TÉRMINOS DE REFERENCIA

CEREMONIA DE INFRAESTRUCTURA DE LLAVE PÚBLICA (PKI)

1. ANTECEDENTES

La revolución digital está transformando profundamente la forma de vida de las sociedades, entre ellas la manera en que nos comunicamos y la forma en la que prestamos el servicio público. El despliegue digital y su aprovechamiento comprometen a todos los ciudadanos, al Estado, al sector privado, a la academia y a la sociedad civil, sin embargo, es obligación del Estado garantizar el servicio seguro y oportuno de la digitalización del país desde la conectividad, la educación, la economía, la seguridad y el gobierno digital.

Como en el país existen aún fuertes brechas que superar respecto a los indicadores internacionales en materia digital y de competitividad, es necesario la transformación digital con un sólido liderazgo al interior de las entidades públicas. Es en ese marco que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (en adelante PCM-SGTD), ha desplegado grandes esfuerzos para encaminar este proceso en el Estado hacia un mejor servicio a los ciudadanos:

Definiciones de términos:

Líder Digital: Se estableció el rol del líder digital como un miembro de la Alta Dirección de las entidades públicas. El líder dirige la estrategia de gobierno digital en las entidades con un claro enfoque en la atención de las necesidades del ciudadano. El Perú se ha convertido en el primer país de la Alianza del Pacífico en establecer el rol del líder digital al interior del Estado siguiendo las recomendaciones de la OCDE.	**Plataforma Digital para la Declaración Jurada de Intereses:** Se estableció una plataforma digital para que los funcionarios del Poder Ejecutivo declaren sus intereses en un entorno digital identificándose y firmando digitalmente con su DNI electrónico **como muestra clave de transparencia y gobierno abierto.**
Comités de Gobierno Digital: Se establece un único colegiado al interior de las entidades públicas que incorpora como miembros principales a los servidores responsables de la atención al ciudadano y la gestión de talento para dirigir una transformación digital orientada a nuestros ciudadanos. El Perú es el primer país de la Alianza del Pacífico en establecer este modelo de gobernanza para el gobierno digital.	**Promulgación de la Ley de Gobierno Digital:** El **Perú se constituye en uno de los primeros países en promulgar una Ley de Gobierno Digital** con pilares centrados en identidad digital, interoperabilidad, arquitectura digital, datos, seguridad digital y servicios digitales que implican una orientación integral de los proyectos de tecnologías digitales hacia los ciudadanos y que aseguran el despliegue de las tecnologías digitales como base de la economía digital en el país y de un Estado Digital más transparente, eficiente, confiable, productivo y cercano con el ciudadano.
Seguridad Digital: Se estableció la orientación de la seguridad digital del Estado como un entorno de confianza en el mundo digital para los ciudadanos. El Perú es el segundo país de la Alianza del	**Promulgación del Decreto Supremo 118-2018-PCM** que declara de interés nacional el desarrollo de gobierno digital, la innovación y la economía digital con enfoque territorial y crea el Comité de Alto Nivel por un Perú Digital, Innovador y

Pacífico, después de Colombia, en orientar la seguridad digital hacia ciudadanos.	Competitivo que convoca a las entidades responsables de los ámbitos fundamentales de la digitalización del Estado.
Plataforma Digital Única GOB.PE del Estado para Orientación al Ciudadano: Se estableció una única plataforma para orientar a los ciudadanos con un sólido trabajo en equipo y un esfuerzo extraordinario de todos los Ministerios. El Perú es el primer país de la Alianza del Pacífico que ha desplegado una Plataforma Única GOB.PE y el 3er. país en el mundo luego de www.gob.uk (Reino Unido) y www.gob.mx (México).	**Perú lidera el cumplimiento del Mandato 3 de la Declaración de Cali firmada por los Presidentes de Alianza del Pacífico** que promueve **el reconocimiento transfronterizo de firmas digitales** el cual impacta directamente en la seguridad y agilidad jurídica de las acciones internacionales, en el comercio internacional, en el cumplimiento de tratados de libre comercio, en la facilitación del intercambio comercial con bloques de países como APEC, Unión Europea entre otros, elevando la competitividad de los países miembros.

Así también, como parte de los avances en materia de transformación digital, el Perú y el Banco Interamericano de Desarrollo (BID) suscribieron el 12 de septiembre de 2018 el Contrato de Préstamo N° PE4399/OC-PE el mismo que permitirá garantizar la interoperabilidad entre las entidades públicas para simplificar los trámites más demandados por los ciudadanos, establecer un sólido Centro de Seguridad Digital en el Estado, construir una identidad y una carpeta digital para los ciudadanos, ampliar la Plataforma GOB.PE, establecer una sólida estrategia de datos para la toma de decisiones en el Estado y digitalizar los servicios públicos más importantes para el ciudadano.

El Proyecto tiene un monto de inversión de US$ 64.6 millones, siendo el monto del préstamo de US$ 50 millones y la contrapartida nacional de US$ 14.6 millones. Siendo los objetivos específicos: (i) simplificación, estandarización y mejora regulatoria; (ii) mejora y ampliación de las capacidades de interoperabilidad de las entidades del Estado; (iii) mejora de la gestión en la atención a ciudadanos y empresas; y (iv) mejora de las condiciones para la planificación y coordinación de los servicios.

La contratación se encuentra programada en el POA del “Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional" según el siguiente detalle:

- **Subcomponente 3.3.3.2.2 Equipos SWAT para Digitalizar 24 Servicios**
- **Componente 3: Mejora de la Gestión en la atención a Ciudadanos y Empresas.**

La contratación contribuye **al logro de metas programadas** en el “Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional", específicamente a la meta:

- **Meta:** 24 servicios digitales se ubican en el portal gob.pe al año.

2. BASE NORMATIVA

- Constitución Política del Perú
- Ley Nº 29158, Ley Orgánica del Poder Ejecutivo.
- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Decreto Legislativo N° 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa.
- Decreto Legislativo N° 1310, Decreto Legislativo que aprueba medidas adicionales de simplificación administrativa.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y modificatorias.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano, Gob.pe, y establece disposiciones adicionales para el desarrollo del Gobierno Digital
- Decreto Supremo N° 118-2018-PCM, por el que declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Resolución Ministerial N° 156-2021-PCM, que aprueba el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.

3. NORMAS TÉCNICAS

La prestación del servicio se efectuará de manera general contemplando lo señalado en la Ley N° 27269, Ley de Firmas y Certificados Digitales, en su Reglamento y en la Guía de Acreditación de Entidades de Certificación EC V4.1. Asimismo, se deben tomar en cuenta las normas legales señaladas en el numeral 2, Base normativa.

Para el desarrollo del servicio a brindarse se deberá cumplir de manera específica con lo señalado en el Plan de Administración de Llaves de la Entidad de Certificación Nacional del Estado Peruano (ECERNEP) y de la Entidad de Certificación del Estado Peruano de la Presidencia del Consejo de Ministros (ECEP PCM) a elaborarse y aprobarse dentro del desarrollo del servicio.

De igual manera, para la prestación del servicio y la provisión de los entregables indicados se deberá contemplar lo señalado en los siguientes documentos técnicos y estándares en sus últimas versiones:

- IETF RFC 3647, Internet X.509 *Public Key Infrastructure - Certificate Policy and Certification Practices Framework*.

- FIPS PUB 140-2, *Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules*.
- *Recommendation* ITU-T X.509.
- RFC 5280, Internet X.509 P*ublic Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile*.
- ETSI EN 319 411-1, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*.
- ETSI EN 319 412-3, *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons*.
- NTP-ISO/IEC 17799, EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.
- CPA *Canada WebTrust Principles and Criteria for Certification Authorities*. Versión 2.2.

4. OBJETIVO DEL SERVICIO

Desarrollar una ceremonia de llaves para la generación de seis (06) pares de llaves asimétricas correspondientes a dos (02) nuevas jerarquías de Infraestructura de Llave Pública (PKI[1] por sus siglas en inglés) del Estado Peruano conforme al diseño de arquitectura que se presenta en el Gráfico 1, en lo que comprende la parte encerrada dentro de la línea roja punteada, cumpliendo los requisitos establecidos en las presentes especificaciones técnicas, en el marco del "Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional".

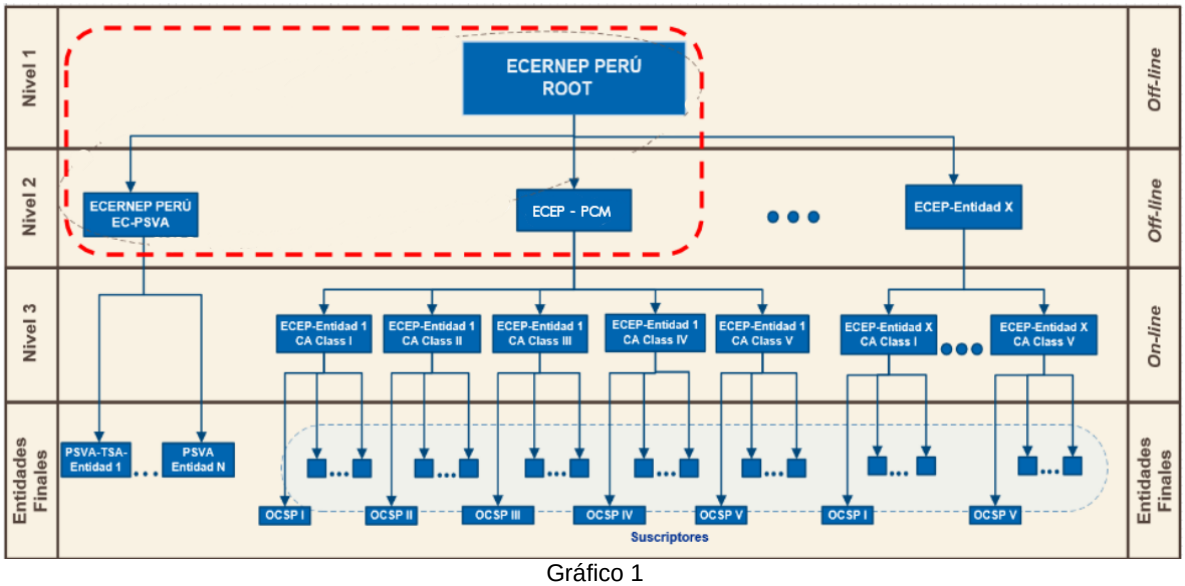

Gráfico 1

5. OBJETIVOS ESPECÍFICOS

- Efectuar la transferencia de conocimientos en el uso de sistemas criptográficos.
- Definir los algoritmos criptográficos y de resumen a utilizarse para la generación de llaves asimétricas y para la emisión de certificados y de listas de certificados cancelados (CRL)[2].

