial de Firma Electrónica (IOFE).- Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:

- La integridad de los documentos electrónicos;
- La identidad de su autor, lo que es regulado conforme a Ley.

El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

Integridad.- Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Interoperabilidad.- Es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información. Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas: interoperabilidad a nivel de componentes, interoperabilidad a nivel de aplicación e interoperabilidad entre dominios o infraestructuras PKI.

Ley.- Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Lista de Certificados Digitales Cancelados (Certificate Revocation List o CRL por su sigla en inglés): Es aquella lista en la que se incorporan todos los certificados cancelados o revocados (cancelados de oficio) por la ECERNEP, de acuerdo con lo establecido en el **Reglamento** de la Ley de Firmas y Certificados Digitales y en la Política y Declaración de Prácticas de Certificación de la ECERNEP.

Llave (o clave) privada.- Es una de las llaves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

Llave (o clave) pública.- Es la otra llave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La llave pública puede ser conocida por cualquier persona.

Mecanismos de firma digital.- Es un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma digital. Dichos mecanismos varían según el nivel de seguridad que se les aplique.

Medios electrónicos.- Son los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar de documentos electrónicos.

Medios electrónicos seguros.- Son los medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de Certificación Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.

Medios telemáticos.- Es el conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Modificación del certificado: La modificación de un certificado digital consiste en cambiar los datos contenidos en él sin efectuar una renovación de llaves.

Neutralidad tecnológica.- Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.

Niveles de seguridad.- Son los diversos niveles de garantía que ofrecen las variedades de firmas digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos.

No repudio.- Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

En el ámbito del artículo 2 de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

Nombre Común - Common Name (CN).- Es un atributo que forma parte del Nombre Distinguido (Distinguished Name - DN).

Nombre de dominio totalmente calificado o Fully Qualified Domain Name (FQDN).- Es el identificador que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo que puede identificar de forma única a un equipo servidor (o arreglo de estos) en el internet.

Nombre Diferenciado (X.501) - Distinguished Name (DN).- Es un sistema estándar diseñado para consignar en el campo sujeto de un certificado digital los datos de identificación del titular del certificado, de manera que éstos se asocien de forma inequívoca con ese titular dentro del conjunto de todos los certificados en vigor que ha emitido la Entidad de Certificación. En inglés se denomina “Distinguished Name”.

Norma Marco sobre privacidad.- Es la norma basada en la normativa aprobada en la 16 Reunión Ministerial del APEC, que fuera llevada a cabo en Santiago de Chile el 17 y 18 de noviembre de 2004, la cual forma parte integrante de las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.

Notificación electrónica personal.- En virtud del principio de equivalencia funcional, la notificación electrónica personal de los actos administrativos se realizará en el domicilio electrónico o en la dirección oficial de correo electrónico de las personas por cualquier medio

electrónico, siempre que permita confirmar la recepción, integridad, fecha y hora en que se produce. Si la notificación fuera recibida en día u hora inhábil, ésta surtirá efectos al primer día hábil siguiente a dicha recepción.

Par de llaves (o claves).- En un sistema de criptografía asimétrica comprende una llave privada y su correspondiente llave pública, ambas vinculadas matemáticamente.

Política de certificación.- Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas.

Política de sellado de tiempo.- Conjunto de reglas identificadas que indican la aplicabilidad de un sello de tiempo a una comunidad particular y/o clase de aplicación con requisitos comunes de seguridad.

Práctica.- Es el modo o método que particularmente observa alguien en sus operaciones.

Prácticas de Certificación.- Son las prácticas utilizadas para aplicar las directrices de la política establecida en la Política de Certificación respectiva.

Prácticas específicas de Certificación.- Son las prácticas que completan todos los aspectos específicos para un tipo de certificado que no están definidos en la Declaración de Prácticas de Certificación respectiva.

Prácticas de Registro o Verificación.- Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.

Prestador de Servicios de Certificación (PSC).- Es toda entidad pública o privada que indistintamente brinda servicios en la modalidad de Entidad de Certificación, Entidad de Registro o Verificación o Prestador de Servicios de Valor Añadido.

Prestador de Servicios de Valor Añadido (PSVA): Es la entidad pública o privada acreditada por la AAC que brinda servicios como Autoridad de Sellado de Tiempo (TSA), o a través de un Sistema de Intermediación Digital, de un Sistema de Preservación Digital o de un Sistema de creación de firma remota.

Prestador de Servicios de Valor Añadido – Servicio de Sellado de Tiempo (PSVA – TSA): Es la Entidad pública o privada que como una variante de PSVA brinda el servicio de sellado de tiempo, realizando procedimientos que no incluyen la firma digital de usuarios finales.

Prestador de Servicios de Valor Añadido para el Estado Peruano.- Es la Entidad pública que brinda servicios de valor añadido.

Reconocimiento de Servicios de Certificación Prestados en el Extranjero.- Es el proceso a través del cual la Autoridad Administrativa Competente, acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.

Reemisión del certificado.- En la reemisión de un certificado digital se genera un nuevo par de llaves y se emite un nuevo certificado al suscriptor bajo un procedimiento simplificado utilizando su información previamente presentada.

