# INFORME TÉCNICO

## ESTANDARIZACIÓN DEL "EQUIPO INTEGRADO DE CRIPTOGRAFÍA DENOMINADO *PKI APPLIANCE* DEL FABRICANTE PRIMEKEY"

### I. OBJETIVO

El presente documento tiene por objetivo estandarizar el equipo integrado de criptografía denominado *PKI Appliance* del fabricante PrimeKey Solutions AB de Suecia con la finalidad de garantizar la disponibilidad y la continuidad de los servicios de certificación digital de la Planta PKI del RENIEC, en cumplimiento de la Política General de Certificación de la ECERNEP, la Declaración de Prácticas y Políticas de Certificación de la ECEP y Políticas de Seguridad de la ECEP.

### II. ANTECEDENTES

El Registro Nacional de Identificación y Estado Civil (RENIEC) es la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) y la Entidad de Certificación para el Estado Peruano (ECEP), debiendo ofrecer una serie de productos y *servicios* en cumplimiento de los roles asignados en el ámbito del Reglamento de la Ley 27269, Ley de Firmas y Certificados Digitales, dentro del marco de la Infraestructura oficial de Firma Electrónica (IOFE) del Estado Peruano.

El RENIEC para el cumplimiento de las funciones referidas en el párrafo anterior, mediante la Gerencia de Registros de Certificación Digital (GRCD), en el año 2012, ha desplegado el sistema *Enterprise Java Beans Certificate Authority* (EJBCA) del fabricante PRIMEKEY, la cual se ha constituido en el motor principal de la Planta PKI sobre el que se brinda los servicios de generación de certificados digitales, la generación de CRLs, la cancelación y consultas del estado de los certificados, entre otros. Este sistema denominado "Plataforma EJBCA versión 1", es la que provee al RENIEC de capacidades para desenvolverse como ECEP.

Asimismo, con fecha 08 de abril del 2016, la GCRD adquiere un (01) equipo criptográfico "PRIMEKEY *PKI Appliance*", del fabricante PRIMEKEY, mediante adjudicación de menor cuantía (contrato Nº 046-2016-RENIEC/BIENES 08ABR2016). Además, fueron recibidos como parte de la prestación accesoria del "*Servicio de soporte, mantenimiento y garantía de los componentes de infraestructura, hardware y software de la planta PKI y servicio de mesa de ayuda tercer nivel (contrato Nº 007-2016-RENIEC/SERVICIOS 26ENE2016)* dos (02) equipos criptográficos "PRIMEKEY *PKI Appliance*", del fabricante PRIMEKEY. Con estos tres (03) equipos criptográficos se ha desplegado el sistema denominado "Plataforma EJBCA versión 2" para la planta PKI.

En el año 2013, el RENIEC presenta el documento Nacional de Identidad Electrónico (DNIe) conjuntamente con el "Plan de lanzamiento de DNIe 2013-2021" en el cual se detalla la estrategia para la introducción y lanzamiento y masificación del DNIe. Asimismo, en Junio del 2016, el RENIEC presenta el documento "Plan de Masificación del DNIe 2016-2021" en la que se establece llegar a un total de 8'625,538 DNIe emitidos hasta antes del 2021.

## III. DESCRIPCIÓN DE LA INFRAESTRUCTURA PREEXISTENTE

La Planta PKI del RENIEC actualmente cuenta con dos centros de datos, el primero denominado "Centro de Datos Principal" y un segundo denominado "Centro de Datos de Contingencia". Estos dos centros de datos en su conjunto brindan los servicios de certificación digital, mediante los sistemas EJBCA del fabricante PRIMEKEY.