[1] PKI Public Key Infrastructure.
[2] Lista de Certificados Cancelados (CRL por sus siglas en inglés)

- Contar con los perfiles de los certificados digitales y de las listas de certificados cancelados (CRL).
- Contar con el Plan de Administración de Llaves de la ECERNEP.
- Establecer el flujo general de la ceremonia de llaves para las raíces de dos (2) nuevas jerarquías PKI del Estado Peruano cuya gestión corresponde a la ECERNEP.
- Diseñar la ceremonia de llaves para las raíces de dos (2) nuevas jerarquías PKI del Estado Peruano cuya gestión corresponde a la ECERNEP.
- Realizar la ceremonia de llaves para las raíces de dos (2) nuevas jerarquías PKI del Estado Peruano cuya gestión corresponde a la ECERNEP.
- Ejecutar las pruebas de emisión de certificados digitales para la Entidad de Certificación del Estado Peruano (ECEP) online y de Prestador de Servicios de Valor Añadido del Estado Peruano bajo la modalidad de Autoridad de Sellado de Tiempo (PSVA-TSA).

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

El servicio por brindarse comprenderá el diseño y desarrollo de una única ceremonia de llaves para la implementación de dos (2) nuevas jerarquías PKI del Estado Peruano, una basada en algoritmos criptográficos RSA[3] (denominada ECERNEP PERÚ ROOT 5) y otra en algoritmos de curva elíptica[4] (denominada ECERNEP PERÚ ROOT 6), comprendiendo a cada una de las entidades o instancias a cargo de la PCM-SGTD que la componen[5]. Se contempla, además, la realización de actividades preliminares como la definición de los algoritmos y perfiles de certificados digitales a utilizarse, el diseño de la ceremonia y la preparación de equipos con el correspondiente ensayo de ceremonia de llaves, y otras posteriores, como las pruebas de emisión de certificados digitales para la ECERNEP PERÚ ROOT, para la ECERNEP PERÚ EC-PSVA[6], y para la ECEP PCM .

En el Gráfico 2 se observa la secuencia típica de las fases en una ceremonia de llaves:

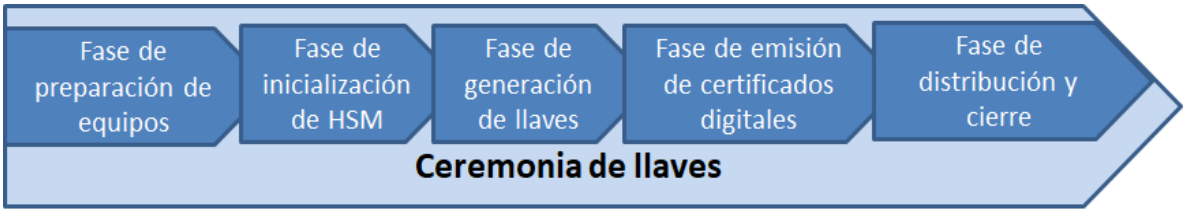

Gráfico 2

A manera de guía en el desarrollo del servicio, el proveedor elaborará un plan de trabajo que incluirá las actividades junto con sus correspondientes entregables conforme se describe en el numeral 6.1.1. Además, como parte del diseño de la ceremonia de llaves, se elaborará un flujo general de la misma que comprenda la secuencia de fases referida contemplando su realización para las entidades de certificación que se encontrarán a cargo de la Secretaría de Gobierno y Transformación Digital (SGTD) conforme se ilustra en el Gráfico 1, bajo cada una de las dos (2) jerarquías PKI mencionadas previamente.

[3] RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública.
[4] También denominado Criptografía de Curva Elíptica (ECC por sus siglas en inglés).
[5] Al hablar de instancias de las nuevas jerarquías PKI del Estado Peruano, nos referimos a cada una de las entidades encerradas con línea punteada en el gráfico del numeral 5.
[6] La EC-PSVA es una instancia de entidad de certificación intermedia o de segundo nivel incluida en el diseño de arquitectura conforme a las buenas prácticas internacionales que mandan que la entidad de certificación raíz no emita certificados digitales a las entidades finales, en este caso a los Prestadores de Servicios de Valor Añadido bajo la modalidad de Autoridad de Sellado de Tiempo (PSVA-TSA), quedando de esta manera la raíz menos expuesta y más protegida.

Para el desarrollo de una ceremonia de llaves se requerirá determinar los roles de los participantes, lo que se reflejará en su diseño y consecuentemente en el *script* o guion que deberá elaborar el proveedor cumpliendo con las exigencias de los documentos referidos en el numeral 3, Normas técnicas, y con las buenas prácticas que determine de acuerdo con su conocimiento y experiencia. Asimismo, establecerá las intervenciones y responsabilidades que corresponden a cada rol.[7] El proveedor asumirá los roles de dirección, coordinación, asesoría y respaldo técnico y procedimental dentro de la ceremonia de llaves, mientras que la PCM-SGTD proveerá el personal para los roles relacionados con la operación de los sistemas criptográficos, la custodia de componentes de llaves, la administración de dominios de seguridad y como testigos.

Asimismo, como parte del servicio, se requerirá la presencia de notario público para las constataciones y certificaciones del caso y la grabación en video de la ceremonia.

El proveedor proporcionará también conforme se refiere en el numeral 6.5. Especificaciones Técnicas (equipos), seis (06) sistemas criptográficos conformados por seis (06) computadoras portátiles y seis (06) dispositivos *Hardware Security Module* (HSM[8]) de escritorio, de los cuales tres (03) corresponderán a cada una de las dos jerarquías PKI previstas.

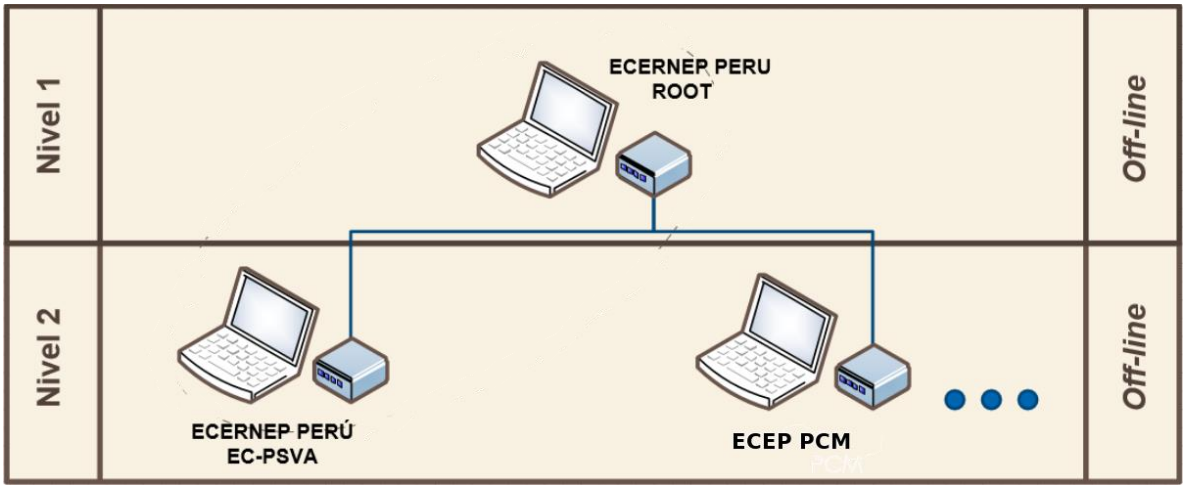

Gráfico 3

Los dispositivos HSM de escritorio a utilizarse para el presente servicio deberán contar con la certificación FIPS 140-2 nivel 3, debiendo asimismo cumplirse las exigencias de esta norma durante el desarrollo de la ceremonia. Además, en la prestación del servicio , y en el diseño y desarrollo de la ceremonia, el proveedor deberá cumplir con los requisitos establecidos en los documentos referidos en el numeral 3, Normas técnicas.