Registro.- En términos informáticos, es un conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos.

Registros de auditoría.- El registro de auditoría contiene todas las acciones o eventos que se llevan a cabo en la ECERNEP y que deben registrarse, los que son guardados en lugares seguros para proteger su integridad.

Reglamento.- El presente documento, denominado Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Renovación del certificado.- La renovación de un certificado digital es el procedimiento por el cual un suscriptor que ya cuenta con un certificado digital solicita la generación de uno nuevo con la información previa del suscriptor y utilizando el mismo par de llaves

Repositorio.- Espacio disponible en medios de almacenamiento de información en servidores o equipos PC que usualmente se encuentra interconectado a una red informática, pudiendo ofrecerse su publicación o puesta a disposición para su descarga en distintos niveles, por ejemplo, en Internet.

Repositorio de respaldo.- Es una carpeta creada en un servidor determinado, la cual está protegida para que sólo ingresen usuarios específicos, y que sirve para colocar dentro de ella la información que necesita ser respaldada para una futura recuperación, en caso sea necesario.

Revocación de un certificado digital.- Cancelación de oficio de un certificado digital efectuada por una entidad de certificación.

RFS.- Remote File System, Lugar donde guarda el HSM los archivos de configuración y referencias a llaves.

Security World.- Archivo cifrado que contiene los datos necesarios para la restauración del entorno de seguridad de ciertos HSM y su computador *(host).*

Sede Digital.- La sede digital es un tipo de canal digital, a través del cual pueden acceder los ciudadanos y personas en general a un catálogo de servicios digitales, realizar trámites, hacer seguimiento de los mismos, recepcionar y enviar documentos electrónicos, y cuya titularidad, gestión y administración corresponde a cada entidad de la administración pública en los ters niveles de gobierno.

Sello de tiempo.- Objeto de datos que vincula la representación de un dato a un momento en particular, estableciendo así evidencia de que este dato existió antes de dicho momento.

Servicio de Valor Añadido.- Son los servicios complementarios de la firma digital brindados dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que certifican los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónico dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

Servicio Digital.- Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

Servicio OCSP (Protocolo del estado en línea del certificado, por sus siglas en inglés).- Es el servicio que permite utilizar un protocolo estándar para realizar consultas en línea (on line) al servidor de la Autoridad de Certificación sobre el estado de un certificado.

Sistema de Intermediación Digital.- Es el sistema web que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

Sistema de Intermediación Electrónico.- Es el sistema web que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

Sistema TSA.- Conjunto de elementos de tecnologías de la información y componentes organizados para dar soporte a la provisión de servicios de sellado de tiempo.

Sistema WEB ("World Wide Web").- Sistema de documentos electrónicos enlazados y accesibles a través de Internet. Mediante un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

Suscriptor.- Es la persona natural responsable de la generación y uso de la llave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su llave privada.

Suscriptor del servicio.- Entidad que requiere los servicios provistos por un Proveedor de Servicios de Valor Añadido bajo la modalidad de sellado de tiempo, TSA, la cual ha explícita o implícitamente aceptado los términos y condiciones para su prestación.

Suspensión: La suspensión es el proceso por el cuál una ECEP, remueve temporalmente un certificado del directorio de certificados válidos o cambia su estado a "suspendido".

Tecnologías digitales.- Se refiere a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis,

acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

Tercero que confía o tercer usuario.- Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

Tiempo Universal Coordinado.- Abreviado UTC, es una escala de tiempo basada en el segundo según se define en la Recomendación ITU-R TF.460-5.

Titular.- Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Unidad de sellado de tiempo.- Del inglés **Time Stamping Unit** o TSU, es un conjunto de hardware y software gestionado como una unidad por la Time Stamping Authority o TSA y que tiene una única llave de firma de sellos de tiempo activa en determinado momento. Bajo la IOFE, las funciones de la TSA son desarrolladas por un Prestador de Servicios de Valor Añadido.

Unidades de backup. Se considera como unidades de backups a las unidades de discos duros, DVDs y CDs.

UTC (k).- Escala de tiempo producida por el laboratorio "k" en estricto acuerdo con UTC, con la meta de alcanzar una precisión de más o menos 100 ns (ver la Recomendación ITU-R TF.536-1). Una lista de los laboratorios UTC(k) se da en la sección 1 de la Circular T distribuida por BIPM y disponible en su sitio WEB (http://www.bipm.org/).

Usabilidad.- En el contexto de la certificación digital, el término Usabilidad se aplica a todos los documentos, información y sistemas de ayuda necesarios que deben ponerse a disposición de los usuarios para asegurar la aceptación y comprensión de las tecnologías, aplicaciones informáticas, sistemas y servicios de certificación digital de manera efectiva, eficiente y satisfactoria.

Usuario final.- En líneas generales, es toda persona que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado.

WebTrust.- Certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades de Certificación que de manera consistente cumplen con los estándares que establece tal organización, los que se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.