### a. Componentes de la Plataforma EJBCA

La plataforma EJBCA se encuentra operando con los siguientes componentes:

**Plataforma EJBCA v1**

Servidor: EJBCA
- Cantidad: 2
- Características técnicas: 02 CPU's, 72 GB de RAM
- Sistema Operativo: Red Hat Enterprise Linux

Servidor: MariaDB Enterprise Cluster - Administración
- Cantidad: 2
- Características técnicas: 01 CPU, 6 GB de RAM
- Sistema Operativo: Red Hat Enterprise Linux

Servidor: MariaDB Enterprise Cluster - Nodos
- Cantidad: 5
- Características técnicas: 01 CPU, 8 GB de RAM
- Sistema Operativo: Red Hat Enterprise Linux

Servidor: Balanceadores
- Cantidad: 4
- Características técnicas: 01 CPU, 4 GB de RAM
- Sistema Operativo: Red Hat Enterprise Linux

Servidor: Equipo criptografico Ncipher Net HSM 2000
- Cantidad: 4
- Características técnicas: 01 CPU, 4 GB de RAM
- Sistema Operativo: Red Hat Enterprise Linux

**Plataforma EJBCA v2**

Servidor: PRIMEKEY PKI Appliance modelo M
- Cantidad: 3
- Características técnicas: 01 CPU, 32 GB de RAM
- Sistema Operativo: Linux VCG
- PKI Appliance versión: PRIMEKEY Appliance 2.5.0

Servidor: Balanceador
- Cantidad: 1
- Servidor: Fortidirector

Servidor: WAF
- Cantidad: 1
- Servidor: FortiWeb 1000d

### b. Integración con otros sistemas

La plataforma EJBCA, en sus dos versiones, interactúa y se integra con los siguientes sistemas correspondientes a la EREP-RENIEC:

- Software del sistema de administración de la Entidad de Registro para el Estado Peruano, que se encarga de la administración de las solicitudes de emisión y cancelación de certificados digitales para personas naturales entregados en el DNI electrónico.

- Software del Sistema Administrativo de la Entidad de Registro para el Estado Peruano, que se encarga de la administración de las solicitudes de emisión y cancelación de certificados digitales para personas jurídicas.

## IV. MARCO LEGAL

El artículo 8° del Reglamento de la Ley de Contrataciones del Estado, aprobado por Decreto supremo N° 350-2015-EF, establece que para la descripción de los bienes y servicios a adquirir o contratar, no se hará referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos. Excepcionalmente el citado artículo del Reglamento establece que solo procede si la Entidad ha implementado el correspondiente proceso de estandarización debidamente autorizado por el Titular de la entidad.

En el numeral 6.1 de la directiva N° 004-2016-OSCE/CD aprobada por Resolución N° 011-2016-OSCE/PRE, indica que debe entenderse por estandarización, al proceso de racionalización consistente en ajustar a un determinado tipo o modelo de los bienes o servicios a contratar, en atención a los equipamientos preexistentes.

Asimismo, de acuerdo al numeral 7.3 de la directiva mencionada, cuyo texto dice "cuando en una contratación en particular el área usuaria – aquella de la cual proviene el requerimiento de contratar o que, dada su especialidad y funciones, canaliza los requerimientos formulados por otras dependencias – considere que resulta inevitable definir el requerimiento haciendo referencia a fabricación o procedencia, procedimiento de fabricación, marca, patentes o tipos, origen o producción determinados o descripción que oriente la contratación hacia ellos, deberá elaborar un informe técnico de estandarización debidamente sustentado, el cual contendrá como mínimo:

a. La descripción del equipamiento o infraestructura preexistente de la Entidad.
b. De ser el caso, la descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda.
c. El uso o aplicación que se le dará al bien o servicio requerido.
d. La justificación de la estandarización, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos de la estandarización antes señalados y la incidencia económica de la contratación.
e. Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria
f. La fecha de elaboración del informe técnico.