[7] El estándar FIPS 140-2 contempla que el módulo criptográfico o dispositivo HSM deberá soportar cuando menos los siguientes roles:
• Usuario (*User*): Desarrolla servicios generales de seguridad.
• Funcionario Criptográfico (*Crypto Officer*): Lleva a cabo la inicialización criptográfica o funciones de gestión (inicialización del módulo, ingreso/salida de claves o de Parámetros Críticos de Seguridad (CSPs), funciones de auditoría, etc.
• Mantenimiento (*Maintenance*): Hace el mantenimiento físico y/o lógico. Incluyendo diagnósticos. Se incluirá este rol si el módulo soporta servicios de mantenimiento.
Otros estándares, como el ISO 21188, *Public Key Infrastructure for Financial Services – Practices and Policy Framework*, en su Anexo D, CA *key generation ceremony*, refieren un conjunto de roles más amplio para ceremonias de llaves.

[8] HSM son las siglas de Hardware Security Module o Módulo de Seguridad de Hardware.

La ceremonia de llaves y las pruebas de los sistemas criptográficos se desarrollará en las instalaciones de la SGTD ubicada en Calle Schell 310 - Miraflores. Personal de seguridad de la SGTD estará a cargo del control de acceso a dicha área. De manera particular, se restringirá el acceso estrictamente al personal participante de la ceremonia en el día o los días que tome su desarrollo. De igual manera, la PCM-SGTD dispondrá de un ambiente para el almacenamiento de los sistemas criptográficos y elementos accesorios para la ceremonia (laptops, dispositivos HSM, tarjetas inteligentes, cintillos o etiquetas autoadhesivas de seguridad, etc.) facilitando su recepción inmediata y su traslado directo al mismo tanto en el momento de su entrega por parte del proveedor, como en el momento en que se concluya con la ceremonia de llaves y estos deban almacenarse hasta su próximo uso.

Se precisa que el local y los ambientes a utilizarse para las pruebas, operación y almacenamiento de los sistemas criptográficos cuentan con mobiliario, instalaciones eléctricas y con controles de seguridad adecuados. Asimismo, los sistemas criptográficos y elementos accesorios serán acompañados por un representante de la PCM-SGTD en sus traslados desde el momento de su recepción, y para su almacenamiento y su operación conforme al procedimiento a ser coordinado entre el proveedor y la PCM-SGTD.

Los bienes tangibles o intangibles asociados a la prestación del servicio, salvo los recursos a ser asignados por el proveedor para su desarrollo según numeral 6.3, Recursos provistos por el proveedor, pasarán a ser propiedad de la PCM-SGTD.

La prestación del servicio será en idioma español. No obstante, si el personal especializado del proveedor a asignarse a la prestación del servicio no habla ni escribe en idioma español, podrá salvarse esta limitación incluyendo en su propuesta los servicios de traductor e intérprete. En cualquier caso, todos los entregables documentarios a ser utilizados el día del desarrollo o ejecución de la ceremonia se proporcionarán en idioma inglés, mientras que los demás entregables pueden ser proporcionados en idioma español o en idioma inglés.

La ceremonia de llaves que comprende el servicio se deberá llevar a cabo de manera tal que se pueda verificar su desarrollo bajo las más altas medidas de seguridad, abarcando tanto controles de seguridad lógicos como físicos, debiendo cumplirse de manera general las normas y estándares referidos en el numeral 3, Normas técnicas, y con las exigencias dadas en el *Anexo I: Marco de la política de emisión de certificados digitales* de la *Guía de Acreditación de Entidades de Certificación EC, Versión 4.1* en sus secciones *1.2.3. Seguridad en la Gestión del ciclo de vida de las claves de los Certificados de la Entidad de Certificación, 1.2.4. Ciclo de vida del módulo criptográfico de la EC, 1.2.9 Gestión de certificados de EC Subordinadas y certificaciones cruzadas*, y en su provisión *61 Seguridad física y del entorno.* De manera particular, se cumplirá también con lo establecido en la norma europea *ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements,* numeral *6.5.1 Key pair generation and installation* en lo que resulte aplicable.

A la conclusión de la ceremonia, el proveedor proporcionará los documentos generados en éstas debidamente suscritos por los participantes y con certificación notarial, además del video de las grabaciones efectuadas, lo que posibilitará constatar *a posteriori* su desarrollo en conformidad con lo establecido en el presente servicio.

6.1. Actividades

6.1.1. Definición del Plan de trabajo

En coordinación con personal de la PCM-SGTD, el proveedor desarrollará un plan de trabajo. Dicho plan de trabajo incorporará como mínimo un cronograma de actividades que abarcará desde su aprobación por la PCM-SGTD, hasta la culminación del servicio.

En el plan de trabajo se establecerán asimismo los plazos definidos para la provisión de los entregables asociados a cada actividad o prestación, contemplándose como mínimo las etapas y las actividades correspondientes:

a) Etapa inicial
   - Establecimiento y presentación de los equipos de trabajo y de los contactos.
   - Presentación del plan de trabajo.
   - Transferencia de conocimientos en el uso de sistemas criptográficos (según numeral 6.1.2).
   - Definición de los algoritmos criptográficos y de resumen a utilizarse para la generación de llaves y para la emisión de certificados y de listas CRL (según numeral 6.1.3).
   - Desarrollo de perfiles de los certificados digitales y de las listas de certificados cancelados (según numeral 6.1.4).
   - Elaboración del Plan de Administración de Llaves (según numeral 6.1.5).

b) Etapa de diseño
   - Diseño del flujo general de la ceremonia (según numeral 6.1.6).
   - Diseño de la ceremonia de llaves (según numeral 6.1.7).

c) Etapa de entrega de equipos y bienes
   - Entrega de equipos y bienes en general señalados en las Especificaciones Técnicas (equipos) según numeral 6.5.

d) Etapa de desarrollo
   - Desarrollo de la ceremonia de llaves y su ensayo (según numeral 6.1.8).

e) Etapa de pruebas
   - Prueba de emisión de certificados digitales a una ECEP y a un PSVA-TSA (según numeral 6.1.9).
   - Copia de respaldo de llaves (según numeral 6.1.10).

A este respecto, el proveedor designará a un miembro de su personal clave con conocimientos administrativos y de gestión de proyectos quien se encargará de convocar a reuniones periódicas de seguimiento en la ejecución del proyecto a la PCM-SGTD al menos una vez por semana, elaborando el acta correspondiente.

6.1.2. Transferencia de conocimientos en el uso de sistemas criptográficos

Como parte del servicio el proveedor desarrollará actividades para la transferencia de conocimientos referidos a la operación de los sistemas criptográficos que proveerá, contemplando la creación de una jerarquía PKI con una entidad de certificación raíz y una entidad de certificación intermedia. Se incluirá como mínimo los siguientes temas:

- Instalación de sistema operativo licenciado en versión profesional y vigente compatible con el software criptográfico de los dispositivos HSM.
- Instalación del software de operación, conexión y configuración del dispositivo criptográfico HSM en el host.
- Inicialización y configuración del dispositivo HSM.
- Generación del juego de tarjetas *smartcard* para su operación mediante mecanismos de conocimiento dividido m de n.
- Generación de pares de llaves criptográficas pública y privada de las Entidades de Certificación (EC).
- Exportación de llaves privadas de las EC.
- Importación de llaves privadas de las EC.
- Borrado de llaves criptográficas.
- Copia de respaldo cifrado de llaves privadas de las EC en medio de almacenamiento externo.
- Restauración de copia de respaldo de llaves privadas de las EC.
- Emisión de certificados digitales de las EC.
- Emisión de listas CRL de las EC.
- Configuración y respaldo de logs de auditoría del sistema.
- Reinicialización (reseteo) del dispositivo HSM a su configuración de fábrica.
- Cierre y resguardo seguro del sistema criptográfico.

El proveedor efectuará la capacitación sobre los puntos referidos al personal designado por la PCM-SGTD en número de diez (10). La capacitación se efectuará de manera teórica y práctica con un dispositivo HSM y software criptográfico iguales a los que serán provistos como parte del servicio. La capacitación podrá efectuarse de manera presencial en local a ser provisto por la PCM-SGTD, ubicado en Calle Schell 310 - Miraflores, o de manera virtual en consideración al estado de emergencia sanitaria a nivel nacional. La capacitación comprenderá un mínimo de ocho (08) horas lectivas. El proveedor emitirá las constancias de capacitación correspondientes en coordinación con la PCM-SGTD.

El proveedor entregará a la PCM-SGTD:
- Las presentaciones efectuadas en formato MS Power Point.
- La videograbación de la capacitación en formato HD MP4.
- Las constancias de asistencia y capacitación del personal participante de la PCM-SGTD.
- Los instructivos correspondientes a cada uno de los temas desarrollados en formato MS Word que incluirán las instrucciones a seguir y los comandos a ejecutarse en el sistema criptográfico en cada caso.

6.1.3. Definición de los algoritmos criptográficos y de resumen a utilizarse para la generación de llaves y para la emisión de certificados y de listas CRL

El proveedor recomendará los algoritmos criptográficos y de resumen a utilizarse para la generación de llaves y para la emisión de certificados y listas CRL para la entidad de certificación ECERNEP PERÚ ROOT, para la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA, y para la entidad de certificación ECEP PCM. Se desarrollará dos variantes de estos perfiles, una para la jerarquía PKI basada en algoritmos criptográficos RSA (denominada ECERNEP PERÚ ROOT

5) y otra para la jerarquía basada en algoritmos de curva elíptica (denominada ECERNEP PERÚ ROOT 6).

El proveedor deberá referir las versiones vigentes de aquellos estándares contemplados en base a los cuales se estaría recomendando el uso de determinados algoritmos criptográficos y sus parámetros. Se tendrá en cuenta aquellos referidos en el numeral 3, Normas técnicas.

