CONVENIO DE COOPERACIÓN INTERINSTITUCIONAL Y PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN DIGITAL PARA LA IMPLEMENTACIÓN DE CERTIFICADOS DE FIRMA ELECTRÓNICA AVANZADA ENTRE LA DIRECCIÓN DE GESTIÓN POR RESULTADOS (DIGER) Y TRIBUNAL SUPERIOR DE CUENTAS (TSC)

NOSOTROS, **ELMER MANUEL FERRERA PADILLA**, mayor de edad, hondureño, casado, con Documento Nacional de Identificación número 0801-1986-09078 y domicilio profesional en el Despacho Ministerial de la Dirección de Gestión por Resultados (DIGER), situada en Boulevard Kuwait, contiguo al Banco Central de Honduras, CA-6, Tegucigalpa, Municipio del Distrito Central, actuando en su condición de Director Ejecutivo con rango de Secretario de Estado de la Dirección de Gestión por Resultados (DIGER), nombrado mediante Acuerdo Ejecutivo Número 230-2026 de fecha tres (03) de marzo de dos mil veintiséis (2026), quien para efectos del presente Convenio se denominará **"LA DIGER"**, como Prestador de Servicios de Certificación debidamente habilitado según Certificado de Acreditación número 001, Tomo: 006, Folio: 001, emitido por la Dirección General de Propiedad Intelectual del Instituto de la Propiedad (Autoridad Administrativa Competente - AAC), de fecha veintidós (22) de octubre del año dos mil veinticinco (2025); conforme a la Ley Sobre Firmas Electrónicas (Decreto No. 149-2013), su Reglamento (Acuerdo Ejecutivo No. 41-2014) y demás normativa aplicable; Y POR OTRA PARTE, **RICARDO ALFREDO MONTES NAJERA** mayor de edad, mayor de edad, casado, Abogado, de este domicilio, portador del Documento Nacional de Identificación numero 0101-1977-00207, actuando en condicion de Presidente y Representante Legal del Tribunal Superior de Cuentas, electo por el Soberano Congreso Nacional, mediante Decreto No. 21-2024 publicado en el diario oficial La Gaceta edicio n nu mero 36,473 de fecha 29 de febrero del año 2024 y facultado para este acto, que en lo sucesivo se denominara, **TRIBUNAL SUPERIOR DE CUENTAS**, quien en lo sucesivo se denominará **"LA ENTIDAD"**; manifestamos haber convenido en celebrar el presente CONVENIO DE COOPERACIÓN Y PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN DIGITAL, sujeto a los siguientes considerandos y cláusulas:

CONSIDERANDOS

CONSIDERANDO: Que mediante Decreto Ejecutivo PCM-05-2022, publicado en el Diario Oficial La Gaceta en fecha seis (06) de abril de dos mil veintidós (2022), el Consejo de Ministros creó la Dirección de Gestión por Resultados (DIGER) como un ente desconcentrado de la Presidencia de la República, dirigido por un funcionario con rango de Secretario(a) de Estado.

CONSIDERANDO: Que mediante Acuerdo Ejecutivo Número 230-2026 de fecha tres (03) de marzo de dos mil veintiséis (2026), se nombró al Ingeniero Elmer Manuel Ferrera Padilla en el cargo de Director Ejecutivo con rango de Secretario de Estado de la Dirección de Gestión por Resultados (DIGER), con facultades legales suficientes para aprobar y ejecutar actos administrativos de representación institucional.

CONSIDERANDO: Que mediante Decreto Ejecutivo PCM-004-2026, publicado en el Diario Oficial La Gaceta en fecha veinticinco (25) de febrero de dos mil veintiséis (2026), se amplían las funciones de la DIGER, la cual es responsable de rectorar, ejecutar, supervisar, coordinar y administrar el marco de planes, políticas, programas y proyectos en materia digital del sector público, incluyendo conectividad, trámites, plataformas digitales, ciberseguridad y tecnologías emergentes.

CONSIDERANDO: Que el Contrato de Préstamo No. 4942/BL-HO, suscrito el diecisiete (17) de marzo de dos mil veintiuno (2021) entre el Banco Interamericano de Desarrollo (BID) y el Gobierno de la República de Honduras, aprobado mediante Decreto Legislativo No. 43-2021, financia la ejecución del "Proyecto de Transformación Digital para una Mayor Competitividad"; y que mediante Decreto Ejecutivo PCM-28-2022, publicado en La Gaceta el veintiséis (26) de noviembre de dos mil veintidós (2022), se designó a la DIGER como organismo ejecutor de dicho proyecto.