## V. DESCRIPCIÓN DEL BIEN REQUERIDO

El tipo de producto a estandarizar es un **equipo integrado de criptografía** denominado *PKI Appliance* fabricado por la empresa de origen sueco PrimeKey Solutions AB. Cabe señalar que, disponiendo el equipo a estandarizarse de componentes de software, estos se encuentran integrados y no pueden individualizarse para un análisis independiente razón por la cual no aplica en este caso la realización de un Informe Técnico Previo de Evaluación de Software. Las especificaciones técnicas del equipo se detallan en el Anexo 01 del presente documento.

## VI. USO O APLICACIÓN DEL BIEN REQUERIDO

Al ser la Planta PKI la encargada de generar los certificados digitales de firma y autenticación que se entregan a los ciudadanos insertados en los DNI electrónicos, se requiere garantizar la disponibilidad y la continuidad de los servicios de certificación digital a efectos de soportar la demanda creada por la ejecución del plan de masificación del DNIe. Los más de 8 millones de DNIe que se tienen planificado emitir (según el Plan de Masificación del DNIe 2016-2021) significan como mínimo más de 16 millones de certificados digitales que tendrá que generar la planta PKI del RENIEC.

Conforme puede ser observado en la Figura 1, con la adquisición de un nuevo (01) equipo PRIMEKEY *PKI Appliance* se cubrirá, asegurará y fortalecerá la disponibilidad de la planta PKI (que actualmente cuenta con 03 PRIMEKEY *PKI Appliance*), a fin de que ésta pueda funcionar en modo activo-activo, con balanceo de carga global y local y bajo un esquema de redundancia.

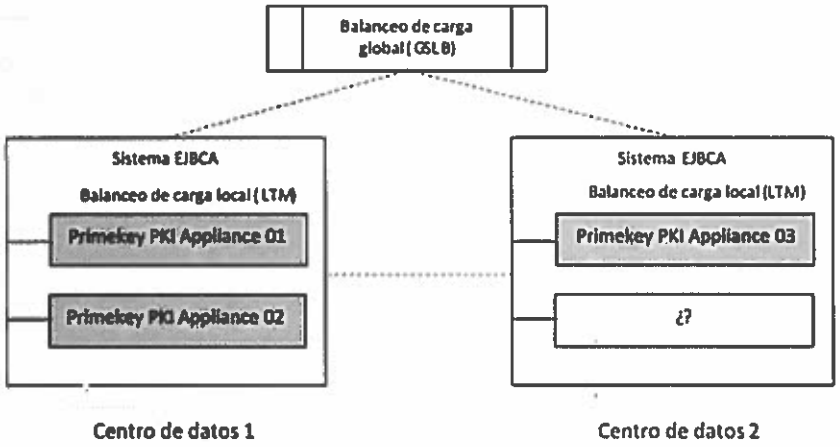


*Figura 1: Modelo de alta disponibilidad y redundancia de la Planta PKI del RENIEC*

Asimismo, en los casos que el RENIEC, para el cumplimiento de sus funciones Institucionales, necesite ampliar la cobertura de sus servicios de certificación digital, podrá instalar e implementar nuevos equipos PRIMEKEY *PKI Appliance* en nuevos Centros de Datos, los cuales se integrarán transparentemente a la infraestructura preexistente.

La adquisición de los bienes será solicitada en su oportunidad por el área usuaria y se realizará cuando exista la necesidad de incrementar el alcance de los servicios ofrecidos a través de ella y cuando el RENIEC lo determine.

## VII. JUSTIFICACIÓN DE LA ESTANDARIZACIÓN

Atendiendo a las Normas Legales señaladas en el literal d) del numeral 7.3 de la Directiva N° 004-2016-OSCE/CD "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular", el RENIEC cumple con lo señalado en la norma, describiendo lo que se indica a continuación:

### ASPECTOS TÉCNICOS

La planta PKI ha dividido el uso de la plataforma EJBCA en dos versiones: Plataforma EJBCA v1 y Plataforma EJBCA v2.