Para el desarrollo de esta actividad, se deberá cumplir con lo establecido en la *Guía de Acreditación de Entidades de Certificación EC, Versión 4.1,* de manera particular contemplando el cuerpo principal del documento, su *Anexo I - Marco de la política de emisión de certificados digitales* y su *Anexo XI - Estándares reconocidos para la acreditación*.

El proveedor entregará a la PCM-SGTD en un documento en formato MS Word las tablas con los algoritmos recomendados añadiendo en cada caso la referencia a los estándares aplicables en versión vigente en los que se sustenta su recomendación y los identificadores de objeto (OID) correspondientes[9].

6.1.4. Desarrollo de perfiles de los certificados digitales y de las listas de certificados cancelados

El proveedor desarrollará los siguientes perfiles de certificados digitales:

- Perfil de certificado digital a emitirse autofirmado por la ECERNEP PERÚ ROOT como entidad de certificación raíz de la jerarquía PKI.
- Perfil de certificado digital a emitirse por la ECERNEP PERÚ ROOT a la ECERNEP PERÚ EC-PSVA como instancia de EC administrada por la ECERNEP.
- Perfil de certificado digital a emitirse por la ECERNEP PERÚ ROOT a la ECEP PCM como instancia de EC administrada por la Presidencia del Consejo de Ministros.
- Perfil de certificados digitales a emitirse por la ECERNEP PERÚ ROOT a las ECEP.
- Perfil de certificados digitales a emitirse por la ECERNEP PERÚ EC-PSVA a los PSVA-TSA.

De igual manera, desarrollará los perfiles de las listas de certificados cancelados (CRL) a emitirse por la entidad de certificación ECERNEP PERÚ ROOT, por la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA, y por la entidad de certificación ECEP PCM.

Se desarrollarán dos versiones de todos estos perfiles, una para la jerarquía PKI basada en algoritmos criptográficos RSA (denominada ECERNEP PERÚ ROOT 5) y otra para la jerarquía basada en algoritmos de curva elíptica (denominada ECERNEP PERÚ ROOT 6).

Para el desarrollo de esta actividad se deberá cumplir con lo establecido en la *Guía de Acreditación de Entidades de Certificación EC, Versión 4.1,* de manera

[9] Los identificadores de objeto para los algoritmos se tienen definidos en documentos como el *RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* y sus actualizaciones o en el repositorio http://oid-info.com.

particular contemplando el cuerpo principal del documento, su *Anexo I - Marco de la política de emisión de certificados digitales* y su *Anexo XI - Estándares reconocidos para la acreditación.*[10] Asimismo, deberán encontrarse adecuados a las exigencias para la incorporación de las jerarquías PKI del Estado Peruano en la lista de confianza de la firma Microsoft, además para la obtención del sello WebTrust y en conformidad con las normas y estándares referidos en el numeral 3, Normas técnicas.

El proveedor entregará a la PCM-SGTD los perfiles de los certificados digitales y de las listas de certificados cancelados. Los entregables serán proporcionados en el "formato de detalle de certificados digitales" y en el "formato de detalle de listas de certificados cancelados (CRL)" a proveerse como parte del diseño de la ceremonia de llaves, tanto en formato MS Word como en el formato electrónico que requiera el sistema criptográfico a utilizarse durante el proceso de emisión de los certificados digitales dentro de la ceremonia de llaves.

6.1.5. Elaboración del Plan de Administración de Llaves

Deberá efectuarse en conformidad con las exigencias respecto de la gestión de llaves establecidas en los documentos pertinentes referidos en el numeral 3, Normas técnicas, de manera particular considerando lo señalado en el *Anexo 2 de la Guía de Acreditación de Entidades de Certificación EC, Requisitos de seguridad para la acreditación.* Este documento se constituirá en insumo de la actividad de Diseño de la ceremonia de llaves, numeral 6.1.7, comprendiendo todo el ciclo de vida de las llaves criptográficas de la entidad de certificación ECERNEP PERÚ ROOT, de la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA, y de la entidad de certificación ECEP-PCM.

El proveedor elaborará y entregará a la PCM-SGTD en formato MS Word el Plan de Administración de Llaves conforme a lo descrito precedentemente.

6.1.6. Diseño del flujo general de la ceremonia de llaves

Deberá diseñarse el flujo general de las fases de la ceremonia a efectuarse conforme se ilustran en el Gráfico 2 teniendo en cuenta la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM, según se visualizan en el Gráfico 1. Se incluirá como mínimo la prueba y preparación de equipos, la generación de las llaves criptográficas, la emisión de los certificados digitales, la emisión de listas CRL, el cierre de la ceremonia y el sellado o resguardo de los sistemas criptográficos (HSM, laptop host y tarjetas *smartcard*) contemplando, además, que las referidas fases deberán repetirse para las dos jerarquías PKI que se tienen previstas, sirviendo de insumo para el desarrollo del *script* o guión de la ceremonia de llaves a diseñarse también como entregables del servicio que brindará.

[10] En la provisión 11 del anexo I de la guía de acreditación se establece que el perfil de los certificados será de la versión X.509 V3 y el de las listas CRL X.509 V2, en conformidad con el estándar ISO/IEC 9594-8 equivalente a la recomendación ITU-T X.509, y guardando conformidad también con la RFC 5280 de la IETF. Se considerará que en la provisión 117 se establece que el arco para los OID a utilizarse para los certificados y políticas de certificación debería provenir de una organización autorizada por ITU, debiendo a su vez contemplarse lo establecido en la vigésima disposición complementaria final, *Gestión de Identificadores de Objetos,* del Decreto Supremo Nº 029-2021-PCM.

El proveedor diseñará y entregará a la PCM-SGTD en formato MS Word, y mediante su correspondiente representación gráfica (diagrama de Gantt, diagrama de flujo u otro que refleje la secuencia y las precedencias), un flujo general de las fases y actividades de la ceremonia a efectuarse teniendo en cuenta las entidades de certificación en la jerarquía PKI, las llaves criptográficas que deberán generarse, los certificados digitales que deberán emitirse y contemplando, además, que las referidas fases y actividades deberán repetirse para las dos jerarquías PKI que se tienen previstas, de manera concordante con los *scripts* o guiones a diseñarse también como entregables del servicio que brindará.

6.1.7. Diseño de la ceremonia de llaves

El diseño de la ceremonia de llaves comprenderá entre los contenidos de su fase de preparación de equipos aspectos como la verificación de su integridad y operatividad, incluyendo los HSM y las laptops que actuarán como *hosts,* la verificación de la integridad y autenticidad del software a instalarse en éstos, el borrado permanente de datos, el formateo e instalación fresca del software necesario para su posterior operación, además de la adecuada configuración y prueba de conectividad entre los hosts y los HSM, todo ello de manera que los sistemas criptográficos queden listos para su operación en las fases sucesivas.

Comprenderá asimismo entre sus contenidos la inicialización de HSMs, la generación de llaves y la emisión de los certificados digitales y primeras CRLs correspondientes a las ECs de cada nueva jerarquía PKI; las actividades de generación y respaldo de los registros de auditoría *(logs)* generados por los sistemas criptográficos; las actividades de distribución tanto de *smartcards*, con su ensobrado y cerrado seguro, como de la documentación generada, la que deberá ser correctamente firmada respetando criterios que posibiliten su auditoría; y las actividades de cierre de la ceremonia, incluyendo el precintado y almacenamiento seguro de *smartcards*, del equipamiento con data sensible, de los dispositivos HSM *off-line* y de la documentación generada.

En el diseño de la ceremonia de llaves, el proveedor deberá garantizar que se contemple lo establecido en las normas técnicas detalladas en el numeral 3, específicamente como mínimo las siguientes:

- El sistema criptográfico únicamente generará llaves de firma bajo, al menos, control dual, requisito que se puede implementar en el propio dispositivo HSM o en el software del sistema[11].
- El sistema criptográfico será operado en un sistema independiente y aislado que no tenga conexión con otros sistemas. El sistema estará desconectado cuando no se precise su uso[12].
- La generación de llaves, y su subsiguiente certificación, se realizará en un entorno físicamente asegurado por roles fiables asignados al personal de la PCM-SGTD bajo, como mínimo, control dual[13] y elementos de conocimiento dividido[14].

[11] CEN/TS 419 261:2015, sección 5.2.5.2.1 [KM1.3]; ETSI EN 319 411-1:2016, sección 6.5.4.a).
[12] CEN/TS 419 261:2015, sección 5.2.5.2.1 [KM1.6].
[13] ETSI EN 319 411-1:2016, sección 6.5.1.a); CPA *Canada WebTrust* for CA 2.2, sección 4.1.
[14] CPA *Canada WebTrust* for CA 2.2, sección 4.1; *CA/Browser Forum Baseline Requirements* 1.4.4, sección 6.1.1.1. y
Guía de Acreditación de Entidades de Certificación EC, Anexo I, provisión 33: "La generación de las claves de la EC deberá ser realizada por personal que pertenezca a la EC, bajo al menos, control de acceso de dos personas y separación de accesos."

Se desarrollará un procedimiento documentado o guion para la realización de la ceremonia de llaves, el que contemplará, al menos, lo siguiente[15]:

- Los roles que participan en la ceremonia de llaves (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.
- La aprobación para la realización de la ceremonia.
- Identificación del hardware criptográfico y los materiales de activación necesarios para la ceremonia.
- Los pasos específicos a realizarse durante la ceremonia, incluyendo los comandos y parámetros a ser digitados por los operadores de los sistemas criptográficos.
- Los requisitos de seguridad física específicos para el local y ambiente donde se desarrollará 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.