CONSIDERANDO: Que conforme al numeral 5) del artículo 8 de la Ley de Contratación del Estado, están excluidos del ámbito de aplicación de dicha Ley los contratos o convenios de colaboración que celebre el Gobierno Central con instituciones descentralizadas,

municipalidades u otros organismos públicos, o los que estos celebren entre sí; exclusión aplicable cuando LA ENTIDAD sea una entidad de derecho público, sin perjuicio de que, cuando LA ENTIDAD sea de derecho privado, el presente instrumento se sujete al Código Civil, Código de Comercio y a las condiciones comerciales específicas pactadas.

CONSIDERANDO: Que el artículo 5 de la Ley Sobre Firmas Electrónicas (Decreto Legislativo No. 149-2013) autoriza a los Poderes del Estado, instituciones públicas y particulares a utilizar firmas electrónicas en documentos electrónicos; y que su artículo 6 establece que los actos y contratos otorgados mediante firma electrónica producirán los mismos efectos jurídicos y probatorios que los celebrados por escrito en soporte de papel.

CONSIDERANDO: Que mediante Resolución número 001-2025, la Dirección General de Propiedad Intelectual del Instituto de la Propiedad, como Autoridad Administrativa Competente (AAC), otorgó a la DIGER la habilitación como Autoridad Certificadora y Prestador de Servicios de Certificación.

CONSIDERANDO: Que la DIGER cuenta con una infraestructura de certificación digital que cumple con los estándares ETSI EN 319 411, ISO/IEC 27001, NIST SP 800-53 y el marco RFC 3647, permitiendo ofrecer servicios seguros de emisión de certificados y sellado de tiempo.

CONSIDERANDO: Que la emisión y uso de certificados digitales requiere delimitar obligaciones técnicas, jurídicas y de seguridad entre las partes, reguladas complementariamente mediante la Declaración de Prácticas de Certificación (CPS) y la Política de Certificación (CP) de LA DIGER.

POR TANTO: Las partes acuerdan suscribir el presente Convenio bajo las siguientes:

CLÁUSULAS DEL CONVENIO

CLÁUSULA PRIMERA: OBJETO DEL CONVENIO

El presente Convenio tiene por objeto establecer el marco de colaboración, coordinación y prestación de servicios entre LA DIGER, en su calidad de Prestador de Servicios de

Certificación (PSC) habilitado, y LA ENTIDAD, para la emisión, gestión, administración, renovación, suspensión, rehabilitación y revocación de certificados digitales de **Firma Electrónica Avanzada** destinados al personal autorizado por LA ENTIDAD, fortaleciendo la seguridad, autenticidad, integridad, trazabilidad y el no repudio en sus procesos institucionales.

En ese sentido, el presente instrumento comprenderá, de manera inicial y progresiva, el desarrollo, implementación y fortalecimiento tambien de otros proyectos tecnológicos relacionados con la digitalización y sistematización de datos institucionales, incluyendo, entre otros:

1) **Integración de la Billetera Digital:** Incorporar la plataforma de la billetera digital ciudadana dentro del ecosistema de trámites del Tribunal Superior de Cuentas como el instrumento oficial de validación y autenticación de la identidad digital del ciudadano.
2) **Acompañamiento Técnico:** Reconocer al Tribunal Superior de Cuentas como una institución acompañante clave de la DIGER, brindando apoyo técnico y tecnológico en el diseño e implementación de futuros proyectos de transformación digital a nivel del Estado.
3) **Impulso a la Transparencia y Gobierno Digital:** Integrar, evaluar y ejecutar de manera conjunta las iniciativas y propuestas tecnológicas presentadas por el Tribunal Superior de Cuentas que estén orientadas al fortalecimiento del gobierno digital y la transparencia institucional.
4) **Interconexión Segura de Datos:** La conexión e intercambio de información con otras instituciones para el consumo seguro de datos por parte del Tribunal Superior de Cuentas.
5) **Salvaguarda de la Información:** Asegurar que todo intercambio, tratamiento y consumo de datos interinstitucionales se realice bajo los estándares de seguridad y ciberseguridad actuales dictados por las normas vigentes de la DIGER, protegiendo la confidencialidad e integridad de la información de ambas instituciones.