Anexo 2 – Perfiles de Certificado Digital de la ECEP-RENIEC

1. Certificados de la ECEP-RENIEC Nivel 2 y Nivel 3

   1.1. Certificado Digital de la *ECEP-RENIEC offline Nivel 2*

La *EC offline de Nivel 2* emite certificados a las EC de clases de Nivel 3. El perfil del certificado de la *EC offline de Nivel 2* se presenta en la siguiente tabla:

Perfil de Certificado ECEP-RENIEC				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECERNEP PERU CA ROOT 3	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Validity	(Not After - Not Before)	16 años	Sí	-
Subject	CN	ECEP-RENIEC	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**2.5.29.32.0**	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	1		
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecernep.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecernep.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/ecernep.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 8 - Perfil de certificado digital ECEP *off-line* (Nivel 2)

1.2. Certificados Digitales de las *EC de clases online Nivel 3*

Las *EC de clases online de Nivel 3* que emiten los certificados de entidad final son cuatro (04), detallándose su perfil en la tabla a continuación:

Perfil de Certificado de las *EC de clases {1,2,3,4} online de Nivel 3*				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	8 años	Sí	-
Subject	CN	ECEP-RENIEC CA Class (1/2/3/4)	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**2.5.29.32.0**	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	0		
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/ecep.crt	Sí	No
	ocsp (URI)	-	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 9 - Perfil de certificados digitales ECEP *on-line* (Nivel 3)

Se detalla en la tabla a continuación el perfil de los certificados de las *EC de clases online de nivel 3 de segunda generación* que emiten certificados de entidad final:

Perfil de Certificado de las *EC de clase {1, 2} II online de Nivel 3*				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	8 años	Sí	-
Subject	CN	ECEP-RENIEC CA Class (1/2) II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**2.5.29.32.0**	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	0		
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/ecep.crt	Sí	No
	ocsp (URI)	-	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 10 - Perfil de certificados digitales ECEP *on-line* Nivel 3 clase 2, segunda generación

Se detalla en la tabla a continuación el perfil del certificado de la *EC de clases online de nivel 3 clase 2 CA PN* que emite certificados de entidad final:

Perfil de Certificado de las *EC de clase 2 PN online de Nivel 3*				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	8 años	Sí	-
Subject	CN	ECEP-RENIEC CA PN	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**2.5.29.32.0**	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	0		
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/ecep.crt	Sí	No
	ocsp (URI)	-	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 11 - Perfil de certificados digitales ECEP on-line Nivel 3 clase 2 PN

2. Certificados Digitales de Entidad Final emitidos por la ECEP-RENIEC

   La ECEP-RENIEC emite diferentes tipos de certificados por cada clase, resumidos en la siguiente tabla; el tipo de certificado indica el propósito para el cual se utilizará dicho certificado y los valores de los campos y extensiones que contiene en su perfil.

Clase	Class 1				Class 2	Class 3		Class 4	Totales
Contenedor	soft	hard	swp	tee	hard	soft	hard	-	
AUT					X				1
AUT_II					X				1
AUT_pn					X				1
P_AUT					X				1
P_AUT_II					X				1
P_AUT_pn					X				1
FIR					X				1
FIR_II					X				1
FIR_pn					X				1
P_FIR					X				1
P_FIR_II					X				1
P_FIR_pn					X				1
CIF					X	X	X		3
CIF_II					X				1
CIF_pn					X				1
P_CIF					X	X	X		3
P_CIF_II					X				1
P_CIF_pn					X				1
FAU	X	X	X	X		X	X		6
FAU_II	X	X	X	X					4
P_FAU	X	X	X	X		X	X		6
P_FAU_II	X	X	X	X					4
AA								X	1
P_AA								X	1
DC								X	1
P_DC								X	1
SSL_TLS								X	1
P_SSL_TLS								X	1
Sub Total	4	4	4	4	18	4	4	6	48
Total	**16**					**8**		**6**	
OCSP	**Class 1**					**Class 3**		**Class 4**	**Totales**
OCSP 1	X								1
OCSP 1_II	X								1
OCSP 2									1
OCSP 2_II									1
OCSP 3						X			1
OCSP 4								X	1
Total	**2**					**1**		**1**	**6**

Tabla 12 - Perfiles ECEP-RENIEC

Como se observa, la ECEP-RENIEC emite cuarenta y ocho (48) tipos de certificados para suscriptores y seis (06) para el servicio OCSP.

Es importante resaltar que la Class 2 está reservada para el RENIEC, en conformidad con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales (Ley N° 27269) y en la Ley Orgánica del Registro Nacional de Identificación y Estado Civil (Ley N° 26497). Por lo tanto, solamente la ECEP-RENIEC puede emitir los certificados de Class 2 contenidos en el DNIe.