**La plataforma EJBCA v1**

La plataforma EJBCA v1, está compuesta por el software EJBCA community v4.09 que se encuentra enlazado hacia los equipos HSMs (*Hardware Security Module*) nChiper Net HSM 2000, del fabricante THALES. Dicho equipo cuenta con una configuración de seguridad denominado "*Security World*" que es el único medio por el cual se puede comunicar el HSM con la plataforma EJBCA v1. Para la administración y gestión de las tareas administrativas de dicho equipo es necesario contar con el quorum de personas que tienen que estar presentes físicamente, las cuales son Custodios de las Smartcards de Administración del HSM.

**La plataforma EJBCA v2**

La plataforma EJBCA v2, está compuesta por tres (03) equipos criptográficos integrados que contienen, entre otros, software de fábrica y un HSM (Hardware Security Module) SafeGuard CryptoServer SE del fabricante UTIMACO. Ambos componentes se encuentran embebidos en un mismo equipo físico denominado *PKI Appliance* de la empresa PRIMEKEY, por lo que no pueden ser cambiados como partes independientes.

La plataforma EJBCA (versiones v1 y v2) se encuentra instalada, configurada y operando en los centro de datos administrado por la Sub Gerencia de Certificación e Identidad Digital dentro de un entorno seguro y asociado al Sistema de Gestión de la Calidad (ISO 9001) y al Sistema Seguridad de la Información (ISO 27001) con que cuenta el proceso misional de Certificación Digital del RENIEC, garantizando la confidencialidad, integridad y disponibilidad de los servicios.

En base a lo descrito líneas arriba y según la Figura 1, es necesario adquirir un cuarto equipo con características técnicas similares o superiores a los tres (03) con los que ya se cuenta. El cuarto equipo permitirá configurar un sistema en alta disponibilidad y en redundancia, con mecanismos de balanceo de carga global y local, lo que permitirá brindar un servicio con disponibilidad 24x7.

### VERIFICACIÓN DE LOS PRESUPUESTOS PARA LA ESTANDARIZACIÓN

***a. La Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados***

En la actualidad la planta PKI del RENIEC cuenta con tres (03) dispositivos del tipo **"Equipo integrado de criptografía denominado *PKI Appliance* del fabricante PRIMEKEY"** detallados en el numeral ***III. Descripción de la Infraestructura Preexistente***, los cuales forman parte de la infraestructura tecnológica con la que se provee servicios de certificación digital, dentro del marco de la acreditación del RENIEC como, ECEP y ECERNEP; conforme lo estable la Ley N° 27269 - Ley de Firmas y Certificados Digitales, su Reglamento y de las regulaciones dadas por la AAC - INDECOPI

***b. Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura***

El bien que se requiere es complementario a la infraestructura preexistente y permitirá implementar un clúster de dispositivos que posibilite la prestación de servicios de certificación digital de alta disponibilidad, los que resultan imprescindibles para soportar la creciente emisión de DNI electrónicos, el que se estima en volúmenes de hasta 8'625,538 unidades hasta antes del 2021 conforme se refiere en el numeral II. El equipo podrá ser de características y prestaciones similares o superiores a las de los equipos ya disponibles en la planta PKI del RENIEC, pero deberá ser del mismo fabricante, lo que se sustenta en criterios económicos y operativos.

**INCIDENCIA ECONÓMICA DE LA CONTRATACIÓN.**

En el caso de no llevarse a cabo la estandarización de los equipos integrados de criptografía denominados *PKI Appliance* del fabricante PRIMEKEY, los servicios de certificación digital no contarían con la alta disponibilidad mencionados en el numeral IV del presente informe, ello conllevaría a la posibilidad latente de caídas de los servicios mencionados con el consecuente perjuicio de los usuarios y detrimento de la imagen del RENIEC como prestador de servicios de Certificación digital. Además se incurrirá en mayores gastos para el RENIEC, viéndose obligada la entidad a convocar una licitación pública para adquirir equipamiento alternativo de otros fabricantes, los cuales no necesariamente serán compatibles con la infraestructura con la que actualmente se cuenta. La integración de equipos de diferentes fabricantes suele significar una mayor inversión y mayores riesgos operativos y económicos, entre otros aspectos. También suele requerirse el desarrollo de interfaces, adecuación a herramientas administrativas ya implementadas, gestión de servicios de soporte, mantenimiento y garantía que no necesariamente son comunes a los preexistentes, además de labores extras de entrenamiento y capacitación para el personal. Este escenario significará un mayor gasto económico para la entidad.