CLÁUSULA SEGUNDA: ALCANCE Y MODALIDAD TÉCNICA DEL SERVICIO

LA DIGER proporcionará los servicios de certificación digital bajo las modalidades de **Firma Remota (en la Nube)** y **Certificado Digital en Software (.p12)**, según la naturaleza del trámite y las necesidades operativas acordadas entre las partes:

1. **Firma Remota (en la Nube):** Las claves privadas asociadas a estos certificados digitales se generarán, custodiarán y utilizarán de forma centralizada dentro de la infraestructura de Módulos de Seguridad de Hardware (HSM) de LA DIGER. En esta modalidad no se entregarán dispositivos criptográficos físicos (tokens o tarjetas inteligentes) y el acceso por parte del titular se realizará exclusivamente mediante mecanismos de autenticación robusta o de doble factor (MFA/2FA) en la plataforma.
2. **Certificado Digital en Software (.p12):** LA DIGER generará y emitirá el certificado en un contenedor criptográfico descargable en formato `.p12` (o equivalente). En esta modalidad, la custodia, protección de la contraseña y uso seguro del archivo y de su clave privada serán de exclusiva responsabilidad de LA ENTIDAD o del titular asignado a partir de su entrega o descarga.

CLÁUSULA TERCERA: MARCO DOCUMENTAL Y ANEXOS VINCULANTES

Forman parte integrante, obligatoria y vinculante del presente Convenio los siguientes documentos:

1. **Anexo I:** Glosario de Términos y Definiciones Técnico-Legales.
2. La Declaración de Prácticas de Certificación (CPS) y la Política de Certificación (CP) de LA DIGER vigentes.
3. El documento de "Términos y Condiciones de Uso del Certificado Digital" suscrito por cada titular.
4. El Anexo de Condiciones Comerciales (únicamente cuando LA ENTIDAD sea una persona jurídica de derecho privado).

En caso de divergencia técnica u operativa entre este Convenio y la CPS/CP de LA DIGER, prevalecerá lo establecido en esta última.

CLÁUSULA CUARTA: NATURALEZA JURÍDICA Y CONTRAPRESTACIÓN

Cuando LA ENTIDAD sea una institución pública, el presente instrumento revestirá la naturaleza de convenio de cooperación interinstitucional sin generar contraprestación económica. Cada parte asumirá los gastos derivados del cumplimiento de sus obligaciones con cargo a sus respectivos presupuestos.

Cuando LA ENTIDAD sea una persona jurídica de derecho privado, el instrumento se regirá como un contrato de prestación de servicios sujeto al pago de las tarifas estipuladas en el Anexo de Condiciones Comerciales.

CLÁUSULA QUINTA: VIGENCIA Y TERMINACIÓN ANTICIPADA

El presente Convenio tendrá una duración de tres (3) años a partir de la fecha de su firma, prorrogable automáticamente por períodos iguales, salvo manifestación en contrario enviada por escrito con al menos treinta (30) días de anticipación al vencimiento.

Las partes podrán dar por terminado el convenio anticipadamente por: (a) Mutuo acuerdo; (b) Caso fortuito o fuerza mayor debidamente comprobado que imposibilite la prestación del servicio por más de treinta (30) días calendario; (c) Decisión unilateral notificada por escrito con treinta (30) días de anticipación; o (d) Incumplimiento grave de las obligaciones sin subsanar dentro de los diez (10) días hábiles posteriores al requerimiento formal.

CLÁUSULA SEXTA: CESE DE ACTIVIDADES DE LA DIGER COMO PRESTADOR

En caso de cese de actividades, suspensión, cancelación o no renovación de la acreditación de LA DIGER como Prestador de Servicios de Certificación por parte de la Autoridad Administrativa Competente (AAC/IP), LA DIGER notificará por escrito a LA ENTIDAD con al menos treinta (30) días calendario de anticipación. En tal caso, se procederá a la revocación ordenada de los certificados emitidos, garantizando la transferencia o

conservación segura del registro de trazabilidad y firmas emitidas con anterioridad, sin que ello genere penalidades financieras entre las partes.

CLÁUSULA SÉPTIMA: DESIGNACIÓN DE ENLACES

Dentro de los quince (15) días hábiles posteriores a la firma, cada parte designará mediante oficio o comunicación formal a un enlace administrativo y a un enlace técnico, indicando nombre, DNI, cargo, teléfono y correo electrónico institucional. Los enlaces coordinarán la operatividad, requerimientos, capacitaciones e incidentes técnicos.