A continuación, se presenta el perfil de cada uno de los tipos de certificados que emite la ECEP-RENIEC. En todos los casos, el texto contenido entre los símbolos "<" y ">", indica que se debe reemplazar por la información del suscriptor. Ejemplo: En un certificado emitido para el Sr. Juan Alberto Perez Gonzales el texto "**CN=<APELLIDOS Nombres>"** tomará el valor **"CN=PEREZ GONZALES Juan Alberto"**. Asimismo, el texto contenido entre los símbolos "{" y "}" y entre comas, indica que se debe elegir **uno y solamente uno** de los valores, según el tipo de certificado.

Ejemplo: En un certificado de OCSP responder emitido para la Class 4, el texto "**CN=OCSP Responder Class {1, 2, 3, 4}"** tomará el valor **"CN= OCSP Responder Class 4".**Certificados OCSP responder.

Cada clase de certificados tiene su propio OCSP responder, generados según el siguiente perfil.

Perfil de Certificado OCSP Responder Class {1, 2, 3, 4}

Nombre	Atributo	Valor	Obligatorio	Crítica
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class {1, 2, 3, 4}	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	15 días	Sí	-
Subject	CN	OCSP Responder Class {1, 2, 3, 4}	Sí	-
	SERIALNUMBER	-	-	
	O	Registro Nacional de Identificación y Estado Civil	Sí	
	C	PE	Sí	
	OI	NTRPE-20295613620	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	No
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el emisor: Class 1 -->1.3.6.1.4.1.35300.2.1.3.3.1.103.1010.2, Class 2 -->1.3.6.1.4.1.35300.2.1.3.3.2.103.1010.2, Class 3 -->1.3.6.1.4.1.35300.2.1.3.3.3.103.1010.2, Class 4-->1.3.6.1.4.1.35300.2.1.3.3.4.103.1010.2}	Sí	No
	cPSuri	-		
	explicitText	OCSP Responder Class {1, 2, 3, 4}		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	
Extended Key Usage	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	-	-	-
Authority Information Access	cAIssuers	{Elegir una de las siguientes URL, según el emisor: Class 1 → http://crt.reniec.gob.pe/root3/caclass1.crt Class 2 → http://crt.reniec.gob.pe/root3/caclass2.crt Class 3 → http://crt.reniec.gob.pe/root3/caclass3.crt Class 4 → http://crt.reniec.gob.pe/root3/caclass4.crt}	Sí	No

	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	NULL	Sí	No

Tabla 13 - Perfil de certificados digitales OCSP Responder

El perfil correspondiente al OCSP responder correspondiente a la EC de nivel 3, clases 1 y 2, segunda generación, se detalla en la tabla a continuación:

Perfil de Certificado OCSP Responder Class {1, 2} II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class {1, 2} II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	15 días	Sí	-
Subject	CN	OCSP Responder Class {1, 2} II	Sí	-
	SERIALNUMBER	-	-	
	O	Registro Nacional de Identificación y Estado Civil	Sí	
	C	PE	Sí	
	OI	NTRPE-20295613620	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	No
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el emisor: Class 1 -->1.3.6.1.4.1.35300.2.1.3.3.1.103.1010.2, Class 2 -->1.3.6.1.4.1.35300.2.1.3.3.2.103.1010.2}	Sí	No
	cPSuri	-		
	explicitText	OCSP Responder Class {1, 2} II		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	
Extended Key Usage	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	-	-	-
Authority Information Access	cAIssuers	{Elegir una de las siguientes URL, según el emisor: Class 1 → http://crt.reniec.gob.pe/root3/caclass1ii.crt Class 2 → http://crt.reniec.gob.pe/root3/caclass2ii.crt}	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	NULL	Sí	No

Tabla 14 - Perfil de certificado digital OCSP Responder Class 1, 2, segunda generación

2.1. ECEP-RENIEC CA Class 1

- Bajo la Class 1, contenidos en dispositivos móviles, la ECEP-RENIEC emite certificados digitales para Identidad Digital de los ciudadanos peruanos para los propósitos de Firma y Autenticación, tanto de producción (FIR, AUT) como para pruebas (P_FIR, P_AUT).[15]

2.1.1. Certificado Digital para Identidad Digital contenidos en dispositivos móviles

Perfil de Certificado Class 1 FAU {soft, hard, swp, tee}				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 1	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	máximo 2 año	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FAU *<número de DNI> {soft, hard, swp, tee}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_ID_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		

[15] La Class 1, en cumplimiento del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**{Elegir uno de los siguientes OID, según el tipo de certificado:** **FAU en TEE --> 1.3.6.1.4.1.35300.2.1.3.1.2.103.1003.4** **FAU en SWP --> 1.3.6.1.4.1.35300.2.1.3.1.2.103.1003.5}**	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: FAU en TEE --> Certificado Digital Class 1 de firma y autenticación en móvil TEE FAU en SWP --> Certificado Digital Class 1 de firma y autenticación en móvil SWP}		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass1.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass1.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/caclass1.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 15 - Perfil de Certificado Class 1 FAU {tee, swp}