Ante la culminación de fases en las que se deba dejar los equipos desatendidos, se contemplará en el diseño el procedimiento de su precintado y el de su almacenamiento en el ambiente físico designado. Se contemplará, asimismo, que al iniciarse una siguiente fase se efectuará la correspondiente verificación de integridad de los elementos precintados.

Además, se identificará aquel equipamiento adicional y accesorios que pudiesen requerirse para el correcto desarrollo de la ceremonia de llaves y la posterior operación de los sistemas criptográficos (extensiones de corriente eléctrica, cables USB o de red, etc.).

Para el desarrollo de esta actividad se deberá cumplir con lo establecido en la *Guía de Acreditación de Entidades de Certificación EC, Versión 4.1,* de manera particular contemplando el cuerpo principal del documento, su *Anexo I - Marco de la política de emisión de certificados digitales* y su *Anexo XI - Estándares reconocidos para la acreditación.*[16]

El proveedor proporcionará a la PCM-SGTD los entregables documentarios necesarios para el desarrollo de la ceremonia de llaves según su propio diseño en formato MS Word, estando comprendidos como mínimo los siguientes:

a) *Script* (guion) de ceremonia que comprenda como mínimo los aspectos referidos en la descripción de la actividad.
b) Formato de cartas de testimonio de participantes (por ejemplo, el personal técnico que preparará el sistema criptográfico).
c) Formatos de cartas de testimonio de testigos para la declaración de aspectos relevantes concordantes con su participación dentro de la ceremonia y observaciones.

[15] ETSI EN 319 411-1:2016, sección 6.5.1.f); *CPA Canada WebTrust for CA* 2.2, sección 4.1.
[16] La Guía de Acreditación de Entidades de Certificación EC, establece en su Anexo I, provisión 33, los requisitos para la generación de llaves de las entidades de certificación.

d) Formato de custodio de componente de acceso a llave que incluirá información de identificación, aseveración de la comprensión de su rol y detalles de la tarjeta *smartcard* asignada.
e) Formato de mapa de llaves que incluirá el detalle de todas las llaves privadas a generarse de las instancias en cada nueva jerarquía PKI del Estado Peruano (la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM).
f) Formato de detalle de certificados digitales a generarse de las instancias de Entidad de Certificación en cada nueva jerarquía PKI del Estado Peruano (la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM).
g) Formato de detalle de listas de certificados cancelados (CRL) a generarse de las instancias de Entidad de Certificación en cada nueva jerarquía PKI del Estado Peruano (la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM).
h) Formato de administrador del dominio de seguridad del HSM que incluirá información de identificación, aseveración de la comprensión de su rol y detalles de la tarjeta *smartcard* asignada.
i) Formato del conjunto de tarjetas del componente del dominio de seguridad que incluirá la relación de las tarjetas *smartcards* y los custodios designados.
j) Formato de control de asistencia de ceremonia.
k) Formato de control de entradas/salidas de ceremonia.
l) Formato de control de registro de equipos.
m) Relación de equipamiento adicional y accesorios a requerirse para la ceremonia.

6.1.8. Desarrollo de la ceremonia de llaves

El desarrollo de la ceremonia de llaves se efectuará de acuerdo con el diseño efectuado por el proveedor según el numeral 6.1.7 siguiendo estrictamente lo establecido en el *script* o guion previamente aprobado por la PCM-SGTD.

El proveedor proporcionará a la PCM-SGTD, como mínimo, los siguientes entregables por impreso que resultarán del desarrollo de la ceremonia de llaves según su propio diseño, debidamente suscritos y con legalización notarial de sus firmas:

a) *Script* (guion) de ceremonia de llaves efectuada firmado por los testigos y por el Director de la ceremonia de llaves.
b) Cartas de testimonio firmadas por los participantes.
c) Cartas de testimonio firmadas por los testigos.
d) Documentos de custodia de componente de acceso a llave firmados por custodios y con certificación de notario público.
e) Documento mapa de llaves firmado por el director de la ceremonia y por los testigos.
f) Documento de detalle de certificados generados firmado por el director de la ceremonia y por los testigos.

g) Documentos de administrador del dominio de seguridad del HSM firmados por las personas designadas y por el Especialista de Seguridad de la Información que determine la PCM-SGTD.
h) Documento del conjunto de tarjetas del componente del dominio de seguridad firmado por el Especialista de Seguridad de Información que determine la PCM-SGTD.
i) Documento de control de asistencia de ceremonia de llaves firmado por los participantes.
j) Documento de control de entradas/salidas de ceremonia de llaves firmado por los participantes.
k) Documentos de control de registro de equipos firmados por los participantes.
l) Copia impresa de los registros de los HSM y/o sistemas criptográficos *(logs)* que reflejen el desarrollo de su operación en la ceremonia de llaves firmada por los testigos.
m) Acta notarial del desarrollo de la ceremonia de llaves.

El proveedor dispondrá de una laptop y de una impresora con los insumos necesarios para efectuar las impresiones y copias que se requiera antes y durante el desarrollo de la ceremonia.

Como resultado o conclusión de la ceremonia, la PCM-SGTD dispondrá como mínimo de lo siguiente:
a) Pares de llaves criptográficas RSA y ECC[17] generadas en los dispositivos HSM correspondientes a la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM de las nuevas jerarquías PKI, en los medios y según las condiciones establecidas en el *script.*
b) Certificados digitales emitidos de la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM de las nuevas jerarquías PKI RSA y ECC, en los medios y según las condiciones establecidas en el *script.*
c) Listas de certificados cancelados (CRLs) iniciales vacías por ser las primeras de la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y la entidad de certificación ECEP PCM de las dos nuevas jerarquías PKI (RSA y ECC), en los medios y según las condiciones establecidas en el *script.*
d) Laptops utilizadas en la ceremonia de llaves como hosts de los HSM de las ECs *off-line* debidamente precintadas para guardarse en lugar seguro, y listas para posteriores utilizaciones dentro de su fase operativa. El precintado se efectuará con etiquetas de sellado numeradas, debiendo dicha numeración constar en el *script* o guion correspondiente.
e) Dispositivos HSM de la entidad de certificación ECERNEP PERÚ ROOT, la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA y de la entidad de certificación ECEP PCM de las nuevas jerarquías PKI utilizados en la ceremonia de llaves debidamente precintados para guardarse en lugar seguro, y listas para posteriores utilizaciones dentro de su fase operativa. El precintado se efectuará con etiquetas de sellado numeradas, debiendo dicha numeración constar en el *script* o guion correspondiente.

[17] Criptografía de Curva Elíptica (en inglés: Elliptic curve cryptography, ECC)

f) Licencias de software correspondientes, en caso se utilice algún software propietario.

En caso los dispositivos criptográficos HSM, laptops (host) y tarjetas *smartcards* destinados a la ejecución de la ceremonia de llaves deban mantenerse en el ambiente físico provisto para su utilización en una fase posterior de la ceremonia, éstos deberán precintarse con etiquetas, bolsas, sobres u otros dispositivos numerados y diseñados para mostrar evidencia de manipulación.

Asimismo, la descripción de los componentes listados en el presente numeral se encuentra detallada en el numeral 6.5, Especificaciones Técnicas (equipos).

En caso de que el ambiente físico destinado para el desarrollo de la ceremonia de llaves deba cerrarse para su utilización en una fase posterior de la ceremonia, manteniéndose en él los equipos en uso, el proveedor deberá precintar sus accesos. La ceremonia de llaves se desarrollará en un ambiente adecuado provisto por la PCM-SGTD con ingresos que posibiliten su cerrado seguro y el correspondiente control de acceso, el que contará con personal de seguridad que lo resguarde las 24 horas del día.

De igual manera, deberá precintarse dichos dispositivos criptográficos HSM, laptops (*hosts*) y tarjetas *smartcards* a la culminación de la ceremonia de llaves. El precintado se efectuará con etiquetas de sellado numeradas, debiendo dicha numeración constar en el *script* o guion correspondiente.

El proveedor incluirá dentro de su propuesta al personal clave que deberá brindar sus servicios profesionales en aspectos de dirección, coordinación, asesoría y respaldo técnico y procedimental en el desarrollo de la ceremonia bajo roles según su propio diseño. En el numeral 6.3, Requisitos a ser provistos por el proveedor, se especifica un mínimo de personal clave que deberán ser asignados por el proveedor para la prestación del servicio.

El proveedor dispondrá asimismo del personal requerido que brinde sus servicios técnicos y profesionales como participantes de la ceremonia en roles de apoyo según su propio diseño a efectos de que se logre su adecuado desarrollo.

Adicionalmente, el proveedor incluirá los servicios de un notario público y de un camarógrafo/técnico en videograbación, se tendrá en cuenta que la determinación precisa de los entregables asociados a éstos dependerá de la duración de la ceremonia según el diseño a efectuarse por el proveedor. La descripción de dichos servicios se realiza de acuerdo con lo siguiente:

a) Servicio de grabación en video de la ceremonia de llaves para efectos de control y auditoría.
   - La cantidad de horas a grabarse dependerá del diseño del *script* o guión para la ceremonia de llaves elaborado por el proveedor y al tiempo que tome la ejecución de la ceremonia.
   - Memorias USB con las grabaciones efectuadas a ser provistas en la capacidad y cantidad necesaria.

