AN INFOCERT COMPANY

IN-2022-02-01

POLÍTICA DE SEGURIDAD DE LA ENTIDAD DE REGISTRO DE CAMERFIRMA PERÚ V2.0

Firmado digitalmente por: XAVIER JOAQUIN URIOS HUIGENS
Rol: GERENTE GENERAL
Organización: CAMERFIRMA PERU S.A.C.
Unidad organizacional: GERENCIAIssued by AC CAMERFIRMA PER\xC3\x9A SAC ER [PE1]
Limitación de uso: Explicit Text: CERTIFICADO DE PERSONA FISICA CON VINCULACION A EMPRESA
Fecha: 22/08/2022 17:37:14

ÍNDICE

1. TRATAMIENTO DEL DOCUMENTO

1.1 CONTROL DE ACTUALIZACIONES

VERSIÓN	FECHA	ELABORADO	ACTUALIZACIÓN	BORRADOR	APROBADO
1.0	Abril 2017		Ramiro Muñoz		Ramiro Muñoz
2.0	Junio 2022	Innovate DC (Consultor Externo)			Ramiro Muñoz

1.2 CONTROL DE CAMBIOS

DESCRIPCION DEL CAMBIO	APARTADOS QUE CAMBIAN RESPECTO A VERSIÓN ANTERIOR
AÑADIDO	Adaptación del documento a la nueva imagen de la empresa. S cambio logotipo y fuente/ tamaño y letra.
MODIFICADO	
ELIMINADO	

1.3 MANTENIMIENTO DEL DOCUMENTO

Se requiere mantenimiento y/o revisión de este documento, cada vez que el Responsable de la ER, (Definido en el documento Diagrama Organizacional de CAMERFIRMA PERÚ) lo crea oportuno y, en todo caso, cuando se produzcan cambios en:

- La infraestructura tecnológica u organizativa de la Entidad.
- La evaluación de riesgos preliminar (ver resultados en doc. “Análisis de Riesgos-Resultados”).

Cada vez que se emita una nueva versión de este documento, este debe ser:

- Aprobado por la Responsable de la Entidad de Registro.
- Comunicado a todas las partes interesadas (empleados, colaboradores, etc.) su disponibilidad en el repositorio de Documentación de Obligado Cumplimiento de RRHH, que se encuentra en SharePoint por medio de un correo electrónico.

1.4 VALIDEZ

Hasta su siguiente actualización.

1.5 TRATAMIENTO Y CONFIDENCIALIDAD

Documento de acceso al público.

1.6 DISTRIBUCIÓN

Este documento debe distribuirse entre todos los departamentos involucrados y las partes interesadas que lo requieran.

Cada versión nueva se comunicará a los empleados mediante un correo electrónico desde el departamento de RRHH.

2. INTRODUCCIÓN

AC Camerfirma S.A. (Camerfirma España) es una empresa que fue creada en el año 1999 con domicilio en España, donde se establece como prestador de servicios de certificación al amparo de la LEY 59/2003, de 19 de diciembre, de firma electrónica en España.

Camerfirma España, como entidad líder española en la emisión de certificados empresariales en el sector privado tiene mucho que ofrecer en cuanto a conocimiento de esta tecnología a nivel europeo e incluso mundial. Camerfirma España desde el comienzo de su trayectoria como sociedad anónima en el año 2000, mantiene una estrecha relación con los mercados de Sudamérica y cuenta en su labor con numerosos proyectos de consultoría y de implantación de PKI con las Cámaras de Comercio sudamericanas.

En el año 2014, Camerfirma logró acreditarse como Entidad de Certificación en Perú bajo el nombre de Camerfirma Perú S.A. (Camerfirma Perú). En el año 2017, se acreditó como Entidad de Registro, prestador de servicios de intermediación digital y servicios de emisión de Sellos de Tiempo (Timestamp), para brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

La infraestructura tecnológica y operativa de la EC de Camerfirma Perú es provista y administrada por Camerfirma España. Dicha infraestructura ha obtenido la certificación Webtrust for Certification Authorities, y es verificada anualmente por auditores autorizados.