## VIII. PERIODO DE VIGENCIA DE LA ESTANDARIZACIÓN

El periodo de vigencia de la estandarización definida para el "Equipo integrado de criptografía denominado *PKI Appliance* del fabricante PRIMEKEY" será de tres (03) años, precisando que, de variar las condiciones que determinaron la estandarización, ésta quedará sin efecto.

## IX. CONCLUSIONES

Sobre la base de las consideraciones expuestas en los numerales precedentes y en cumplimiento de la normatividad vigente, corresponde establecer como

estándar el **equipo integrado de criptografía denominado *PKI Appliance* del fabricante PRIMEKEY**, en sus modelos vigentes y en versiones iguales o superiores a las disponibles en la actualidad, con la finalidad de garantizar la disponibilidad y la continuidad de los servicios de certificación digital de la Planta PKI del RENIEC durante la vigencia de la presente estandarización.

## X. FIRMAS DE LOS RESPONSABLES DE LA ESTANDARIZACIÓN

Gerber Incacari Sancho
Administrador de Hardware y Software PKI

Alvaro Cuno Parari
Sub Gerente de Certificación e Identidad Digital (e)

Lima, 04 de Enero del 2017

# ANEXO N° 01

## ESPECIFICACIONES TÉCNICAS

## 1. DENOMINACIÓN DE LA CONTRATACIÓN

Adquisición del Equipo Integrado de Criptografía denominado PKI Appliance del fabricante PrimeKey.

## 2. FINALIDAD PÚBLICA

Con la finalidad de garantizar la disponibilidad y la continuidad de los servicios de certificación digital dentro del cumplimiento de la función como Entidad de Certificación para el Estado Peruano (LEY 27269 de Firmas y Certificados Digitales y el D.S. N° 052-2008-PCM Reglamento de Ley de Firmas y Certificados Digitales), se requiere la implementación de un equipo integrado de criptografía con las especificaciones técnicas señaladas en el Anexo A.

## 3. ANTECEDENTES

Conforme a lo establecido por la Ley N° 27269 – Ley de Firmas y Certificados Digitales, y por disposición expresa de su vigente Reglamento[1], dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), se designó al RENIEC como la única Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), RENIEC como parte de sus actividades brinda el servicio de emisión y cancelación de los certificados digitales.

## 4. OBJETIVOS DE LA CONTRATACIÓN

- **Objetivo General:**

  Implementar un equipo integrado de criptografía con la finalidad de soportar la futura demanda de servicios de certificación digital, garantizando la alta disponibilidad del servicio de certificación digital de la Planta PKI.

- **Objetivos Específicos:**

  Adquirir un equipo integrado de criptografía para implementar la alta disponibilidad y operatividad de los servicios de certificación digital brindados por la Planta PKI.

## 5. ALCANCES Y DESCRIPCIÓN DE LOS BIENES A CONTRATAR

El bien adquirido será instalado en el centro de datos de la Planta PKI del RENIEC, según las consideraciones y los requerimientos establecidos en el presente documento.

### 5.1. Características y Condiciones

#### 5.1.1. Características técnicas

El equipo integrado de criptografía denominado PKI Appliance del fabricante Primekey debe cumplir las características técnicas descritas en el Anexo A.

[1] Aprobado mediante Decreto Supremo N° 052-2008-PCM, modificado mediante el Decreto Supremo Nº 070-2011-PCM.