2.1.2. Certificado Digital para Identidad Digital contenidos en dispositivos móviles para pruebas

Perfil de Certificado para pruebas Class 1 P_FAU {soft, hard, swp, tee}				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 1	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| *<APELLIDOS Nombres>* P_ FAU *<número de DNI> {soft, hard, swp, tee}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_ID_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		

	policyIdentifier (OID)	**{Elegir uno de los siguientes OID, según el tipo de certificado: P_FAU en TEE --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1003.4 P_FAU en SWP --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1003.5}**	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: P_FAU en TEE --> Certificado Digital para pruebas Class 1 de firma y autenticación en móvil TEE P_FAU en SWP --> Certificado Digital para pruebas Class 1 de firma y autenticación en móvil SWP}		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass1.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass1.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/caclass1.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 16 - Perfil de Certificado para pruebas Class 1 P_FAU {tee, swp}

2.1.3. Certificado Digital para Identidad Digital contenidos en dispositivos móviles, segunda generación

Perfil de Certificado Class 1 FAU {soft, hard, swp, tee} II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-

Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 1 II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	máximo 2 año	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FAU *<número de DNI> {tee, swp}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_ID_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**{Elegir uno de los siguientes OID, según el tipo de certificado:** **FAU en TEE --> 1.3.6.1.4.1.35300.2.1.3.1.2.103.1003.4** **FAU en SWP --> 1.3.6.1.4.1.35300.2.1.3.1.2.103.1003.5}**	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: FAU en TEE --> Certificado Digital Class 1 de firma y autenticación en móvil TEE FAU en SWP --> Certificado Digital Class 1 de firma y autenticación en móvil SWP}		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No

Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass1ii.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass1ii.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/caclass1ii.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 17 - Perfil de Certificado Class 1 FAU {tee, swp} II

2.1.4. Certificado Digital para Identidad Digital contenidos en dispositivos móviles para pruebas, segunda generación

Perfil de Certificado para pruebas Class 1 P_FAU {soft, hard, swp, tee} II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 1 II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| *<APELLIDOS Nombres>* P_ FAU *<número de DNI> {tee, swp}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_ID_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		

Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**{Elegir uno de los siguientes OID, según el tipo de certificado:** **P_FAU en TEE --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1003.4** **P_FAU en SWP --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1003.5}**	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: P_FAU en TEE --> Certificado Digital para pruebas Class 1 de firma y autenticación en móvil TEE P_FAU en SWP --> Certificado Digital para pruebas Class 1 de firma y autenticación en móvil SWP}		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass1ii.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass1ii.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/caclass1ii.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No

Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 18 - Perfil de Certificado para pruebas Class 1 P_FAU {tee, swp} II

2.2. Class 2

Bajo la Class 2, contenidos dentro del DNIe, la ECEP-RENIEC emite certificados digitales a los ciudadanos peruanos para los propósitos de Firma, Autenticación y Cifrado, tanto de producción (FIR, AUT, CIF) como para pruebas (P_FIR, P_AUT, P_CIF)[16].

2.2.1.Certificado de producción para Autenticación

Perfil de Certificado Class 2 AUT hard				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* AUT *<número de DNI>* hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**0.4.0.2042.1.2**	Sí	No

[16] La Class 2 contempla lo estipulado en la Resolución Nº 042-2016/CFE-INDECOPI

	cPSuri	-		
	explicitText	Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.2.103.1002.2**	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 2 de Autenticación en hardware		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2) SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 19 - Perfil de Certificado Class 2 AUT hard

2.2.2.Certificado de producción para Firma

Perfil de Certificado Class 2 FIR hard				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	Algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FIR *<número de DNI>* hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	

	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	Algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	0.4.0.2042.1.2	Sí	No
	cPSuri	-		
	explicitText	Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.2.103.1001.2	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 2 de firma en hardware		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
	QcRetentionPeriod	*10*	Sí	No

Qualified Certificate Statements	QcLimitValue	-	No
	QcPDS	https://www.reniec.gob.pe/repository/	Sí

Tabla 20 - Perfil de Certificado Class 2 FIR hard

2.2.3.Certificado de producción para Cifrado

Perfil de Certificado Class 2 CIF hard				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	Algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* CIF *<número de DNI>* hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	Algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyEncipherment, dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	0.4.0.2042.1.2	Sí	No
	cPSuri	-		
	explicitText	Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.2.103.1004.2	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 2 de cifrado en hardware		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No

CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 21 - Perfil de Certificado Class 2 CIF hard

2.2.4.Certificado para pruebas de Autenticación, Firma o Cifrado

Perfil de Certificado para pruebas Class 2 P_{AUT, FIR, CIF} hard				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| *<APELLIDOS Nombres>* P_{AUT, FIR, CIF} <número de DNI> hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> digitalSignature P_FIR --> nonRepudiation P_CIF --> keyEncipherment, dataEncipherment }	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		

	policyIdentifier (OID)	**0.4.0.2042.1.2**	Sí	No
	cPSuri	-		
	explicitText	Política de Certificado Normalizado NCP+ de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: P_AUT en hard--> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1002.2, P_FIR en hard --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1001.2, P_CIF en hard --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1004.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: P_AUT en hard--> Certificado Digital para pruebas Class 2 de Autenticación en hardware, P_FIR en hard --> Certificado Digital para pruebas Class 2 de Firma en hardware, P_CIF en hard --> Certificado Digital para pruebas Class 2 de Cifrado en hardware}		
Subject Alternative Name **{solo para P_FIR y P_CIF}**	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> ClientAuth (1.3.6.1.5.5.7.3.2), SmartcardLogon (1.3.6.1.4.1.311.20.2.2) P_FIR --> EmailProtection (1.3.6.1.5.5.7.3.4) P_CIF --> EmailProtection (1.3.6.1.5.5.7.3.4)}	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 22 - Perfil de Certificado para pruebas Class 2 P_{AUT, FIR, CIF} hard