Camerfirma Perú, como ER, brinda los servicios de registro o verificación de sus clientes a través de su oficina en Perú, tanto en el caso de personas jurídicas como naturales.

2.1 VISTA GENERAL

Este documento tiene como objetivo la descripción de operaciones y prácticas de seguridad de la información que cumple Camerfirma Perú en calidad de Entidad de Registro o Verificación – ER de Camerfirma Perú, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Entidades de Registro o Verificación (ER)” establecida por el INDECOPI.

2.2 IDENTIFICACIÓN

NOMBRE DE LA POLÍTICA:	POLÍTICA DE SEGURIDAD DE LA ENTIDAD DE REGISTRO DE CAMERFIRMA PERÚ
Descripción:	Describe las operaciones y practicas de seguridad de la información que cumplen Camerfirma Perú en calidad de Entidad de Registro
Versión:	2.0
Fecha de Emisión:	Junio 2022
Localización:	http://www.camerfirma.com.pe/

2.3 COMUNIDAD Y ÁMBITO DE APLICACIÓN

Este documento puede ser utilizado por terceros receptores de certificados digitales de Camerfirma Perú y suscriptores del servicio de emisión de certificados digitales como base para confirmar la fiabilidad de los servicios descritos en él.

2.3.1 ENTIDAD DE CERTIFICACIÓN

Camerfirma Perú, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

A Camerfirma Perú, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la ACC a fin de poder ingresar a la IOFE.

2.3.2 ENTIDAD DE REGISTRO

Camerfirma Perú brinda los servicios de Entidad de Registro, la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

2.3.3 PROVEEDOR DE SERVICIOS E INFRAESTRUCTURA

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación de Camerfirma Perú, cuando la entidad de certificación así lo requiere y garantizan la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece Camerfirma Perú son provistos por Camerfirma España.

2.3.4 TITULAR

Es la persona natural o jurídica responsable del Certificado. En el Certificado de Persona Natural, el TITULAR es asimismo SUSCRIPTOR del certificado. En el Certificado de Persona Jurídica, el TITULAR es la Entidad.

2.3.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

2.3.6 PARTE USUARIA

En esta Política se entiende por Parte Usuaria a la persona que voluntariamente confía en los sellos de tiempo emitidos bajo esta política y se sujeta a lo dispuesto en ella por lo que no se requerirá acuerdo posterior alguno.

La Parte Usuaria también puede denominarse como “Tercero que Confía”.

2.3.7 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un certificado emitido bajo esta RPS.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

2.4 USOS DEL CERTIFICADO DIGITAL

2.4.1 ÁMBITO DE APLICACIÓN Y USOS

Los certificados emitidos bajo la Declaración de Prácticas de Camerfirma Perú pueden ser utilizados para los siguientes propósitos:

- Identificación del Titular que firma un documento o que se autentica para acceder a un sistema: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el certificado.

- Integridad del documento firmado: La utilización del certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.

- No repudio de origen: Con el uso de este certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

2.4.2 USOS PROHIBIDOS Y NO AUTORIZADOS

Bajo la presente Política no se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en este documento y en la Declaración de Prácticas de Certificación.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la EC.

3. POLÍTICAS DE SEGURIDAD DE LA ER

3.1 SEGURIDAD DE LA INFORMACIÓN

Camerfirma Perú, en calidad de Entidad de Registro, tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de registro, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de verificación de identidad y registro, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de la ER en los ámbitos legales, regulatorios y contractuales.

3.2 SEGURIDAD FÍSICA

3.2.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de la ER de Camerfirma Perú prevé el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil.