- El formato de grabación será a colores, de tipo digital, con alta definición FULL HD MP4 (1920 x 1080 px) y con audio.
- En la videograbación se llevará el registro incrustado en la imagen captada de la fecha y hora o el archivo generado será firmado digitalmente con sello de tiempo a su culminación.
- De producirse alguna interrupción, se comunicará a los participantes a efectos de que paralicen sus actividades hasta que ésta sea retomada.
- La presentación del video deberá ser previamente coordinado y aprobado por la PCM-SGTD.

b) Notario público colegiado
- Deberá encontrarse presente para las constataciones y certificaciones del caso durante el desarrollo de la ceremonia de llaves y para la elaboración del acta correspondiente.
- Validación de la identidad y certificación de firmas de participantes y testigos dentro de los documentos que se generen en el desarrollo de la ceremonia de llaves;
- Elaboración de acta notarial del desarrollo de la ceremonia de llaves debidamente suscrita, lo cual será proporcionado a la PCM-SGTD.

Además, la PCM-SGTD gestionará la participación de dos testigos para la ceremonia.

6.1.9. Pruebas de emisión de certificados digitales a una ECEP y a un PSVA-TSA

Una vez concluida la ceremonia de llaves, el proveedor procederá a efectuar pruebas de emisión y de cancelación o revocación de certificados para una ECEP y una PSVA-TSA. Las pruebas se efectuarán en ambas jerarquías PKI. Los CSR[18] a ser utilizados para esta prueba serán entregados por la PCM-SGTD.

a) El proveedor proporcionará a la PCM-SGTD los certificados digitales para ECEP y PSVA-TSA emitidos como prueba bajo ambas jerarquías PKI.
b) El proveedor proporcionará a la PCM-SGTD las CRLs (listas de certificados cancelados) correspondientes a la ECERNEP PERÚ ROOT, a la instancia de entidad de certificación ECERNEP PERÚ EC-PSVA, y a la ECEP-PCM donde se visualizará los certificados cancelados como parte de esta misma actividad.

6.1.10. Copia de respaldo de software de certificación digital y llaves

Se deberá efectuar copias de respaldo del software de certificación digital y de las llaves criptográficas generadas en la ceremonia de llaves que permitan restaurar las llaves y/o el sistema en caso de destrucción o pérdida. Se tendrá en cuenta para esto lo especificado en las normas técnicas detalladas en el numeral 3, específicamente lo señalado en la *Guía de Acreditación de Entidades de Certificación EC, Versión 4.1,* de manera particular en la *provisión 34, Almacenamiento, respaldo y recuperación de la clave privada de la EC,* de su *Anexo I - Marco de la política de emisión de certificados digitales.*

El proveedor proporcionará a la PCM-SGTD el conjunto de copias de respaldo en un medio de almacenamiento externo (disco duro o memoria USB), las que

[18] Petición de Firma de Certificado (Certificate Signing Request - CSR por sus siglas en inglés)

serán protegidas con al menos los mismos controles de seguridad utilizados para proteger las claves que se encuentran en uso.

Al culminar el desarrollo de las actividades, como resultados esperados la PCM-SGTD dispondrá de las llaves criptográficas, certificados digitales, listas de certificados cancelados resultantes de la ceremonia de llaves en las diferentes instancias de las nuevas jerarquías PKI del Estado Peruano determinadas bajo los alcances del presente servicio, debidamente generados, emitidos o elaborados. Se dispondrá asimismo de los bienes y equipamiento referidos como prestaciones adicionales bajo el numeral 6.5, Especificaciones técnicas (equipos). Ello, en su conjunto y de manera complementaria a la infraestructura tecnológica de la PCM-SGTD, posibilitará el ejercicio de su rol como ECERNEP, y como ECEP PCM bajo la Infraestructura Oficial de Firma Electrónica.

En relación con la ceremonia a efectuarse, se dispondrá además de los correspondientes entregables documentarios y en video que le otorgan formalidad y que se constituyen en evidencias con efectos de auditoría y archivo.

6.2. Metodología

El proveedor efectuará la prestación del servicio en conformidad con el plan de trabajo y las etapas descritas en el Gráfico 4 a continuación:

Gráfico 4

El proveedor elaborará un informe ejecutivo a la culminación de cada etapa, debiendo en él detallarse los entregables provistos en conformidad con lo establecido en el numeral 6.1.1, Plan de trabajo.

6.3. Recursos provistos por el proveedor

- El proveedor designará a un miembro de su personal clave con conocimientos administrativos y de gestión de proyectos (Jefe de Proyecto) a efectos de que en su nombre realice las actividades y coordinaciones del caso con sus contrapartes en la PCM-SGTD con respecto de lo establecido en el numeral 6.2, Metodología, así como en lo referido al numeral 6.1.1, Plan de trabajo.
- El proveedor contará con las herramientas o recursos para el desenvolvimiento de las tareas que ejecutará su personal clave en la prestación del servicio, como, por ejemplo, equipos laptop, una impresora con suministros, acceso a servicio de Internet, herramientas (extensiones eléctricas, cables de interconexión, elementos de precintado), equipos de medición, entre otros necesarios para la adecuada prestación del servicio.
- Los requisitos mínimos para el personal que asigne el proveedor para la prestación del servicio se especifica en el numeral 6.6, Requisitos.

6.4. Recursos y facilidades provistos por la Entidad

La PCM-SGTD proporcionará los siguientes recursos o facilidades para el desarrollo del servicio por parte del proveedor:

- El área o ambiente físico necesario para efectuar la ceremonia de llaves.
- Un ambiente de trabajo para las coordinaciones técnicas y el desarrollo del servicio.
- Personal de la PCM-SGTD que actuará en los roles de la ceremonia como custodios de componentes de llaves, administradores de dominios de seguridad, custodios de componentes de llaves de dominios de seguridad y testigos.

6.5. Especificaciones técnicas (equipos)

Se contemplan los siguientes equipos para el desarrollo de las actividades descritas bajo el numeral 6.1 del presente documento de servicio que deberán proveerse oportunamente para el desarrollo de la ceremonia y que quedarán en propiedad de la PCM-SGTD:

a) Seis (06) dispositivos HSM de escritorio.
   - Certificación FIPS 140-2 Nivel 3 (verificable mediante número o código de certificación). Modo de operación FIPS 140-2 Nivel 3.
   - Licenciamiento y capacidad de ejecutar operaciones criptográficas RSA y de Curvas Elípticas (ECC), operaciones de generación de llaves, de firma, de cifrado y de resumen SHA-1 y SHA-2.
   - Mecanismos de gestión de llaves “m de n”, los que, destinados a las ECs *off-line,* deberán adecuarse a las necesidades operativas de las nuevas jerarquías PKI del Estado Peruano a implementarse y a los requisitos establecidos en las normas técnicas referidas en el numeral 3 del presente documento de servicio.
   - Alimentación de 220V, 60Hz o directamente de la interfaz USB.
   - Lector de componentes de control de acceso (smartcards o tokens criptográficos USB) integrado o separado.
   - Interfaz USB para su comunicación con el host.

b) Seis (06) laptops.
   - Para ser utilizadas como hosts de los dispositivos HSM a proveerse y en los usos que se deriven del desarrollo de la ceremonia a efectuarse.
   - Alimentación de 220V, 60Hz o autovoltaje.
   - Interfaz USB para su comunicación con los dispositivos HSM.
   - Disco duro de estado sólido (SSD) mínimo de 240GB.
   - Procesador mínimo de 4 núcleos reales (físicos).
   - Memoria RAM mínima DDR4 de 8GB.
   - Pantalla mínima de 14”.
   - Módulo Trusted Platform Module TPM 2.0
   - Sistema operativo licenciado en versión profesional y vigente compatible con el software criptográfico de los dispositivos HSM.
   - Asimismo, deberá incluir todo software, y de ser el caso las licencias, que sea necesario para realizar la ceremonia y poder operar los dispositivos después de la ceremonia.

c) Tres (03) discos duros externos.
   - Interfaz USB 3.0

- Capacidad mínima de 500GB compatibles con las laptops a proveer, que podrán utilizarse para copias de respaldo, traslados de solicitudes CSR, etc.

d) Seis (06) unidades de memoria flash USB.
   - Capacidad mínima de 32GB, que podrán utilizarse para copias de respaldo, traslados de solicitudes CSR, etc.

e) Ciento veinte (120) componentes de control de acceso (smartcards o tokens criptográficos USB) para gestión, administración y/o operación de los HSM (es decir, veinte por cada HSM).

El proveedor entregará una Carta de Garantía del Fabricante y una Carta de Soporte Técnico en favor de la PCM-SGTD para los equipos HSM (literal *a*) donde consten las condiciones de garantía y de soporte técnico que éste ofrece para los mismos, debiendo comprender un plazo mínimo de un (01) año. Dichas cartas deberán proporcionarse al momento de la entrega del producto 6; no obstante, en la presentación de la oferta deberán adjuntar una carta de autorización del fabricante. Para el caso del soporte técnico, deberá contemplarse el acceso a una plataforma web para el registro de tickets ilimitado con una disponibilidad de 8x5, los mismos que podrán ser atendidos en idioma español o inglés.

Para el caso de las laptops y discos duros (literales de la *b* hasta la *c*) el proveedor entregará una Carta de Garantía del Fabricante o del proveedor y una Carta de Soporte Técnico en favor de la PCM-SGTD donde consten las condiciones de garantía y de soporte técnico que éste ofrece para los mismos, debiendo comprender un plazo mínimo de tres (03) años. Dichas cartas deberán proporcionarse al momento de la entrega del producto 6. Para el caso del soporte técnico, deberá contemplarse el acceso a una plataforma web para el registro de tickets ilimitado con una disponibilidad de 8x5, los mismos que podrán ser atendidos en idioma español o inglés.