2.2.5.Certificado de producción para Autenticación, segunda generación

Perfil de Certificado Class 2 AUT hard II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2 II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* AUT *<número de DNI>* hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**0.4.0.2042.1.2**	Sí	No
	cPSuri	-		
	explicitText	Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.2.103.1002.2**	Sí	No
	cPSuri	-		

	explicitText	Certificado Digital Class 2 de Autenticación en hardware		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2) SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2ii.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 23 - Perfil de Certificado Class 2 AUT hard II

2.2.6.Certificado de producción para Firma, segunda generación

Perfil de Certificado Class 2 FIR hard II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	Algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2 II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FIR *<número de DNI>* hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	Algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No

Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	0.4.0.2042.1.2	Sí	No
	cPSuri	-		
	explicitText	Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.2.103.1001.2	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 2 de firma en hardware		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2ii.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	No
	QcLimitValue	-	No	
	QcPDS	https://www.reniec.gob.pe/repository/	Sí	

Tabla 24 - Perfil de Certificado Class 2 FIR hard II

2.2.7.Certificado de producción para Cifrado, segunda generación

Perfil de Certificado Class 2 CIF hard II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	Algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2 II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* CIF *<número de DNI>* hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	Algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyEncipherment, dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	0.4.0.2042.1.2	Sí	No
	cPSuri	-		
	explicitText	Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.2.103.1004.2	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 2 de cifrado en hardware		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2ii.crt	Sí	No

Authority Information Access	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 25 - Perfil de Certificado Class 2 CIF hard II

2.2.8.Certificado para pruebas de Autenticación, Firma o Cifrado, segunda generación

Perfil de Certificado para pruebas Class 2 P_{AUT, FIR, CIF} hard II				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2 II	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| *<APELLIDOS Nombres>* P_{AUT, FIR, CIF} <número de DNI> hard	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> digitalSignature P_FIR --> nonRepudiation P_CIF --> keyEncipherment, dataEncipherment }	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**0.4.0.2042.1.2**	Sí	No
	cPSuri	-		

	explicitText	Política de Certificado Normalizado NCP+ de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: P_AUT en hard--> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1002.2, P_FIR en hard --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1001.2, P_CIF en hard --> 1.3.6.1.4.1.35300.2.1.3.4.2.103.1004.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: P_AUT en hard--> Certificado Digital para pruebas Class 2 de Autenticación en hardware, P_FIR en hard --> Certificado Digital para pruebas Class 2 de Firma en hardware, P_CIF en hard --> Certificado Digital para pruebas Class 2 de Cifrado en hardware}		
Subject Alternative Name **{solo para P_FIR y P_CIF}**	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> ClientAuth (1.3.6.1.5.5.7.3.2), SmartcardLogon (1.3.6.1.4.1.311.20.2.2) P_FIR --> EmailProtection (1.3.6.1.5.5.7.3.4) P_CIF --> EmailProtection (1.3.6.1.5.5.7.3.4)}	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass2ii.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass2ii.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 26 - Perfil de Certificado para pruebas Class 2 P_{AUT, FIR, CIF} hard II

2.2.9.Certificado de producción para Autenticación para CA PN

Perfil de Certificado Class 2 AUT PN				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA PN	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* AUT *<número de DNI> pn*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	-	-	-
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/capn.crl	Sí	No

Authority Information Access	cAIssuers	http://crl.reniec.gob.pe/root3/capn.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 27 - Perfil de Certificado Class 2 AUT hard PN

2.2.10. Certificado de producción para Firma para CA PN

Perfil de Certificado Class 2 FIR PN				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	Algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA PN	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FIR *<número de DNI>* pn	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	Algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí

	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
Authority Information Access	cAIssuers	http://crl.reniec.gob.pe/root3/capn.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	No
	QcLimitValue	-	No	
	QcPDS	https://pki.reniec.gob.pe/repositorio/	Sí	

Tabla 28 - Perfil de Certificado Class 2 FIR hard PN

2.2.11. Certificado de producción para Cifrado para CA PN

Perfil de Certificado Class 2 CIF PN				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	Algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA PN	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<APELLIDOS Nombres>* CIF *<número de DNI>* pn	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	Algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyEncipherment, dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No

	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
Subject Alternative Name	rfc822Name	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
Authority Information Access	cAIssuers	http://crl.reniec.gob.pe/root3/capn.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 29 - Perfil de Certificado Class 2 CIF PN