CLÁUSULA OCTAVA: OBLIGACIONES DE LA DIGER

1. Emitir, gestionar, suspender, rehabilitar y revocar certificados digitales conforme a su CPS, CP y la Ley Sobre Firmas Electrónicas.
2. Mantener la infraestructura PKI con niveles de disponibilidad, rendimiento y continuidad operativa conformes a los estándares ISO/IEC 27001 y ETSI EN 319 411.
3. Mantener disponibles la Revocación de Certificados (CRL), servicios de validación en línea (OCSP) y servicios de sellado de tiempo (TSA).
4. Capacitar a los enlaces y operadores designados por LA ENTIDAD en el uso del Portal de Solicitudes Web.
5. Preservar la confidencialidad, seguridad y trazabilidad de la información procesada durante el ciclo de vida de los certificados.

CLÁUSULA NOVENA: OBLIGACIONES DE LA ENTIDAD Y ROL DE UNIDAD DE REGISTRO DELEGADA

1. Actuar como Unidad de Registro Delegada o Punto de Registro, asumiendo la responsabilidad legal de verificar, validar y confirmar la identidad, vigencia del cargo

y relación laboral o contractual de los solicitantes en el Portal de Solicitudes Web de LA DIGER.

2. Tramitar las solicitudes de emisión a través del Portal de Solicitudes Web de LA DIGER de forma indexada y digital. La aprobación por parte del operador de LA ENTIDAD mediante sus credenciales institucionales sustituirá la firma autógrafa y constituirá declaración bajo juramento de la veracidad de la información.
3. Notificar inmediatamente a LA DIGER cualquier cese de funciones, destitución, renuncia o cambio de perfil de un titular para proceder a la revocación inmediata de su certificado.
4. Velar por que cada titular firme la aceptación de los "Términos y Condiciones de Uso del Certificado Digital" antes de su emisión.
5. Reportar cualquier incidente de ciberseguridad o compromiso de credenciales.

CLÁUSULA DÉCIMA: LIMITACIÓN Y DESLINDE DE RESPONSABILIDAD

LA DIGER no responderá por los daños o perjuicios directos o indirectos derivados del uso indebido, negligente o fraudulento de los certificados digitales por parte de los titulares o de los operadores de LA ENTIDAD, ni por la revelación de factores de autenticación (OTP/MFA/PIN/PUK/CONTRASEÑA) imputable a los usuarios. Asimismo, LA DIGER no será responsable por interrupciones del servicio causadas por fallas en las redes de telecomunicaciones de terceros, ataques cibernéticos generalizados o eventos de fuerza mayor ajenos a su infraestructura de HSM y PKI.

CLÁUSULA DÉCIMA PRIMERA: CONDICIONES DE CUSTODIA Y NO REPUDIO

El certificado digital y la clave privada son de uso exclusivo e intransferible del titular. La firma electrónica avanzada generada mediante esta infraestructura goza de la presunción de

autoría, integridad y no repudio. LA ENTIDAD y el titular son responsables del resguardo confidencial de sus claves de acceso y factores de autenticación (OTP/MFA).

CLÁUSULA DÉCIMA SEGUNDA: SUSPENSIÓN, REHABILITACIÓN Y REVOCACIÓN

LA DIGER procederá a la suspensión, rehabilitación o revocación de un certificado digital bajo las siguientes reglas:

1. **Suspensión:** Inhabilitación temporal por solicitud motivada de LA ENTIDAD, sospecha de compromiso de credenciales o por investigación administrativa interna.
2. **Rehabilitación:** Reactivación operativa del certificado suspendido únicamente previa solicitud formal y justificada por escrito del enlace autorizado de LA ENTIDAD, confirmando la subsanación de la causa que originó la suspensión.
3. **Revocación:** Extinción definitiva de la validez del certificado por cese laboral o solicitud directa del titular, solicitud formal de LA ENTIDAD, pérdida de control del MFA, falsedad de datos o uso indebido del certificado comprobado por LA DIGER, o por mandato de autoridad judicial/administrativa competente.

CLÁUSULA DÉCIMA TERCERA: RÉGIMEN SANCIONADOR

Cualquier uso indebido, negligencia, cesión de credenciales o aprobación maliciosa por parte de los operadores o titulares de LA ENTIDAD facultará a LA DIGER para suspender inmediatamente los accesos al Portal y notificar a la máxima autoridad de LA ENTIDAD a fin de que inicie los procesos disciplinarios o administrativos correspondientes, sin perjuicio de las acciones civiles y penales aplicables bajo las leyes hondureñas.