En el caso de las unidades de memoria USB (literal d) deberá proporcionar una Carta de Garantía del Fabricante o del proveedor donde consten las condiciones de garantía que ofrece para estos, dicha carta será proporcionada al momento de la entrega del producto 6, debiendo comprender un plazo mínimo de un (01) año.

Los equipos y bienes (literales de la *a)* hasta la *e*)) deberán ser nuevos, sin uso, y de la versión más reciente e incorporan todas las últimas mejoras en cuanto a diseño y funcionamiento a la fecha de presentación de la propuesta del proveedor (con fecha de fabricación no mayor a 01 año).

La atención por parte del proveedor para la ejecución de la garantía en caso de fallas reportadas por la PCM-SGTD debe darse con un tiempo de respuesta máxima de 04 horas, con cobertura 24x7 (incluyendo sábados, domingos y feriados) los 365 días del año. Si hubiera la necesidad de realizar un mantenimiento al equipo fuera de las instalaciones de la PCM-SGTD, el proveedor reemplazará con otro equipo igual o con características superiores durante el tiempo del mantenimiento.

En caso de la ejecución de la garantía, el proveedor deberá asumir los costos asociados al traslado del equipo a las instalaciones del fabricante, así como el retorno de este (o de un nuevo equipo de ser el caso) a las instalaciones de la PCM-SGTD.

Asimismo, el proveedor deberá presentar un informe de ejecución de garantía, en el cual detalle la ejecución de la garantía por parte del fabricante, así como también debe indicar el modelo, número de serie del equipo, y las pruebas realizadas por el fabricante.

NOTAS:

Para la prestación del servicio el proveedor proveerá:

a) Elementos de precintado como etiquetas, bolsas, sobres o cintillos numerados y *antitampering* para su utilización en dispositivos HSM, laptops, dispositivos de almacenamiento, entre otros, provistos para la prestación del servicio, al igual que para las puertas y accesos al ambiente provisto por la PCM-SGTD donde se efectuará la ceremonia. Se deberá incluir tres juegos adicionales de elementos de precintado para usos futuros de la SGTD.
b) Extensiones eléctricas y cables de interconexión para los equipos a proveerse según se requiera para la prestación del servicio.
c) De considerar el proveedor en la etapa de diseño elementos adicionales no contemplados en el presente documento, éstos deberán ser provistos a la PCM-SGTD sin costo adicional alguno.
d) Las licencias del software que necesite instalar el proveedor para ejecutar la ceremonia de llaves en las laptops que actuarán como hosts de los HSMs deberán emitirse a nombre de la PCM y serán de vigencia perpetua.
e) En el caso de uso de software propietario, se otorgará el correspondiente licenciamiento perpetuo a nombre de la PCM.
f) En caso de instalarse software libre, tratándose de un sistema operativo el proveedor efectuará la suscripción correspondiente a nombre de la PCM por un período mínimo de un año.
g) Bajo cualquier variante del software que se instale y utilice para ejecutar la ceremonia de llaves se cumplirá con dejarlo habilitado para su uso y operación posterior a la prestación del servicio por personal de la PCM-SGTD en las distintas labores relacionadas con el ciclo de vida de los dispositivos HSM.

6.6. Requisitos

a) Experiencia general:
   - Experiencia general mínima de cinco (05) servicios en entidades públicas o privadas en los últimos 05 años, serán válidos experiencias en servicios o consultorías de Tecnologías de Información, por ejemplo, Ceremonia de llaves o claves de infraestructura pública o Servicios de TI o Servicio de provisión de plataforma en la nube o servicios similares.
   - El proveedor deberá acreditar un monto facturado acumulado equivalente a S/. 500,000.00 (Quinientos mil y 00/100 soles) por la contratación de servicios en los últimos cinco (05) años.

b) Experiencia específica:
   - Experiencia específica mínima de tres (03) servicios relacionados a ceremonia de llaves o claves, ceremonia de infraestructura de llave pública, o ceremonia de infraestructura de certificación digital o implementación de plataformas de firma digital o ejecución de auditorías para entidades de certificación o servicios de TI para servicios de certificación digital PKI o servicio de provisión de plataforma en la nube.

La acreditación y/o sustentación de la experiencia, deberá ser a través de contratos, órdenes de servicio u otra documentación que permita acreditar fehacientemente la experiencia solicitada.

El proveedor a fin de garantizar el cumplimiento y desarrollo correcto de las actividades y la entrega de los productos deberá contar con por lo menos el siguiente personal clave (no pudiendo una misma persona ejercer más de un rol):

(i) Un (01) Jefe del Proyecto
(ii) Un (01) Director de la Ceremonia de Llaves
(iii) Un (01) Especialista Técnico en Ceremonia de Llaves

Rol del Personal Clave

a) Jefe de Proyecto
El proveedor deberá designar a un miembro de su personal con conocimientos administrativos y de gestión de proyectos a efectos de que coordine la ejecución del cronograma y el plan de trabajo con sus contrapartes en la PCM-SGTD.

b) Director de la Ceremonia de Llaves
El proveedor designará a un miembro de su personal para que ejerza el rol de Director de Ceremonias, el que primeramente diseñará y luego liderará la ejecución de la ceremonia de llaves leyendo el *script* o guión, asegurándose que los participantes siguen el procedimiento establecido y de que se toma nota de cualquier posible desviación. A su vez, dirigirá el desarrollo del ensayo de la ceremonia de llaves y participará de la capacitación.

c) Especialista Técnico en Ceremonia de Llaves
El proveedor designará cuando menos a un especialista técnico para que desarrolle un rol activo en lo concerniente a la preparación de los dispositivos HSM a proveerse como parte del presente servicio, a la preparación de las laptops, impresora y otros equipos a proveerse, quedando estos listos para su operación durante el desarrollo de la ceremonia de llaves y las pruebas establecidas. A su vez, apoyará y asesorará en el desarrollo de la ceremonia a los operadores de los sistemas criptográficos y participará del ensayo de la ceremonia de llaves y de la capacitación.

Perfil del Equipo Clave requerido

Jefe de Proyecto

a) Formación Académica
- Profesional titulado en ingeniería de sistemas o informática o industrial o economía o administración.
- Estudios relacionados a gestión de proyectos de tecnologías de la información que deben tener como mínimo una duración de 20 horas, y la constancia respectiva puede ser emitida por instituciones nacionales o internacionales.
- Se aceptan estudios internacionales.

b) Experiencia
- Experiencia general mínima de cinco (05) servicios en el sector público o privado, vinculado a su especialidad.
- Experiencia específica mínima de dos (02) servicios relacionados a tecnologías de la información.
- Experiencia específica mínima de dos (02) servicios relacionados a la dirección o gerencia o jefatura o coordinación en proyectos de tecnologías de la información.

Director de la Ceremonia de Llaves

a) Formación Académica
- Profesional titulado en ingeniería de sistemas o informática o tecnologías de la información o ciencias de la computación o electrónica o telecomunicaciones o abogado.
- Estudios relacionados a seguridad de la información o ISO 27001 que deben tener como mínimo una duración de 40 horas, y pueden ser emitidos por instituciones nacionales o internacionales.
- En el caso de títulos profesionales obtenidos en el extranjero no es obligatorio la revalidación por SUNEDU, y en caso de estar en un idioma diferente al español, deberá acompañarse una traducción simple.

b) Experiencia
- Experiencia general mínima de tres (03) servicios en el sector público o privado, vinculado a su especialidad.
- Experiencia específica mínima de un (01) servicio como director o maestro en ceremonia de llaves de una Autoridad de Certificación de entidades financieras, entidades públicas, entidades emisoras de certificados digitales TLS, nacionales o extranjeras.

Especialista Técnico en Ceremonia de Llaves

a) Formación Académica
- Profesional titulado en ingeniería de sistemas o informática o tecnologías de la información o ciencias de la computación o electrónica o telecomunicaciones.
- Estudios relacionados a dispositivos criptográficos HSM o seguridad de la información o ISO 27001 que deben tener como mínimo una duración de 40 horas, y pueden ser emitidos por instituciones nacionales o internacionales.
- En el caso de títulos profesionales obtenidos en el extranjero no es obligatorio la revalidación por SUNEDU, y en caso de estar en un idioma diferente al español, deberá acompañarse una traducción simple.

b) Experiencia
- Experiencia general mínima de tres (03) servicios en el sector público o privado, vinculado a su especialidad.
- Experiencia específica mínima de un (01) servicio relacionado a la operación o gestión de dispositivos HSM o seguridad de la información o firma electrónica o digital o infraestructura de llave pública (PKI) o ceremonias de llaves, pudiendo haber ejercido como coordinador o responsable o especialista técnico.

Queda a discreción del proveedor proponer un mayor número de personal clave o no clave. No obstante, el costo deberá estar previsto en el costo total del servicio.