### 5.1.2. Normas Técnicas

La instalación de un equipo integrado de criptografía deberá alinearse con los procedimientos establecidos conforme a la norma NTP ISO/IEC 27001:2013 con los que cuenta la Planta PKI, Asimismo, deberá integrar las funcionalidades necesarias y configurarse para que su operación se dé dentro de procedimientos establecidos en conformidad con dicha norma.

### 5.1.3. Acondicionamiento, montaje o instalación

Para el acondicionamiento del equipo integrado de criptografía se deberá considerar lo siguiente:

***a. Acondicionamiento e instalación***

- Realizar el montaje y la instalación del equipo en el respectivo gabinete, estas actividades serán realizadas por el personal del proveedor en el centro de datos de la Planta PKI.
- La instalación del equipo adquirido deberá incluir los elementos y accesorios necesarios para su montaje en el rack, así como la conectividad respectiva hacia la red Ethernet.

***b. Configuración del equipo***

- Se deberá incluir la configuración de red del equipo integrado de criptografía.

### 5.1.4. Garantía

a. El proveedor deberá brindar una garantía al hardware y software por (01 año) en partes, mano de obra y On-Site, para todas sus partes y componentes por defectos de fábrica y/o vicios ocultos a partir de la fecha en la que se otorga la conformidad de recepción del bien. También se aceptará carta emitida por el fabricante. Los reportes de falla deben ser atendidos por el proveedor, call center o por el Centro Autorizado de Servicio (CAS), de acuerdo a los términos de garantía establecidos.

## 5.2. Requisitos del proveedor y/o personal

El proveedor no debe estar inhabilitado para contratar con el Estado Peruano (constancia vigente).

## 5.3. Lugar y plazo de prestación

**Lugar**

- El bien deberá ser ingresado en el Almacén Central del RENIEC, Jr. Cuzco 653, Lima Cercado.
- La instalación y configuración y puesta en funcionamiento del equipo ofertado será realizado en el centro de datos de la Planta PKI del RENIEC, Jr. Bolivia 109, torre Centro Cívico, piso 3.

**Plazo**

El plazo de entrega e instalación del equipo será de sesenta días (60) calendario, como máximo, contados a partir del día siguiente de la suscripción del contrato o recepción de la orden de compra, lo que ocurra primero.

## 5.4. Entregable

| ITEM | DESCRIPCION | U/M | CANTIDAD |
|---|---|---|---|
| 1 | Equipo integrado de criptografía denominado PKI APPLIANCE del fabricante PrimeKey | Unidad | 01 |

## 5.5. Otras obligaciones

**Obligaciones del contratista**

El proveedor proporcionará todo lo necesario para la instalación del bien ofertado a fin de que pueda dar cumplimiento a lo descrito en el presente documento.

Cualquier dispositivo, implementación, configuración o accesorios no contemplados en el presente documento y que sean necesarios para la instalación, configuración y puesta en funcionamiento del equipo será responsabilidad del proveedor y sin cargo para la Entidad.

**Obligaciones de la Entidad**

El RENIEC proporcionará las facilidades de acceso para que el proveedor instale el bien ofertado en la Planta PKI del RENIEC.

Toda actividad deberá ser coordinada previamente con el personal de RENIEC.

## 5.6. Confidencialidad

Toda información del RENIEC a que tenga acceso el proveedor así como su personal, es estrictamente confidencial. El proveedor y su personal deben comprometerse a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito del RENIEC.

Sobre la inobservancia del párrafo anterior, ésta se entenderá como un incumplimiento que no puede ser revertido, por lo que se procederá a la resolución del contrato, bastando para ello una comunicación notarial (artículo 136° del Reglamento).

## 5.7. Conformidad

La conformidad del servicio será emitida por la Sub Gerencia de Certificación e Identidad Digital de la Gerencia de Registros de Certificación Digital, previo informe

de la Sub Gerencia de Soporte Técnico Operativo, quien verificará las características técnicas.