CLÁUSULA DÉCIMA CUARTA: PROPIEDAD INTELECTUAL

LA DIGER mantiene la propiedad exclusiva de los componentes técnicos, lógicos y normativos de su PKI (software, CPS, CP, configuraciones). El presente convenio no otorga licencias adicionales ni transferencias de propiedad intelectual a LA ENTIDAD.

CLÁUSULA DÉCIMA QUINTA: CONFIDENCIALIDAD, HÁBEAS DATA Y SUPERVIVENCIA

Las partes mantendrán en estricta confidencialidad la información técnica y personal tratada. La gestión de datos personales se sujetará a la garantía constitucional del Hábeas Data (Art. 182 de la Constitución de la República), a la Ley de Transparencia y Acceso a la Información Pública y a las políticas internas de ciberseguridad de LA DIGER. La obligación de confidencialidad establecida en esta cláusula sobrevivirá a la terminación o expiración de este Convenio por un período de **cinco (5) años**.

CLÁUSULA DÉCIMA SEXTA: CESE DEL SERVICIO Y CONSERVACIÓN DE REGISTROS

Al finalizar el convenio, LA DIGER revocará los certificados activos asociados a LA ENTIDAD e inhabilitará los accesos. LA DIGER conservará las evidencias electrónicas y registros de trazabilidad por un plazo mínimo de cinco (5) años (o el plazo que determine su CPS/CP) para fines de auditoría o requerimientos judiciales.

CLÁUSULA DÉCIMA SÉPTIMA: MODIFICACIONES

El convenio podrá modificarse o ampliarse únicamente mediante adendas escritas debidamente firmadas por las autoridades de ambas partes.

CLÁUSULA DÉCIMA OCTAVA: LEGISLACIÓN APLICABLE Y SOLUCIÓN DE CONTROVERSIAS

Este convenio se rige por la legislación de la República de Honduras. Cualquier discrepancia o desacuerdo sobre su interpretación o ejecución se resolverá prioritariamente mediante negociación directa y arreglos amigables. De no alcanzarse un acuerdo en un plazo de treinta (30) días calendario, las partes se someterán a los tribunales de la ciudad de Tegucigalpa, Municipio del Distrito Central.

CLÁUSULA DÉCIMA NOVENA: SUSCRIPCIÓN DIGITAL Y ACEPTACIÓN

Ambas partes declaran su conformidad con todas y cada una de las cláusulas del presente instrumento. Asimismo, acuerdan que el presente Convenio podrá ser suscrito mediante firma manuscrita autógrafa o mediante **Firma Electrónica Avanzada** emitida por un Prestador de Servicios de Certificación debidamente acreditado, gozando de la misma validez legal, eficacia probatoria y plena obligatoriedad. En fe de lo cual, se firma en dos (2) ejemplares de igual valor y tenor en la ciudad de Tegucigalpa, Municipio del Distrito Central, a los diez días del mes de agosto del año 2026

Elmer Manuel Ferrera Padilla
Firmado digitalmente por Elmer Manuel Ferrera Padilla
Fecha: 2026.08.10 11:43:22 -06'00'

ELMER MANUEL FERRERA PADILLA

Director Ejecutivo con rango de Secretario de Estado

Dirección de Gestión por Resultados (DIGER)

LA DIGER

Firmado digitalmente por Ricardo Alfredo Montes Najera
Fecha: 2026.08.10 11:51:06 -06'00'

RICARDO ALFREDO MONTES NAJERA

Magistrado Presidente Tribunal Superior de Cuentas

ANEXO I: GLOSARIO DE TÉRMINOS Y DEFINICIONES TÉCNICO-LEGALES

1. **Autenticación:** Proceso técnico de verificación de la identidad de un usuario, sistema o dispositivo antes de concederle acceso a recursos informáticos o autorizar transacciones digitales.

2. **Autoridad de Certificación (CA / AC):** Entidad o unidad organizativa de la DIGER, debidamente acreditada por la Autoridad Administrativa Competente (AAC/IP), responsable de la emisión, gestión, renovación, suspensión, rehabilitación y revocación de certificados digitales.

3. **Autoridad de Registro (RA / AR):** Entidad, unidad u operador designado para verificar y validar la identidad y requisitos de los solicitantes de certificados. Para efectos de este Convenio, LA ENTIDAD actúa en condición de Punto o Unidad de Registro Delegada.

4. **Autoridad de Sellado de Tiempo (TSA):** Servicio informático brindado por LA DIGER que expide sellos de tiempo que garantizan con certeza jurídica la fecha y hora exactas de creación o firma de un documento electrónico.