6.7. Productos Esperados

En función al desarrollo de las actividades señaladas en los numerales precedentes , el servicio contempla la presentación de 07 productos, según se detalla a continuación:

N°.	Producto	Plazo	Plazo para otorgar conformidad y/u observaciones	Plazo para subsanar observaciones
1	**Producto 1:** Plan de Trabajo que incorpora como mínimo un cronograma de actividades que abarcará desde su aprobación por la PCM-SGTD hasta la culminación del servicio, y conforme a lo descrito en el numeral 6.1.1 del presente Servicio.	Hasta los siete (07) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 05 días calendario desde el día siguiente hábil de su recepción del respectivo producto en la Unidad Ejecutora 018.	Hasta 05 días calendario a partir del día siguiente hábil de notificado al proveedor.
2	**Producto 2:** Documento que contiene la definición de los algoritmos criptográficos y de resumen a utilizarse para la generación de llaves y para la emisión de certificados y de listas CRL, y conforme a lo descrito en la actividad 6.1.3 del presente servicio.	Hasta los quince (15) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 07 días calendario desde el día siguiente hábil de su recepción del respectivo producto en la Unidad Ejecutora 018.	Hasta 07 días calendario a partir del día siguiente hábil de notificado al proveedor.
3	**Producto 3:** a) Perfiles de los certificados digitales y de las listas de certificados cancelados, conforme a lo descrito en la actividad 6.1.4 del presente servicio. b) Plan de Administración de Llaves conforme a lo descrito en la actividad 6.1.5 del presente Servicio.	Hasta los treinta (30) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 10 días calendario desde el día siguiente hábil de su recepción del respectivo producto en la Unidad Ejecutora 018.	Hasta 10 días calendario a partir del día siguiente hábil de notificado al proveedor.
4	**Producto 4:** Transferencia de conocimiento en el uso de sistemas criptográficos y conforme a lo descrito en la actividad 6.1.2 del presente servicio.	Hasta los cincuenta (50) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 10 días calendario desde el día siguiente hábil de su recepción del respectivo producto en la Unidad Ejecutora 018.	Hasta 10 días calendario a partir del día siguiente hábil de notificado al proveedor.
5	**Producto 5:** a) Documento que contiene el flujo general de las fases y actividades de la ceremonia de llaves, y su correspondiente representación gráfica (diagrama de Gantt, diagrama de flujo u otro que refleje la secuencia y las precedencias), y conforme a lo descrito en la actividad 6.1.6 del presente Servicio. b) Documentación necesaria para el desarrollo de la ceremonia de llaves, conforme a lo descrito en la actividad 6.1.7 del presente Servicio.	Hasta los sesenta y cinco (65) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 10 días calendario desde el día siguiente hábil de su recepción del respectivo producto en la Unidad Ejecutora 018.	Hasta 10 días calendario a partir del día siguiente hábil de notificado al proveedor.
6	**Producto 6:** Equipos y bienes conforme a lo descrito en el numeral 6.5 del presente Servicio.	Hasta los setenta y seis (76) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 10 días calendario desde el día siguiente hábil de su recepción del respectivo producto en la Unidad Ejecutora 018.	Hasta 10 días calendario a partir del día siguiente hábil de notificado al proveedor.
7	**Producto 7:** a) Desarrollo de la ceremonia de llaves y su ensayo conforme a lo descrito en la actividad 6.1.8 del presente Servicio.	Hasta los noventa (90) días calendario, contados a partir del día siguiente hábil de suscrito el contrato.	Hasta 10 días calendario desde el día siguiente hábil de su recepción del respectivo producto	Hasta 10 días calendario a partir del día siguiente hábil

N°.	Producto	Plazo	Plazo para otorgar conformidad y/u observaciones	Plazo para subsanar observaciones
	b) Prueba de emisión de certificados digitales a una ECEP y a un PSVA-TSA bajo ambas jerarquías PKI, conforme a lo descrito en la actividad 6.1.9 del presente Servicio. c) Conjunto de copias de respaldo en un medio de almacenamiento externo USB, las que serán protegidas con al menos los mismos controles de seguridad utilizados para proteger las claves que se encuentran en uso, conforme a lo descrito en la actividad 6.1.10 del presente Servicio.		en la Unidad Ejecutora 018.	de notificado al proveedor.

Para la conformidad técnica, el proveedor presentará los productos y los documentos de pago respectivos mediante carta dirigida a la UE 018 a cargo del Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas a Nivel Nacional (PROMSACE), con atención al Área Usuaria correspondiente, haciendo referencia al número de documento contractual, servicio contratado y al Proyecto, de forma electrónica a la mesa de partes virtual: **tramitevirtual@promsace.gob.pe**, hasta el levantamiento del estado de emergencia sanitaria y/o hasta cuando establezca el Estado Peruano y/o hasta cuando lo establezca el Proyecto, luego del término de lo establecido por el Estado Peruano y/o el Proyecto el Área Usuaria comunicará vía correo electrónico la fecha a partir de la cual la presentación se realizará a través de la Mesa de Partes del PROMSACE, sito en la Calle Las Flores 375, San Isidro, Lima en horario comprendido entre las 8:30 a.m. y las 4:30 p.m., de Lunes a Viernes.

En caso de presentar una observación, el proveedor deberá subsanar las observaciones en los plazos indicados en este numeral. Asimismo, de existir segunda observación, la entidad podrá rescindir el contrato.

6.8. Lugar

El servicio será prestado en la ciudad de Lima. Para ello se programarán reuniones virtuales y/o presenciales cuando corresponda y en el marco de las disposiciones vigentes de la emergencia sanitaria nacional.

Asimismo, el proveedor podrá prestar sus servicios en las oficinas de la Secretaría de Gobierno y Transformación Digital, previa coordinación con la Secretaría de Gobierno y Transformación Digital.

6.9. Plazo

El plazo del servicio tendrá una duración de noventa (90) días calendario, como máximo, contados a partir del día siguiente hábil de suscrito el contrato y según se detalla en el numeral 6.7 del presente documento.

6.10. Presupuesto del Servicio

El costo total estimado del servicio asciende a S/. 500,000.00 (Quinientos mil con 00/100 Soles) incluidos los impuestos de ley que serán pagados según se detalla en el numeral 6.12 del presente documento.

El servicio es a todo costo.

6.11. Supervisión y Conformidad

La supervisión y la coordinación de la prestación del servicio estará a cargo del equipo técnico designado por la Subsecretaría de Política y Regulación Digital.

Previo informe favorable de la Subsecretaría de Política y Regulación Digital, la conformidad de servicio será emitida por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros quien correrá traslado de dicha conformidad, al área administrativa de la Unidad Ejecutora del Proyecto.

6.12. Forma de pago

Los pagos al contratista serán de la siguiente manera:

CONCEPTO	% DE PAGO
A la entrega y conformidad del Producto N° 1	5%
A la entrega y conformidad del Producto N° 2	5%
A la entrega y conformidad del Producto N° 3	10%
A la entrega y conformidad del Producto N° 4	10%
A la entrega y conformidad del Producto N° 5	10%
A la entrega y conformidad del Producto N° 6	30%
A la entrega y conformidad del Producto N° 7	30%
Total	**100%**

6.13. Penalidades

Aplican las penalidades por mora en la ejecución del servicio. En caso de retraso injustificado del proveedor en la ejecución de las prestaciones objeto del contrato, el Contratante le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplicará hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente o, de ser el caso, del ítem que debió ejecutarse.
La penalidad se aplica, automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$Penalidad\ diaria = \frac{0.10 \times Monto\ vigente}{F \times Plazo\ vigente\ en\ días}$$

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F =0.40.

b) Para plazos mayores a sesenta (60) días:
   b.1) Para bienes, servicios en general y consultorías: F = 0.25
   b.2) Para obras: F = 0.15

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato o ítem que debió ejecutarse o, en caso de que estos involucran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En ese último caso, la calificación del retraso como justificado por parte del Contratante no da lugar al pago de gastos generales ni costos directos de ningún tipo

Esta penalidad será deducida de los pagos a cuenta, del pago final o en la liquidación final.

Asimismo, de existir retraso injustificado en el levantamiento de observaciones, se aplicará la penalidad por los días de atraso conforme al presente numeral.

7. CONFIDENCIALIDAD

El proveedor deberá declarar que conoce y acepta expresamente, previo a la firma del Contrato; el secreto industrial y/o información confidencial consistente en la totalidad de la tecnología, datos, especificaciones, sistemas de cómputo, métodos, procesos y en general; dado que todos los aspectos relacionados con el producto materia del servicio son de propiedad de la Subsecretaría de Política y Regulación Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, y en tal virtud, la divulgación, comunicación, transmisión o utilización para beneficio de cualquier persona distinta a la Subsecretaría de Política y Regulación Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, así como la grabación, duplicado o cualquier otra forma de reproducción de cualquier información a la que tenga acceso en virtud de las actividades que realice vinculado a la Subsecretaría de Política y Regulación Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros será considerada ilegal. El proveedor acepta que será responsable por los daños y perjuicios que pudieran ocasionarse a la Subsecretaría de Política y Regulación Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, como consecuencia de cualquier infracción de confidencialidad.

8. PROPIEDAD INTELECTUAL

El proveedor aceptará expresamente que toda la documentación, información e instalación realizada para la Subsecretaría de Política y Regulación Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, son de propiedad de la Subsecretaría de Política y Regulación Digital de la Secretaría de Gobierno y Transformación Digital y por ende de la Presidencia del Consejo de Ministros (PCM).

9. SEGUROS

El proveedor será responsable de asumir las obligaciones que contraiga con su personal clave y no clave, sean éstas laborales, personales o de cualquier índole; estando eximido el Contratante de cualquier responsabilidad en caso de accidentes, daños, mutilaciones o muerte de alguno de ellos, que pudieran ocurrir durante el desarrollo del servicio. Estos riesgos deberán ser cubiertos íntegramente por las pólizas de seguros pertinentes que el proveedor deberá contratar.

Asimismo, el proveedor está obligado a implementar a todo costo, durante toda la ejecución de la contratación, los protocolos sanitarios vigentes que le correspondan.