2.2.12. Certificado para pruebas de Autenticación, Firma o Cifrado para CA PN

Perfil de Certificado para pruebas Class 2 P_{AUT, FIR, CIF} PN				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA PN	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| *<APELLIDOS Nombres>* P_{AUT, FIR, CIF} <número de DNI> pn	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_PN_RENIEC_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> digitalSignature P_FIR --> nonRepudiation P_CIF --> keyEncipherment, dataEncipherment }	Sí	Sí

Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
Subject Alternative Name **{solo para P_FIR y P_CIF}**	rfc822Name	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> - P_FIR --> EmailProtection (1.3.6.1.5.5.7.3.4) P_CIF --> EmailProtection (1.3.6.1.5.5.7.3.4)}	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/capn.crl	Sí	No
Authority Information Access	cAIssuers	http://crl.reniec.gob.pe/root3/capn.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements **{solo para P_FIR}**	QcRetentionPeriod	10	Sí	No
	QcLimitValue	-	No	
	QcPDS	https://pki.reniec.gob.pe/repositorio/	Sí	

Tabla 30 - Perfil de Certificado para pruebas Class 2 P_{AUT, FIR, CIF} PN

2.3. Class 3

Bajo la Class 3, la ECEP-RENIEC emite certificados a personas físicas (suscriptor) en su calidad de trabajadores de Entidades Públicas. En esta clase, se emiten certificados para los propósitos de Firma y Autenticación y para Cifrado, tanto de producción (FAU, CIF) como para pruebas (P_FAU, P_CIF).

2.3.1. Certificado de producción para Firma y Autenticación

Perfil de Certificado Class 3 FAU {soft, hard}				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 3	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		

	C	PE		
Validity	(Not After - Not Before)	máximo 1 año	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FAU *<número de RUC> {soft, hard}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 0.4.0.2042.1.1 Emitido en hard --> 0.4.0.2042.1.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Política de Certificado Normalizado **NCP** de acuerdo con ETSI EN 319411-1, Emitido en hard --> Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1}		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.1 Emitido en hard --> 1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.2 }	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Certificado Digital Class 3 de firma y autenticación en software Emitido en hard --> Certificado Digital Class 3 de firma y autenticación en hardware}		

Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass3.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	No
	QcLimitValue	-	No	
	QcPDS	https://www.reniec.gob.pe/repository/	Sí	

Tabla 31 - Perfil de Certificado Class 3 FAU {soft, hard}

2.3.2.Certificado de producción para Cifrado

Perfil de Certificado Class 3 CIF {soft, hard}				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 3	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	máximo 1 año	Sí	-
Subject	CN	*<APELLIDOS* Nombres> CIF *<número de RUC> {soft, hard}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-

	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyEncipherment, dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 0.4.0.2042.1.1 Emitido en hard --> 0.4.0.2042.1.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Política de Certificado Normalizado **NCP** de acuerdo con ETSI EN 319411-1, Emitido en hard --> Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1}		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 1.3.6.1.4.1.35300.2.1.3.1.3.103.1004.1 Emitido en hard --> 1.3.6.1.4.1.35300.2.1.3.1.3.103.1004.2 }	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Certificado Digital Class 3 de cifrado en software Emitido en hard --> Certificado Digital Class 3 de cifrado en hardware}		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage				
	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No

	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass3.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 32 - Perfil de Certificado Class 3 CIF {soft, hard}

2.3.3.Certificado para pruebas de Firma y Autenticación y de Cifrado

Perfil de Certificado para pruebas Class 3 {P_FAU, P_CIF} {soft, hard}				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 3	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| *<APELLIDOS Nombres>* {P_FAU/P_CIF} *<número de RUC>*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No

Key Usage	-	{Elegir, según el tipo de certificado: P_FAU--> digitalSignature, nonRepudiation P_CIF --> keyEncipherment, dataEncipherment }	Sí	Sí
Certificate Policies	**policyIdentifier (OID)**	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 0.4.0.2042.1.1 Emitido en hard --> 0.4.0.2042.1.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Política de Certificado Normalizado **NCP** de acuerdo con ETSI EN 319411-1, Emitido en hard --> Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1}		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: P_FAU en soft --> 1.3.6.1.4.1.35300.2.1.3.4.3.103.1003.1 P_FAU en hard --> 1.3.6.1.4.1.35300.2.1.3.4.3.103.1003.2, P_CIF en soft--> 1.3.6.1.4.1.35300.2.1.3.4.3.103.1004.1, P_CIF en hard --> 1.3.6.1.4.1.35300.2.1.3.4.3.103.1004.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: P_FAU en soft --> Certificado Digital para pruebas Class 3 de Firma y Autenticación en software, P_FAU en hard--> Certificado Digital para pruebas Class 3 de Firma y Autenticación en hardware, P_CIF en soft --> Certificado Digital para pruebas Class 3 de Cifrado en software, P_CIF en hard--> Certificado Digital para pruebas Class 3 de Cifrado en hardware}		
Subject Alternative Name **(Solo para FAU)**	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-