5. **Certificado Digital:** Documento o archivo electrónico emitido y firmado digitalmente por la CA que vincula un par de claves criptográficas con la identidad de su titular.

6. **Ciclo de Vida del Certificado:** Conjunto de etapas secuenciales que atraviesa un certificado digital: solicitud, verificación, emisión, activación, uso, renovación, suspensión, rehabilitación, revocación y expiración.

7. **Clave Privada:** Código criptográfico reservado e intransferible. En la modalidad de firma remota, es generada y custodiada centralizadamente dentro de los HSM de LA DIGER, manteniéndose bajo el control exclusivo del titular mediante autenticación robusta.

8. **Clave Pública:** Código criptográfico contenido en el certificado digital, de libre acceso, utilizado para verificar la validez de una firma electrónica avanzada o cifrar datos.

9. **CPS (Certification Practice Statement / Declaración de Prácticas de Certificación):** Documento detallado aprobado ante la AAC que especifica las

prácticas, controles, procedimientos operativos e infraestructura de seguridad de LA DIGER.

10. **CP (Certificate Policy / Política de Certificación):** Marco normativo y técnico que establece los requisitos de idoneidad, reglas de uso y niveles de seguridad bajo los cuales se emiten y gestionan los certificados.
11. **CRL (Certificate Revocation List / Lista de Revocación de Certificados):** Listado firmado digitalmente por la CA que contiene los números de serie de los certificados revocados antes de su vencimiento.
12. **Estampado Cronológico (Timestamping):** Mecanismo criptográfico que demuestra objetivamente que un conjunto de datos o documento existía en un instante de tiempo específico y que no ha sido alterado.
13. **Firma Electrónica Avanzada:** Conjunto de datos en forma electrónica consignados en un mensaje de datos, vinculada de manera exclusiva al firmante, que permite su identificación y la detección de modificaciones posteriores, con la misma validez y eficacia probatoria que la firma autógrafa (Decreto No. 149-2013).
14. **Firma Remota o en la Nube:** Modalidad operativa en la que la clave privada del titular se genera, almacena y opera dentro de la infraestructura centralizada de HSM de LA DIGER. El titular accede al uso de su clave privada mediante autenticación de doble factor (MFA/2FA), sin requerir dispositivos físicos.
15. **Firmante:** Persona natural autenticada y autorizada para hacer uso de la clave privada asociada a un certificado digital válido a fin de suscribir documentos electrónicos.
16. **HSM (Hardware Security Module / Módulo de Seguridad de Hardware):** Dispositivo criptográfico físico y lógico de alta seguridad, operado exclusivamente por LA DIGER, configurado para la generación y custodia segura de claves criptográficas.

17. **Identidad Digital:** Conjunto de atributos y credenciales electrónicas debidamente validadas que permiten identificar unívocamente a una persona en el entorno digital.
18. **Interoperabilidad:** Capacidad técnica y funcional de los sistemas informáticos para interactuar e interpretar documentos y firmas electrónicas de manera consistente.
19. **OCSP (Online Certificate Status Protocol):** Protocolo en línea que permite a las aplicaciones verificar en tiempo real la validez y estado actual (activo, suspendido o revocado) de un certificado digital.
20. **PKI (Public Key Infrastructure / Infraestructura de Clave Pública):** Conjunto integrado de hardware, software, políticas, estándares y procedimientos para gestionar certificados digitales y criptografía de clave pública.
21. **Rehabilitación de Certificado:** Acto técnico y administrativo mediante el cual se levanta la suspensión temporal de un certificado digital previamente inhabilitado, devolviéndole su plena validez jurídica e interactiva.
22. **Revocación:** Acto administrativo y técnico mediante el cual la CA invalida de forma definitiva la eficacia legal y operativa de un certificado digital antes de su fecha de vencimiento.
23. **RFC 3647:** Estándar técnico internacional emitido por la IETF que establece la estructura para la elaboración de CP y CPS.
24. **Suscriptor:** Institución pública o persona jurídica de derecho privado (LA ENTIDAD) que suscribe el Convenio con LA DIGER para habilitar y gestionar el uso de certificados para su personal.
25. **Suspensión de Certificado:** Inhabilitación temporal de un certificado digital por un período determinado, durante el cual no produce efectos jurídicos.
26. **Titular del Certificado:** Persona natural identificada a cuyo nombre se expide el certificado digital, responsable del resguardo de sus credenciales de acceso.

27. **Trazabilidad:** Capacidad de registrar y auditar la secuencia histórica completa de eventos, solicitudes y operaciones aplicadas a un certificado digital.