3.2.2 SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO

A fin de proteger al personal y el equipamiento en las instalaciones de la ER de Camerfirma Perú, los medios que garanticen la seguridad física de los equipos y del personal, implementan los siguientes controles:

a) Señalización de zonas seguras
b) Provisión de extinguidores contra incendios
c) No hay presencia de cableado eléctrico expuesto
d) Uso de estabilizadores y supresores de picos

3.2.3 PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Las áreas de archivo de documentos en papel y archivos electrónicos, se encuentran protegidas constantemente contra acceso no autorizado:

a) Se encuentran en ambientes separados de las áreas públicas de registro.
b) Solo se permite el ingreso a personal autorizado
c) El ingreso y salida del personal es registrado
d) Los terceros y el personal de limpieza puede ingresar con autorización del Responsable de Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área
e) El ingreso y salida de documentos es registrado

f) Se encuentra cerrada bajo llave cuando no esté siendo usada
g) Cuando sea asignado un personal nuevo se verifican sus antecedentes

Las operaciones de validación y registro pueden realizarse en las instalaciones de Camerfirma Perú o en las instalaciones del cliente o cualquier otro lugar definido por él en presencia del Operador de Registro, el cual será responsable de proteger la información proporcionada por el cliente.

3.2.4 PROTECCIÓN CONTRA LA EXPOSICIÓN AL AGUA

Las instalaciones se encuentran protegidas contra exposición al agua, en particular, las áreas de archivo permanecen distantes de zonas de filtración de agua o humedad, ya sea en el techo o en las paredes colindantes.

3.2.5 PROTECCIÓN CONTRA INCENDIOS

Las instalaciones poseen las siguientes medidas para la prevención y protección contra incendios:

a) Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de Camerfirma Perú
b) Se cuenta con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.
c) Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores es guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado

3.2.6 ARCHIVO DE MATERIAL

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), se encuentran protegidos en las áreas de archivo, en contenedores de protección contra fuegos y se sitúan en diversas dependencias para eliminar riesgos asociados a una única ubicación.

El acceso a estos contenedores se encuentra restringido a personal autorizado.

3.2.7 GESTIÓN DE RESIDUOS

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), que requieran ser eliminados o su soporte electrónico requiera ser desechado, deberán ser borrados o destruidos de manera irrecuperable.

3.2.8 COPIA DE SEGURIDAD EXTERNA

Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores es guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado.

3.3 ROLES DE CONFIANZA

Los roles de confianza se encuentran definidos de la siguiente manera:

- Responsable de la ER
- Responsable de Seguridad
- Responsable de Privacidad
- Operadores de Registro
- Auditores

Estos roles son asignados formalmente por el Responsable de Camerfirma Perú en calidad Entidad de Registro.

La descripción de los roles incluye las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que son puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las mismas.

3.3.1 NÚMERO DE PERSONAS REQUERIDAS POR LABOR

Los cambios en los documentos normativos requieren de la autorización de los Responsables de la ER, el Responsable de Seguridad y el de Privacidad, dichos roles no son incompatibles y pueden ser asumidos por un mismo cargo.

3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los roles de confianza emplean controles de acceso físico para el acceso a las áreas de archivo, así como lógicos para las comunicaciones con la EC. Los controles de acceso a los sistemas de Registro dependen de la configuración de los sistemas de la EC de Camerfirma Perú.

3.3.3 AUDITORÍA

El auditor asignado por el INDECOPI será siempre una persona independiente de las operaciones de registro.

3.4 GESTIÓN DEL PERSONAL

3.4.1 CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los roles de confianza deben tener conocimiento y entrenamiento en las operaciones de registro digital, la Política de Seguridad de la Información y la Política y el Plan de Privacidad de Datos.

Asimismo, deben tener experiencia relacionada a los temas de certificación digital.

3.4.2 PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Se verificarán los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de registro, incluyendo:

- Verificación de antecedentes criminales
- Verificación de antecedentes crediticios

Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.