Extended Key Usage	-	{Elegir, según el tipo de certificado: P_AUT--> EmailProtection (1.3.6.1.5.5.7.3.4), ClientAuth (1.3.6.1.5.5.7.3.2), SmartcardLogon (1.3.6.1.4.1.311.20.2.2) P_CIF --> EmailProtection (1.3.6.1.5.5.7.3.4)}	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass3.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements **(Solo para FAU)**	QcRetentionPeriod	10	Sí	No
	QcLimitValue		No	
	QcPDS	https://www.reniec.gob.pe/repository/	Sí	

Tabla 33 - Perfil de Certificado para pruebas Class 3 {P_FAU, P_CIF} {soft, hard}

2.4. Class 4

Bajo la Class 4, la ECEP-RENIEC emite certificados a sistemas de información (equipos, servidores, dominios) de las Entidades de la Administración Públicas.

El titular y suscriptor de los certificados digitales de Class 4 de Agente Automatizado (AA), Domain Controller (DC) y SSL, será el representante legal de la Entidad Pública o la persona que se designe como tal.

2.4.1. Certificado de producción Agente Automatizado

Perfil de Certificado Class 4 AA				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 4	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	máximo 1 año	Sí	-
Subject	CN	*<Nombre del Agente Automatizado>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	OU	*<RUC de la entidad>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	

Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.4.103.1005.3**	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 4 de Agente Automatizado		
Subject Alternative Name	rfc822Name	*<email>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	-	-	-
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass4.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 34 - Perfil de Certificado Class 4 AA

2.4.2.Certificado para pruebas de Agente Automatizado

Perfil de Certificado Class 4 P_AA				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 4	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		

Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	||SOLO PRUEBAS|| <Nombre del Agente Automatizado>	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	OU	*<RUC de la entidad>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.4.4.103.1005.3	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital para pruebas Class 4 de Agente Automatizado		
Subject Alternative Name	rfc822Name	*<email>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	-	-	-
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass4.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 35 - Perfil de Certificado Class 4 P_AA

2.4.3.Certificado de producción Domain Controller

Perfil de Certificado Class 4 DC				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 4	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	máximo 1 año	Sí	-
Subject	CN	*<Nombre del servidor Active Directory>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	OU	*<RUC de la entidad>*	-	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, keyEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.4.103.1006.3**	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 4 de Domain Controller		
Subject Alternative Name	dNSName	*<Nombre DNS del Servidor Active Directory>*	Sí	No
	otherName	*<MS GUID = Globally Unique Identifier del Servidor Active Directory>*	Sí	
	rfc822Name	*<email>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No

	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass4.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 36 - Perfil de Certificado Class 4 DC

2.4.4.Certificado para pruebas Domain Controller

Perfil de Certificado Class 4 P_DC				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 4	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	*||SOLO PRUEBAS|| <Nombre del servidor Active Directory>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	OU	*<RUC de la entidad>*	-	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, keyEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.4.4.103.1006.3	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital para pruebas Class 4 de Domain Controller		

Subject Alternative Name	dNSName	*<Nombre DNS del Servidor Active Directory>*	Sí	No
	otherName	*<MS GUID = Globally Unique Identifier del Servidor Active Directory>*	Sí	
	rfc822Name	*<email>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass4.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 37 - Perfil de Certificado Class 4 P_DC

2.4.5.Certificado de producción SSL/TLS

Perfil de Certificado Class 4 SSL/TLS				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 4	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<DNS, nombre FQDN o número de IP>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	OU	*<RUC de la entidad>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	-	No	
	OI	*NTRPE-20295613620*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No

Key Usage	-	digitalSignature, keyEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.4.103.1007.3**	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital Class 4 de SSL/TLS		
Subject Alternative Name	dNSName	*<Nombre DNS del subdominio de *.reniec.gob.pe>*	Sí	No
	dNSName	*<Nombre DNS adicional del subdominio de *.reniec.gob.pe>*	No	
	rfc822Name	*<email>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass4.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 38 - Perfil de Certificado Class 4 SSL/TLS

2.4.6.Certificado para pruebas SSL/TLS

Perfil de Certificado Class 4 P_SSL/TLS				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 4	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	40 días	Sí	-
Subject	CN	*<DNS, nombre FQDN o número de IP>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	

	OU	*<RUC de la entidad>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	||SOLO PRUEBAS||	Sí	
	OI	NTRPE-20295613620	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	-
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, keyEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.4.4.103.1007.3	Sí	No
	cPSuri	-		
	explicitText	Certificado Digital para pruebas Class 4 de SSL/TLS		
Subject Alternative Name	dNSName	*<Nombre DNS del subdominio de *.reniec.gob.pe>*	Sí	No
	dNSName	*<Nombre DNS adicional del subdominio de *.reniec.gob.pe>*	No	
	rfc822Name	*<email>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl	Sí	No
Authority Information Access	cAIssuers	http://crt.reniec.gob.pe/root3/caclass4.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tabla 39 - Perfil de Certificado Class 4 P_SSL/TLS