### 5.8. Forma de pago

El pago se realizará a los 15 días calendarios siguientes al otorgamiento de la conformidad respectiva, en concordancia al artículo 14
9° del Reglamento de la Ley de Contrataciones del Estado.

### 5.9. Responsabilidad por vicios ocultos

De acuerdo al artículo 40° de la Ley de Contrataciones del Estado y artículo 146° de su Reglamento, el plazo máximo de responsabilidad del proveedor para esta contratación será de un (01) año, contado a partir de otorgada la conformidad.

# Anexo A

## ESPECIFICACIONES TÉCNICAS DE EQUIPO INTEGRADO DE CRIPTOGRAFÍA

*El equipo debe cumplir con las siguientes características mínimas:*

- *Certificación de seguridad: FIPS 140-2-Nivel 3*
- *Descripción: Hardware y software Criptográfico integrado en un solo dispositivo.*
- *Formato Appliance, altura máxima 2U*
- *Procesador de 64 Bits, mínimo con 4 núcleos de 2.0 GHz*
- *Memora RAM 32 GB o superior*
- *Capacidad de almacenamiento: Discos duros internos, 2x240 GB SSD o superiores, configurados en RAID.*
- *02 interfaces de red Gigabit Ethernet (RJ45) habilitados.*
- *Alta disponibilidad: Capacidad para balanceo de carga y replicación en múltiples nodos.*
- *El equipo deberá estar preparado para integrarse a un clúster (considerando hardware y software de las mismas características).*
- *"Deberá permitir criptografía simétrica: AES, DES y triple DES.*
- *Criptografía asimétrica: DSA, ECC, RSA (1024 A 8192 bits).*
- *Criptografía Hashing: SHA-1,SHA-2 (224 A 512 bits)"*
- *API: deberá soportar PKCS #11, JCE, CSP, CNG.*
- *Virtualización: deberá contar con una capa de virtualización que controle el flujo de datos entre los componentes de software.*
- *Interfaz de usuario: deberá disponer de una GUI basada en web para la administración y operación del equipo. La autenticación de los roles de los usuarios que acceden al dispositivo debe hacerse mediante el uso de smartcard.*
- *Debe tener embebido un software de gestión para Autoridad de Certificación (AC) con certificación Common Criteria EAL 4+ o equivalente.*
- *Autorización, suscripción o licencia emitida a nombre de RENIEC de los softwares que conforman el appliance.*
- *Backup y actualizaciones: deberá poder actualizarse y permitir la generación automática de copias de respaldo.*
- *Deberá contar con 02 fuentes de poder redundantes.*
- *El modelo del equipo ofertado debe estar vigente, a la fecha de entrega en el mercado (no descontinuado).*
- *La instalación física del equipo debe ser realiza por personal (técnico del proveedor o del fabricante)*
- *Alimentación 220 VAC o auto rango de 100-240 V.*
- *Deberá incluir lectora smartcard e incluyendo mínimo de10 tarjetas smartcard*

***Garantía:***

a) *El proveedor deberá brindar una garantía al Hardware y Software, por un (01) año en partes, mano de obra y On-Site, para todas sus partes y componentes por defectos de fábrica y/o vicios ocultos, También se aceptara carta emitida por el fabricante. Los reportes de falla deben ser atendidos por el proveedor, call center o por el Centro Autorizado de Servicio (CAS), de acuerdo a los términos de garantía establecidos.*

b) *La atención por parte del proveedor, para la ejecución de la garantía en caso de fallas reportadas por el RENIEC debe darse con un tiempo de respuesta de 4 horas, con cobertura de 8x5 los 365 días del año.*

c) *En concordancia de la Ley 28612, los equipos en mención, no limitan nuestra autonomía informática ni obligan a utilizar un determinado software.*