3.4.3 REQUISITOS DE CAPACITACIÓN

Todos los empleados de la organización que participan de los servicios de registro deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral:

- El equipo y software requerido para operar.
- Los aspectos de la RPS, Política de Seguridad, Plan de privacidad y otra documentación relevante que afecte sus funciones.
- Requisitos legislativos en relación a sus funciones.
- Sus roles en relación al Plan de Contingencias.

3.4.4 FRECUENCIA DE LAS CAPACITACIONES

Las sesiones de capacitación y entrenamiento deben ser llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

3.4.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN EN EL TRABAJO

No se implementará rotación de los trabajadores.

3.4.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Se cuenta con un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona será inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

Dichas sanciones se encuentran establecidas en los contratos de cada empleado y/o contratista.

3.4.7 REQUERIMIENTOS DE CONTRATISTAS

El personal contratado para fines específicos dentro de las operaciones de Camerfirma Perú en calidad Entidad de Registro, será evaluado respecto de sus antecedentes criminales, conocimiento y experiencia. Asimismo, no deberá tener acceso sin supervisión a las áreas de archivo y no tendrá acceso a los sistemas de registro brindados por la EC de Camerfirma Perú.

3.5 PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

3.5.1 TIPOS DE EVENTOS REGISTRADOS

Los sistemas de información sensible son provistos por la EC de Camerfirma Perú ya que es esta quien administra y define los logs de auditoría.

Se guardarán los contratos de los titulares y suscriptores, así como las solicitudes de los procesos de registro, como evidencia de las transacciones realizadas y para efectos de auditoría.

La ER de Camerfirma Perú genera reportes de los siguientes eventos:

- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos debe registrar la hora, fecha e identificadores software/hardware.

3.5.2 FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO

Los registros de auditoría serán procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales.

El procesamiento de los registros de auditoría incluirá la verificación de que dichos registros no hayan sido manipulados.

3.5.3 PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro se conservarán por un periodo de diez (10) años.

3.5.4 PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Las áreas de archivo donde se almacenan los contratos de los suscriptores y los titulares, así como las solicitudes de los procesos de registro estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.

La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

3.5.5 COPIA DE SEGURIDAD DEL REGISTRO DE AUDITORÍA

Todas las solicitudes y contratos físicos serán generados con copia y los documentos electrónicos tendrán una copia por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el Responsable de Camerfirma Perú en calidad Entidad de Registro.

3.6 AUDITORÍA

La ER realiza auditorías internas de manera periódica (mensual o bimestralmente). El Responsable de Seguridad hace uso de los logs respecto a los siguientes temas:

- Sistema de Registro, para validar que el OR instaló directamente los certificados en el repositorio del cliente y no en el repositorio de Windows de su propio computador.
- Sistema Operativo del computador del OR.
- Contabilización de los dispositivos criptográficos[1] que maneja el OR, para validar el número de tarjetas emitidas y entregadas por el OR, el número de tarjetas dañadas y el número de tarjetas almacenadas correspondiente al total de tarjetas recibidas por el OR. Los dispositivos criptográficos dañados o mal impresos serán devueltos a la Oficina Central de Camerfirma Perú para su correcta destrucción.
- La correspondencia entre los formatos firmados de emisión y revocación de certificados, contra las solicitudes que se encuentran en el Sistema de Registro.

Las evaluaciones técnicas de INDECOPI se llevarán a cabo una vez al año y cada vez que INDECOPI lo requiera.

[1]Los dispositivos criptográficos (tarjeta inteligente y/o token)

3.6.1 NOTIFICACIÓN AL TITULAR QUE CAUSA UN EVENTO

Las notificaciones automáticas dependen de los sistemas de la EC de Camerfirma Perú, para todos los eventos relacionados con el uso de los certificados por parte de un titular.

3.6.2 VALORACIÓN DE VULNERABILIDAD

Los sistemas de registro son administrados por la EC de Camerfirma Perú, por lo que la protección perimetral de redes corresponde a la infraestructura de WISeKey certificado con el sello de WebTrust.

3.7 ARCHIVO

3.7.1 PROTECCIÓN DEL ARCHIVO

El archivo físico está protegido con controles de acceso físico para impedir el acceso a personas no autorizadas. Los documentos se encuentran firmados de manera manuscrita y digital respectivamente para prevenir cualquier modificación.

El ingreso y salida de documentos físicos y digitales es registrado para impedir la pérdida o destrucción no autorizada.

Debe tomarse en consideración la posibilidad de re-firmado de los archivos cuando los avances en las tecnologías generen potencialmente una posibilidad de afectación a los mismos o la generación de microformas según Decreto Legislativo 681.

3.7.2 PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO

Mensualmente, la integridad del archivo es verificada.

3.8 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

La ER de Camerfirma Perú mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones de registro. Dicho plan y documentos adicionales respecto a seguridad son confidenciales y serán revelados ante el auditor el día de la auditoría.

4. RESPONSABILIDAD

Camerfirma España, como proveedor de infraestructura y gestión de operaciones de los servicios de la EC de Camerfirma Perú, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC de Camerfirma Perú.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por Camerfirma España de acuerdo a su documento Declaración de Prácticas de Certificación, publicado en:

www.camerfirma.com

Camerfirma Perú es responsable de exigir y supervisar las operaciones de los servicios que son administrados por Camerfirma España.

Como Entidad de Registro, es responsable de la correcta identificación de las personas naturales o jurídicas y de la seguridad en la entrega de certificados digitales, siempre que esta sea realizada por los Operadores de Registro autorizados.

Las peticiones, quejas o reclamos sobre los servicios prestados por Camerfirma Perú a través de Camerfirma España son recibidas directamente por Camerfirma Perú como prestador de servicios digitales o a través de la Entidad de Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone Camerfirma Perú es permanente. Estos reclamos serán comunicados en un lapso no mayor de 5 días a Camerfirma España, para su debida atención.

4.1 RESPONSABLE DE LOS DOCUMENTOS DE LA ER

Nombre: Xavier Urios

Cargo: Gerente General de Camerfirma Perú

Dirección de correo electrónico: xurios@cocep.org.pe

4.2 RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad de Camerfirma Perú gestiona la implementación y vela por el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

5. CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

Camerfirma Perú, como Autoridad emisora de sellos de tiempo, cumple los requerimientos legales establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales – Ley 27269.

6. CONFORMIDAD

Este documento ha sido aprobado por la Autoridad de la ER de Camerfirma Perú, y tiene carácter normativo sobre todos los servicios de sellado de tiempo, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

ANEXO I. ACRÓNIMOS

AC	Autoridad de Certificación
AR	Autoridad de Registro
CPS	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL	*Certificate Revocation List.* Lista de certificados revocados
CSR	*Certificate Signing Request.* Petición de firma de certificado
DES	*Data Encryption Standard*. Estándar de cifrado de datos
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm.* Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
DSADCF	Dispositivo seguro de almacén de datos de creación de firma
FIPS	*Federal Information Processing Standard Publication*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization.* Organismo Internacional de Estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso a directorios
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PA	*Policy Authority.* Autoridad de Políticas
PC	Política de Certificación
PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA-1	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

TCP/IP *Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

ANEXO II. DEFINICIONES

Autoridad de Certificación	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y la Parte Usuaria, vinculando una determinada clave pública con una persona.
Autoridad de políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y DPC.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	El establecimiento de una relación de confianza entre dos AC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada **datos de verificación de firma.**
Clave privada	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada **datos de creación de firma.** La clave privada de la AC será usada para firma de certificados y firma de CRL's
CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.

Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.
DSCF	*Dispositivo Seguro de creación de firma*. Elemento software o hardware empleado por el suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
Entidad	Dentro del contexto de las políticas de certificación de Camerfirma, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el suscriptor.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes

Suscriptor	Dentro del contexto de las políticas de certificación de Camerfirma, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Parte Usuaria	Dentro del contexto de las políticas de certificación de Camerfirma, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado