PERUSECURITY

DECLARACIÓN DE PRACTICAS DE REGISTRO V.1.0

Entidad de Registro Peru Media Security SAC

ÍNDICE

1 TRATAMIENTO DEL DOCUMENTO

1.1 CONTROL DE ACTUALIZACIONES

Versión	Descripción	Elaborado	Fecha
1.0	PRIMERA VERSION DEL DOCUMENTO	Consultor	15/02/2023

1.2 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 PERÚ MEDIA SECURITY SAC) 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 excel. “Matriz de riesgos”).
- Cada vez que se emita una nueva versión de este documento, este debe ser:
  - Aprobado por la responsable de la Entidad de Registro.
  - Comunicar a todas las partes interesadas (empleados, colaboradores, etc.) su disponibilidad en el repositorio del sitio web.

1.3 VALIDEZ

Hasta su siguiente actualización.

1.4 TRATAMIENTO Y CONFIDENCIALIDAD

Documento de acceso al público.

1.5 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 Administración.

2 INTRODUCCIÓN

La ER PERÚ MEDIA SECURITY SAC. se constituye como Entidad de Registro o Verificación de la Entidad de AC CAMERFIRMA PERÚ S.A.C., y brinda servicios de recepción de solicitudes de emisión, de revocación, re-emisión de los certificados digitales, tanto para el caso de personas jurídicas como personas naturales respecto de los servicios brindados por esta Entidad de Certificación.

2.1 VISTA GENERAL

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza la ER PERÚ MEDIA SECURITY SAC para la administración de sus servicios como Entidad de Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registro o Verificación– ER" establecida por el INDECOPI, en calidad de Autoridad Administrativa Competente de la Infraestructura Oficial de la Firma Electrónica del Perú.

2.2 IDENTIFICACIÓN

Nombre de la Política:	Declaración de Prácticas de Registro de la ER PERÚ MEDIA SECURITY SAC
Descripción:	Describe las operaciones y prácticas que utiliza la ER PERÚ MEDIA SECURITY SAC para la administración de sus servicios como Entidad de Registro
Versión:	1.0
Fecha de Emisión:	Febrero 2023
Localización:	http://www.perusecurity.pe/

2.3 COMUNIDAD Y ÁMBITO DE APLICACIÓN

Este documento puede ser utilizado por terceros receptores de certificados digitales de la ER PERÚ MEDIA SECURITY SAC 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

AC CAMERFIRMA PERÚ S.A.C., 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.

AC CAMERFIRMA PERÚ S.A.C., como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la Autoridad Administrativa Competente a fin de poder ingresar a la IOFE.

2.3.2 ENTIDAD DE REGISTRO

La ER PERÚ MEDIA SECURITY SAC 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 AC CAMERFIRMA PERÚ S.A.C., 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 AC CAMERFIRMA PERÚ S.A.C., son provistos por AC CAMERFIRMA PERÚ S.A.C.

2.3.4 TITULAR

El Titular del certificado es el responsable de los efectos jurídicos generados por la utilización de una firma digital. Tratándose de personas naturales, éstas son firmantes/titulares del certificado y de las firmas digitales que se generen a partir de aquél. En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes o personas vinculadas, los suscriptores poseedor y responsable de la generación y uso de las claves, salvo el caso de las firmas digitales que generen a través de agentes automatizados para las cuales las personas jurídicas son titulares de los certificados y de las firmas digitales generadas a partir de éstos

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 del 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 corresponderá a la persona jurídica. La atribución de responsabilidad del 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 certificados 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 La ER PERÚ MEDIA SECURITY SAC pueden ser utilizados para los siguientes propósitos:

- **Certificado de Persona Jurídica – Atributo de Vinculación a Entidad (Certificados para personas jurídicas)**: Determinan la relación de vinculación laboral o mercantil entre una persona natural y una Entidad (campo organización del certificado). En el marco legal peruano la Entidad es considerada el Titular del certificado y la Persona Natural el Suscriptor del certificado.

- **Certificado de Persona Jurídica – Atributo de Representante Legal (Certificados para personas jurídicas)**: Determina la relación de representación legal o de apoderado general entre la persona natural y una Entidad con personalidad jurídica (descrita también en el campo Organización del certificado). En el marco legal peruano la Entidad es considerada el Titular del certificado y la Persona Natural el Suscriptor del certificado.

- **Certificado de Persona Jurídica (Certificados para personas jurídicas)**: Este certificado se emite a una entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

- **Certificado de Persona Jurídica – Atributo de Facturación Electrónica (Certificados para**

personas jurídicas): Este certificado es exclusivo para la realización de facturas electrónicas y se emite a una Entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. La acción de las claves se asocia al uso de un certificado de vinculación dota de integridad y autenticidad a las facturas sobre los que se aplica. En el marco legal peruano la Entidad es considerada Titular del certificado y la Persona Natural Suscriptor del certificado.

- **Certificado de Persona Natural (Certificados para personas físicas)**: Determina la identidad de la persona natural firmante para actuar en su propio nombre.

- **Certificado de Sello Electrónico de Empresa para agentes automatizados (Certificados para personas jurídicas):** Este certificado se emite a una entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS. En el marco legal peruano, la Entidad es considerada Titular y Suscriptor del certificado.

- **Certificado de Persona Jurídica - Atributo Profesional Colegiado**: Determina la relación de vinculación entre una persona natural y un Colegio profesional del Perú (campo organización del certificado).

2.4.2 USOS PROHIBIDOS Y NO AUTORIZADOS

Bajo la presente Política no se permite el uso que sea contrario a la normativa peruana, española y de la UE siempre que éstas últimas no contradigan la normativa peruana, 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 (DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CAMERFIRMA 2003-2008-2016).

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

3 CLÁUSULAS GENERALES

3.1 OBLIGACIONES

Este apartado incluye todas las obligaciones, garantías y responsabilidades de la ER frente a los usuarios y terceras partes que voluntariamente confían en los servicios de certificación digital, así como las obligaciones asumidas por las partes.

3.1.1 ENTIDAD DE REGISTRO

Las ER son las entidades delegadas por la EC para realizar las tareas de registro y aprobación de las solicitudes de certificados, por lo tanto, la ER también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

- Respetar lo dispuesto en la CPS y en la Política de Certificación correspondiente.
- Proteger sus claves privadas que les servirán para el ejercicio de sus funciones.
- Comprobar la identidad de los Sujetos/Firmantes y Solicitantes de los certificados cuando resulte necesario, acreditando definitivamente la identidad del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización, de acuerdo con lo establecido en las secciones correspondientes del documento CPS.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- Proporcionar al Firmante, en caso de certificados individuales, o al futuro poseedor de claves, en caso de certificados de organización, acceso al certificado.
- Entregar, en su caso, el dispositivo criptográfico correspondiente.
- Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o Firmante.
- Respetar lo dispuesto en los contratos firmados con AC CAMERFIRMA PERÚ S.A.C., y con el Sujeto/Firmante.
- Informar a AC CAMERFIRMA PERÚ S.A.C., de las causas de revocación, siempre y cuando tomen conocimiento.
- Ofrecer información básica sobre la política y uso del certificado, incluyendo

especialmente información sobre AC CAMERFIRMA PERÚ S.A.C., y la Declaración de Prácticas de Certificación aplicable, así como de sus obligaciones, facultades y responsabilidades.

- Ofrecer Información sobre el certificado y el dispositivo criptográfico.
- Recopilar información y evidencias del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de dichos elementos.
- Informar del método de imputación exclusiva al poseedor de la clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico.

3.1.2 SOLICITANTE

El solicitante de un certificado digital estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Respetar lo dispuesto en la Declaración de Prácticas de Registro.
2. Suministrar a la ER la información necesaria para realizar una correcta identificación.
3. Confirmar la exactitud y veracidad de la información suministrada.
4. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

3.1.3 SUSCRIPTOR

El suscriptor para hacer uso del certificado digital asume la obligación de conocer y comprender plenamente las características y limitaciones determinadas en esta Declaración de Prácticas de Certificación y de las Políticas y contratos comerciales vinculados.

El suscriptor de un certificado estará obligado a:

1. Respetar lo dispuesto en el presente documento.
2. Proteger sus claves privadas de forma segura.

3.1.4 PARTE USUARIA

Las terceras partes que voluntariamente confíen en los certificados digitales (Partes

Usuarias) asumen la obligación de:

- Verificar el estado de activación en que se encuentra el certificado digital, mediante consulta a la CRL u otro medio que se disponga para la verificación de estado del certificado.

- En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:
    - La fecha de revocación o de caducidad es posterior a la fecha en que se emitió el certificado.
    - La función criptográfica que se empleó sigue siendo segura.
    - Que la longitud de la Clave criptográfica y el algoritmo de firma electrónica siguen siendo de práctica habitual.
    - Tener en cuenta cualquier limitación en el uso del certificado digital indicado en la política o en las prácticas de certificación correspondientes.
    - Tomar en consideración cualquier límite prescrito en otros acuerdos de servicio.

3.2 RESPONSABILIDAD

La ER será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. La exactitud de toda la información contenida en los certificados emitidos.
2. La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
3. Cualquier responsabilidad que se establezca por la legislación vigente.

AC CAMERFIRMA PERÚ S.A.C., como proveedor asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital.

PERU MEDIA SECURITY SAC 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 La ER PERÚ MEDIA SECURITY SAC se pueden realizar: A través de la línea telefónica (+511) 500 54 41 - (+511) 500 54 42 y por correo electrónico a la casilla: entidad.registro@perusecurity.com.pe para la atención a titulares y terceros.

3.2.1 RESPONSABLE DE LOS DOCUMENTOS DE LA ER

Nombre: Carlos A. Torres Aparicio

Cargo: Gerente General de la ER PERÚ MEDIA SECURITY SAC

Dirección de correo electrónico: carlos@perusecurity.com.pe

3.2.2 EXONERACIÓN DE RESPONSABILIDAD

La ER no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
2. Por el uso de los certificados digitales siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Declaración de Prácticas.
3. Por el uso indebido o fraudulento de los certificados digitales emitidos por La ER PERÚ MEDIA SECURITY SAC.
4. Por el uso de la información contenida en el certificado o en la CRL.
5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o usuario en la normativa vigente, en la presente Declaración de Prácticas, en las Políticas Correspondientes o en los contratos establecidos por las partes.
6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.
7. Fraude en la información presentada por el solicitante.

3.2.3 LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

La ER no se responsabilizará por las pérdidas por transacciones.

3.3 RESPONSABILIDAD FINANCIERA

La ER no asume ningún tipo de responsabilidad financiera.

Se establecen garantías particulares a través de seguros específicos que se negociarán individualmente.

3.4 INTERPRETACIÓN Y EJECUCIÓN

3.4.1 LEGISLACIÓN

La ejecución, interpretación, modificación o validez de las presentes Prácticas se regirá por lo dispuesto en la legislación vigente aplicable.

3.4.2 INDEPENDENCIA

La invalidez de una de las cláusulas contenidas en esta Declaración de Prácticas no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

3.4.3 PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas será definido en los contratos de los titulares y con respeto a la legislación vigente.

3.5 TARIFAS

3.5.1 TARIFAS DE EMISIÓN DE CERTIFICADOS

Las tarifas por los servicios de registro y certificación digital serán definidas directamente con sus clientes, se envía documento tributario a través del correo electrónico enviado a la cuenta declarada por el solicitante.

3.5.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

Sin estipular.

3.5.3 TARIFAS POR EL ACCESO AL CONTENIDO DE ESTAS POLÍTICAS DE CERTIFICACIÓN

El acceso al contenido de la presente Declaración de Prácticas de Registro será gratuito.

3.6 POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN

3.6.1 DECLARACIÓN DE PRÁCTICAS

LA ER PERÚ MEDIA SECURITY SAC demostrará que cuenta con la fiabilidad necesaria para la provisión del servicio de emisión de certificados digitales.

En particular:

- Dispondrá de un análisis de riesgos para evaluar los activos de la empresa y las amenazas, de tal forma que determine si son necesarios controles de seguridad u operativos para protegerlos.
- Dispondrá de una Declaración de Prácticas y procedimientos usados para dar respuesta a todos los requerimientos expuestos en estas políticas.
- La Declaración de Prácticas identificará las obligaciones de todos los agentes (internos y externos) implicados en el soporte al servicio de la emisión de certificados digitales.
- LA ER PERÚ MEDIA SECURITY SAC pondrá a disposición de suscriptores y usuarios la Declaración de Prácticas y cualquier documentación relevante que garantice la conformidad con esta política. LA ER PERÚ MEDIA SECURITY SAC no tiene que publicar la documentación que considere de uso confidencial.
- LA ER PERÚ MEDIA SECURITY SAC distribuirá a todos los suscriptores y usuarios los términos y condiciones de uso.
- La autoridad responsable de la Declaración de Prácticas se asegurará que estas están implantadas de forma correcta.
- LA ER PERÚ MEDIA SECURITY SAC comunicará los cambios que llegue a realizar en la Declaración de Prácticas, estas deberán ser aprobadas y puestas a disposición de suscriptores y usuarios.

3.6.2 DECLARACIÓN INFORMATIVA

LA ER PERÚ MEDIA SECURITY SAC informará a todos los suscriptores y potenciales usuarios, los términos y condiciones sobre el uso de los certificados digitales.

Esta Declaración al menos especificará por cada política distinta utilizada:

- Política de Registro aplicada.
- Al menos, un algoritmo resumen que se utilizará para representar a los datos.
- Cualquier limitación en el uso del servicio.
- Las obligaciones del suscriptor.
- Las obligaciones de los usuarios.
- Información de cómo verificar la validez de un certificado digital de forma que un usuario pueda considerar razonable confiar en él y cualquier posible limitación en la validez de este.
- El periodo de tiempo de retención de los ficheros de auditoría.
- El marco jurídico aplicable, incluido cualquier declaración de cumplimiento de las regulaciones jurídicas nacionales.
- Limitaciones de responsabilidad.
- Proceso de resolución de disputas.
- Si la ER ha sido auditada por un organismo independiente respecto a la conformidad con estas prácticas.
- Disponibilidad del servicio y expectativas de resolución ante incidentes que afecten a la emisión de certificados digitales.

3.7 PUBLICACIÓN Y REGISTRO

3.7.1 PUBLICACIÓN DE LA INFORMACIÓN SOBRE CERTIFICACIÓN

La Declaración de Prácticas de Registro y toda la documentación pertinente y relevante

vigente de PERU MEDIA SECURITY SAC. En calidad de ER de AC CAMERFIRMA PERU S.A.C., así como sus versiones anteriores son publicadas en la siguiente dirección web: http://www.perusecurity.com.pe

3.7.2 FRECUENCIA DE PUBLICACIÓN

La presente declaración de prácticas y sus modificaciones, así como toda documentación relevante y pública de la ER, serán publicadas al día útil siguiente luego de su aprobación por parte del INDECOPI.

3.7.3 CONTROLES DE ACCESO A LOS REGISTROS

AC CAMERFIRMA PERU S.A.C. es quien administra los registros de información de los titulares y suscriptores de los certificados emitidos bajo intermediación de PERU MEDIA SECURITY SAC. Es por ello que la AC es la responsable de la implementación de los controles para restringir el acceso a estos registros únicamente a personas autorizadas.

3.8 AUDITORÍAS

3.8.1 FRECUENCIA DE LAS AUDITORÍAS

Las auditorías internas se llevarán según EL PLAN DE AUDITORIAS INTERNAS (PAI) de PERU MEDIA SECURITY SAC en calidad Entidad de Registro de AC CAMERFIRMA PERÚ S.A.C

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

3.8.2 CALIFICACIONES DE LOS AUDITORES

La selección de los auditores depende del INDECOPI. El auditor debe:

- Ser autorizado por el INDECOPI.
- El auditor no deberá haber laborado para LA ER PERÚ MEDIA SECURITY SAC, ni deberá haber tenido ninguna relación comercial con la misma, ni de efectos de auditoría en el mismo alcance de evaluación, en los últimos 2 años calendario.

3.8.3 RELACIÓN DEL AUDITOR CON LA ER

Los auditores o asesores deben ser independientes de LA ER PERÚ MEDIA SECURITY SAC.

3.8.4 AUDITORÍA DE LOS REGISTROS

Los sistemas de información sensible son provistos por la EC, por lo que PERU MEDIA SECURITY S.A.C. en calidad Entidad de Registro de AC CAMERFIRMA PERU S.A.C. sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC. Los registros son revisados como parte de la auditoría de AC CAMERFIRMA PERÚ S.A.C, de manera anual.

3.8.5 AUDITORÍA DEL ARCHIVO

Los archivos son revisados de manera anual como parte de la auditoría de AC CAMERFIRMA PERÚ S.A.C.

3.8.6 AUDITORÍA DE LOS PROCEDIMIENTOS Y CONTROLES

Los procedimientos y controles implementados son auditados por AC CAMERFIRMA PERÚ S.A.C de manera anual. Las auditorías internas son llevadas a cabo, como mínimo, una vez al año en la ER. Asimismo, PERU MEDIA SECURITY SAC cuenta con los siguientes documentos relacionados a las auditorias:

- PROCEDIMIENTO DE AUDITORÍAS INTERNAS (PAI)
- FORMATO DE AUDITORÍA INTERNA
- PLAN DE AUDITORIAS INTERNAS

3.9 CONFIDENCIALIDAD

3.9.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

AC CAMERFIRMA PERÚ S.A.C, como proveedor de operaciones de La ER PERÚ MEDIA SECURITY SAC, considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el

consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

AC CAMERFIRMA PERÚ S.A.C, dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

La información privada custodiada, son los siguientes documentos:

- Contrato firmado
- Copia de documento de identidad del solicitante
- Copia del documento de identidad del representante legal
- Video llamada de validación
- Vigencia de poderes
- Ficha Ruc
- Constancia de no adeudo de jurado nacional de elecciones

3.9.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Se considerará como información no confidencial:

a) La contenida en la presente Política y en las Prácticas de Certificación

b) La información contenida en los certificados.

c) Cualquier información cuya publicidad sea impuesta normativamente

3.9.3 DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN DE CERTIFICADOS

AC CAMERFIRMA PERÚ S.A.C., como proveedor de operaciones de La ER PERÚ MEDIA SECURITY SAC, difunde la información relativa a la revocación de un certificado mediante la publicación periódica de las correspondientes CRLs.

AC CAMERFIRMA PERÚ S.A.C., dispone de un servicio de consulta de CRL y Certificados en el sitio de Internet: https://www.camerfirma.com.pe/validador-de-certificados/

AC CAMERFIRMA PERÚ S.A.C., dispone de un servicio de consulta online de estado de los

certificados basado en el estándar OCSP en la dirección http://ocsp.camerfirma.com. El servicio OCSP ofrece respuestas estandarizadas bajo el RFC 2560 sobre el estado de un certificado digital, es decir, si el certificado consultado está activo, revocado o si ha sido emitido o no por la autoridad de certificación.

La política de difusión de información de revocación de certificados en AC subordinadas Externas con uso de tecnología propia, se realizará en base a sus propias CPS.

3.9.4 ENVÍO A LA AUTORIDAD COMPETENTE

AC CAMERFIRMA PERÚ S.A.C., proporcionará la información solicitada por la autoridad competente o al organismo regulador correspondiente, en los casos y forma establecidos en la legislación vigente.

3.10 DERECHOS DE PROPIEDAD INTELECTUAL

AC CAMERFIRMA PERÚ S.A.C. y la ER PERÚ MEDIA SECURITY SAC tienen derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

4 MEDIDAS DE CONTINGENCIA

4.1 PROTECCIÓN CONTRA COMPROMISOS DE LAS CLAVES DEL SUSCRIPTOR

Actualmente LA ER PERÚ MEDIA SECURITY SAC no gestiona ni almacena las claves privadas de los titulares, por lo cual no hay ni hubo algún caso de compromiso de la clave privada de un suscriptor dentro de las operaciones de registro. Sin embargo, en caso de que el mismo titular presente un caso en que se comprometa su certificado, PERÚ MEDIA SECURITY SAC tiene los procedimientos que debe seguir una persona natural o jurídica en caso de compromiso de la clave privada están en este documento ***DECLARACIÓN Y PRACTICAS DE***

REGISTRO en las secciones **10 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS y 11 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN**; este documento está publicado en la sección de la página web "repositorio" de la página de www.perusecurity.pe

Las responsabilidades y garantías financieras que ofrece la ER están detalladas en el documento DECLARACIÓN DE PRACTICA DE REGISTRO en la sección 16 MATERIAS DE NEGOCIO Y LEGALES, también en el alcance de la póliza que se envió.

4.2 COMPROMISO DE LAS CLAVES DEL OPERADOR DE REGISTRO

PERÚ MEDIA PERU MEDIA SECURITY SAC cuenta con el documento *PLAN DE CONTINGENCIAS Y RECUPERACIÓN DE DESASTRES apartado 1.7 donde se detalla el procedimiento.*

N°	Actividad	Responsable(s)
1	Notificar a la Entidad Certificadora: Al ser comprometida la clave privada por robo, hurto, pérdida, sospecha de haber perdido el control de su clave, entre otros motivos, lo primero que se debe de hacer es informar a la Entidad de Certificación para la revocación del certificado del Operador de Registro de la ER.	Operador de Registro y Oficial de Seguridad
2	Delegación de funciones: Las funciones deberán ser asumidas por otro Operador de Registro, cuya clave no se encuentre comprometida. En caso que las claves de todos los Operadores se encuentren comprometidas, no se podrán emitir certificados digitales hasta la renovación de cada uno.	Operador de Registro y Oficial de Seguridad
3	Eliminar la clave privada. Guardar la clave pública. El Oficial de Seguridad asegurará que las acciones mencionadas en este ítem sean completadas.	Operador de Registro y Oficial de Seguridad

4	Solicitar un nuevo certificado y repetir los pasos de generación	Operador de Registro
5	Comunicar al Responsable de la ER y registrar el hecho en un acta.	Oficial de Seguridad

5 ESPECIFICACIÓN DE LA ADMINISTRACIÓN

5.1 CONTINGENCIA EN CASO DE INDISPONIBILIDAD DE SERVICIOS DE RECEPCIÓN DE SOLICITUDES DE REVOCACION

PERÚ MEDIA PERU MEDIA SECURITY SAC cuenta con el documento *PLAN DE CONTINGENCIAS Y RECUPERACIÓN DE DESASTRES apartado 1.6 donde se detalla el procedimiento.*

N°	Actividad	Responsable(s)
1	En caso que no se cuente con disponibilidad del sistema de registro, notificar del problema por correo electrónico corporativo al titular de los certificados sobre el problema.	Operador de Registro
2	Notificar del problema por correo electrónico corporativo a la EC sobre el problema.	Operador de Registro
3	Registrar la fecha y la hora.	Operador de Registro
4	Hacer seguimiento de la solicitud hasta que sea ejecutada.	Operador de Registro
5	Comunicar al Responsable de la ER y registrar el hecho en un acta, incluyendo el tiempo de solicitud.	Área de soporte

5.2 CONTINGENCIA EN CASO DE INDISPONIBILIDAD DE SERVICIOS DE RECEPCIÓN DE SOLICITUDES DE RE- EMISIÓN

PERU MEDIA SECURITY SAC cuenta con el documento PLAN DE CONTINGENCIAS Y RECUPERACIÓN DE DESASTRES apartado 1.4 donde se detalla el procedimiento.

N°	Actividad	Responsable(s)
1	En caso que no se cuente con disponibilidad del sistema de registro, notificar del problema por correo electrónico corporativo al titular de los certificados sobre el problema.	Operador de Registro
2	Notificar del problema por correo electrónico corporativo a la EC sobre el problema.	Operador de Registro
3	Registrar la fecha y la hora.	Operador de Registro
4	Hacer seguimiento de la solicitud hasta que sea ejecutada.	Operador de Registro
5	Comunicar al Responsable de la ER y registrar el hecho en un acta, incluyendo el tiempo de solicitud.	Área de soporte

5.3 AUTORIDAD DE LAS POLÍTICAS

El encargado de la ER designado es responsable de la administración de las políticas y actualización de los documentos.

5.3.1 PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS

Cualquier elemento de esta Declaración de Prácticas de Registro es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la web de la ER PERÚ MEDIA SECURITY SAC.

En la web de la ER PERÚ MEDIA SECURITY SAC se mantendrá un histórico con las versiones anteriores de las políticas.

Los usuarios afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación vía llamada telefónica (+511) 500 5441 - (+511) 500 54 42) o al correo entidad.registro@perusecurity.com.pe.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA (Departamento jurídico de Camerfirma).

Si un cambio en la política afecta de manera relevante a un número significativo de usuarios de la política, la PA (Departamento jurídico de Camerfirma) puede discrecionalmente asignar un nuevo OID a la política modificada.

5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

Para la aprobación y autorización de una ER se deberán respetar los procedimientos especificados por la PA (Departamento jurídico de Camerfirma). Las partes de la DPC de una ER que contenga información relevante en relación con su seguridad, toda o parte de esa DPC no estará disponible públicamente.

6 SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

6.1 SOLICITUD DE CERTIFICADOS A PERSONA JURÍDICA

6.1.1 SERVICIOS BRINDADOS

La ER PERÚ MEDIA SECURITY SAC brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de emisión, revocación y re-emisión[1] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

b) Atención de solicitudes de emisión, revocación y re-emisión[2] de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

c) Atención de solicitudes de emisión, revocación y re-emisión[3] de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

d) Atención de solicitudes de emisión, revocación y re-emisión[4] de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados brindados por la ER PERÚ MEDIA SECURITY SAC corresponden a AC CAMERFIRMA PERÚ S.A.C., acreditada ante el INDECOPI que se encuentran publicadas en la siguiente dirección: www.perusecurity.pe/repositorio

1 La re-emisión dependerá de lo establecido en la Política de Certificación de la AC CAMERFIRMA PERÚ, S.A.C.

2 La re-emisión dependerá de lo establecido en la Política de Certificación de la AC CAMERFIRMA PERÚ, S.A.C.

3 La re-emisión dependerá de lo establecido en la Política de Certificación de la AC CAMERFIRMA PERÚ, S.A.C.

4 La re-emisión dependerá de lo establecido en la Política de Certificación de la AC CAMERFIRMA PERÚ, S.A.C.

6.1.2 AUTORIZADAS PARA REALIZAR LA SOLICITUD

En todos los casos, tanto certificados para persona jurídica (de atributos como certificados para agentes automatizados), la solicitud debe ser hecha por un representante designado por la persona natural o jurídica, el cual deberá presentar al Operador de Registro de la ER un documento que acredite sus facultades como representante.

6.1.3 MODALIDADES DE ATENCIÓN

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante un contrato de adquisición de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de la ER de LA ER PERÚ MEDIA SECURITY SAC
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER
- De realizarse de manera remota, deberá realizarse mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de la ER PERÚ MEDIA SECURITY SAC, utilizando un certificado digital reconocido por el IOFE.

6.1.4 SOLICITUD DE CERTIFICADOS DE ATRIBUTOS

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado.

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado. Esta lista deberá ser debidamente firmada por el Representante Legal.

6.1.5 SOLICITUD DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

6.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Conforme con la Guía de Acreditación de ER del INDECOPI, en el caso de personas jurídicas, la ER PERÚ MEDIA SECURITY SAC no asignará un nombre de titular que haya sido ya asignado a un titular diferente. La ER PERÚ MEDIA SECURITY SAC se reserva el derecho de rechazar una solicitud de emisión de certificado digital a causa de un conflicto de nombres.

Por otro lado, no le corresponde a la ER PERÚ MEDIA SECURITY SAC determinar si al solicitante de un certificado digital le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado digital. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

6.1.7 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA JURÍDICA

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información proporcionada por los solicitantes será validada a través de un mecanismo de consulta a las bases de datos de Migraciones para validar la información del Carné de Extranjería. Para el caso de pasaporte será validada por la ER PERÚ MEDIA SECURITY SAC mediante la base de datos oficiales correspondiente. Se acreditará su existencia y vigencia mediante su pasaporte.

En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

6.1.8 CONTRATO DEL TITULAR

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato, que en adelante llamaremos “contrato del titular”. A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados. La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

6.1.9 VERIFICACIÓN DE SUSCRIPTORES

Los aspirantes a suscriptores son validados en cualquiera de las siguientes modalidades:

- De manera presencial en las instalaciones de la ER PERÚ MEDIA SECURITY SAC en calidad de ER.
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER
- De manera remota por video llamada grabada como evidencia de la atención y descarga del certificado, la llamada será realizada por un operador de la ER.

El proceso de verificación de sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER debe requerirá a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo. Además, debe presentar el original de su propio documento oficial de identidad.

6.2 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

6.2.1 SERVICIOS BRINDADOS

La ER PERÚ MEDIA SECURITY SAC brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de emisión, revocación y re-emisión[5] de certificados para personas naturales. Los certificados corresponden a la Entidad de Certificación de AC CAMERFIRMA PERÚ SAC, que se encuentran publicados en la siguiente dirección: www.camerfirma.com.pe

6.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

Aquellas que tienen plena capacidad de ejercicio de sus derechos civiles. Las personas naturales asumirán la responsabilidad de titulares y suscriptores de los certificados digitales que adquieran.

6.2.3 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada mediante un contrato de adquisición de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de la ER de PERU MEDIA SECURITY SAC
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER.
- De realizarse de manera remota, se realizará mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de la ER PERÚ MEDIA SECURITY SAC, utilizando un certificado digital reconocido por la IOFE.

5 La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de AC CAMERFIRMA PERÚ S.A.C.

6.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento, portando el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.

6.2.5 CONTRATO DEL SUSCRIPTOR

El solicitante deberá firmar un contrato, que en adelante llamaremos "contrato del suscriptor", el cual contiene las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por la ER PERÚ MEDIA SECURITY SAC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera digital o manuscrita por el solicitante, para luego ser archivado por la ER PERÚ MEDIA SECURITY SAC.

A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

6.2.6 VERIFICACIÓN DE SUSCRIPTORES

Los aspirantes a suscriptores deben ser validados en cualquiera de las siguientes modalidades:

- De manera presencial en las instalaciones de la ER PERÚ MEDIA SECURITY SAC en calidad de ER
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER.
- De manera remota por video llamada grabada como evidencia de la atención y descarga del certificado, la llamada será realizada por un operador de la ER.

6.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER PERÚ MEDIA SECURITY SAC a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, será validada por la ER PERÚ MEDIA SECURITY SAC a través de un mecanismo de consulta a las bases de datos de Migraciones para validar la información del Carné de Extranjería. Se acreditará su existencia y vigencia mediante su carnet de extranjería. Para el caso de pasaporte será validada por la ER PERÚ MEDIA SECURITY SAC mediante la base de datos oficiales correspondiente. Se acreditará su existencia y vigencia mediante su pasaporte.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER PERÚ MEDIA SECURITY SAC no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

7 PROCESAMIENTO DE LA SOLICITUD

7.1 RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de LA ER PERÚ MEDIA SECURITY SAC puede decidir establecer otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

7.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

En caso que una solicitud sea aprobada por la ER de LA ER PERÚ MEDIA SECURITY SAC realizará lo siguiente:

a) Comunicar a la EC su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la ER PERÚ MEDIA SECURITY SAC.

b) Se requerirá la firma del contrato del suscriptor.

7.3 REGISTRO DE DOCUMENTOS

La ER PERU MEDIA SECURITY SAC registra y archiva la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos son protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

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.

La comunicación entre los sistemas de registro y los sistemas de certificación de la EC serán realizadas por un canal cifrado SSL, mediante un certificado digital emitido por un EC con el sello de Webtrust o una certificación equivalente. Las comunicaciones entre la ER y la EC serán llevadas a cabo a través de mecanismos que permitan una comunicación ininterrumpida para garantizar la atención oportuna de las solicitudes de emisión del

certificado, así como la actualización de la relación de certificados emitidos y revocados. Las comunicaciones referidas a la aprobación o revocación de certificados serán llevadas a cabo mediante un mecanismo que garantice el no repudio.

7.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor.

Los módulos criptográficos distribuidos por LA ER PERÚ MEDIA SECURITY SAC cuentan con la certificación FIPS 140-2 o equivalente. Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la respectiva AC CAMERFIRMA PERÚ S.A.C., en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

7.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER PERÚ MEDIA SECURITY SAC enviará a la EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de cinco (05) días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

7.6 EMISIÓN DEL CERTIFICADO

La emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud. Dicho certificado tiene la vigencia de uno (1), dos (02) o tres (3) años.

8 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES

La ER PERÚ MEDIA SECURITY SAC recibe solicitudes de re-emisión rutinaria. La re-emisión rutinaria es un proceso programado, que puede ejecutarse cada vez que un nuevo par de claves debe ser emitido debido a que la fecha de expiración de un certificado digital es cercana y menor de un plazo máximo de un (01) año. Solamente los titulares de certificados digitales pueden solicitar la re-emisión por certificado digital.

Luego de la expiración de un certificado digital re-emitido, deberá seguirse el proceso de solicitud de emisión de un nuevo certificado digital.

8.1 SOLICITUD DE RE-EMISIÓN CERTIFICADOS DE PERSONA JURÍDICA

8.1.1 SERVICIOS BRINDADOS

La ER PERÚ MEDIA SECURITY SAC brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de re-emisión[7] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
b) Atención de solicitudes de re-emisión de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
c) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
d) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

c) Los certificados corresponden a AC CAMERFIRMA PERÚ S.A.C., acreditada y que se encuentra publicada en la siguiente dirección: www.camerfirma.com.pe

[7] La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de AC CAMERFIRMA PERÚ S.A.C.

8.1.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

Solo los titulares de certificados pueden solicitar la re-emisión de certificados, por lo que en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante así como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER PERÚ MEDIA SECURITY SAC, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

8.1.3 MODALIDADES DE ATENCIÓN

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER PERÚ MEDIA SECURITY SAC
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER, el Operador de Registro
- De realizarse de manera remota, se realizará mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER PERÚ MEDIA SECURITY SAC, utilizando un certificado digital reconocido por el INDECOPI.

8.1.4 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

8.1.5 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso de que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

8.1.6 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA JURÍDICA

La ER PERÚ MEDIA SECURITY SAC comprobará que la información del titular y del suscriptor contenida en la solicitud continúa siendo válida, respecto de la existencia de la persona jurídica en los Registros Públicos y de los suscriptores en la base de datos del RENIEC.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

En el caso de empresas constituidas en el extranjero, el solicitante deberá acreditar la continuidad de su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

En el caso de suscriptores extranjeros, estos tendrán que presentar al Operador de Registro, su documento oficial de identidad, pasaporte o carnet de extranjería que será validada por la ER PERÚ MEDIA SECURITY SAC a través de un mecanismo de consulta a las bases de datos de Migraciones para validar la información del Carné de Extranjería. Se acreditará su existencia y vigencia mediante su carnet de extranjería. Para el caso de pasaporte será validada por la ER PERÚ MEDIA SECURITY SAC mediante la base de datos oficiales correspondiente. Se acreditará su existencia y vigencia mediante su pasaporte.

8.2 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA NATURAL

8.2.1 SERVICIOS BRINDADOS

La ER PERÚ MEDIA SECURITY SAC brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de re-emisión[8] de certificados para personas naturales de nacionalidad peruana.

b) Atención de solicitudes de re-emisión[9] de certificados de atributos para personas naturales de nacionalidad extranjera.

c) Los certificados corresponden a AC CAMERFIRMA PERÚ S.A.C., acreditada y que se encuentra publicada en la siguiente dirección: www.camerfirma.com.pe

8.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado.

8.2.3 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER PERÚ MEDIA SECURITY SAC
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER, el Operador de Registro.
- De manera remota por video llamada grabada como evidencia de la atención y descarga del certificado, la llamada será realizada por un operador de la ER.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en LA ER PERU MEDIA SECURITY SAC, utilizando un certificado digital reconocido por la IOFE.

8.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

[8] La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de AC CAMERFIRMA PERÚ S.A.C.

[9] La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de AC CAMERFIRMA PERÚ S.A.C.

8.2.5 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER PERÚ MEDIA SECURITY SAC a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER PERÚ MEDIA SECURITY SAC no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

9 PROCESAMIENTO DE LA SOLICITUD DE RE-EMISIÓN

9.1 RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

La solicitud es rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar

con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de AC CAMERFIRMA PERÚ S.A.C., decide establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

9.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por la ER PERÚ MEDIA SECURITY SAC realizará lo siguiente:

a) Comunicar a la EC su aprobación para la re-emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC.

b) Se requerirá la firma del contrato del suscriptor.

9.3 REGISTRO DE DOCUMENTOS

La ER PERU MEDIA SECURITY SAC registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

9.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor, en un módulo criptográfico con la certificación FIPS 140-2. Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la EC de AC CAMERFIRMA PERÚ S.A.C., en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

9.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Una vez validada la identidad del solicitante, si el resultado de la validación es positivo, la ER PERÚ MEDIA SECURITY SAC enviará a la EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de cinco (05) días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

9.6 RE-EMISIÓN DEL CERTIFICADO

La re-emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud.

10 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

10.1 CIRCUNSTANCIAS PARA REALIZAR LA SOLICITUD

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica
- Cuando la información contenida en el certificado ya no resulte correcta.

- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Por decisión de la legislación respectiva.

10.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

10.2.1 SERVICIOS BRINDADOS

La ER PERÚ MEDIA SECURITY SAC brinda los siguientes servicios a personas jurídicas y naturales:

a) Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.

b) Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.

c) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

d) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

e) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

f) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados corresponden a AC CAMERFIRMA PERÚ S.A.C., que se encuentran publicadas en la siguiente dirección: www.camerfirma.com.pe

10.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

De acuerdo a lo estipulado por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son:

- El titular del certificado
- El suscriptor del certificado.
- La EC o ER que emitió el certificado.
- Un juez que de acuerdo a la Ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento.

En el caso de personas jurídicas, los titulares de certificados pueden solicitar la revocación de certificados, por lo que, en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

10.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS SOLICITANTES

En los casos de que la solicitud sea presencial:

- Los suscriptores deben presentar en la ER como mínimo su documento oficial de identidad.
- El representante asignado por la persona jurídica debe presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.

- Los terceros (diferentes de la EC, el suscriptor y el titular) deberán presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo a la ley vigente, junto a la orden judicial respectiva.

10.2.4 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada por los titulares y suscriptores mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER PERÚ MEDIA SECURITY SAC
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER, el Operador de Registro
- De manera remota, mediante una solicitud firmada digitalmente por el representante asignado por la persona jurídica o por el suscriptor. El certificado digital a emplear no debe ser el que se desea revocar. En caso de que la solicitud sea enviada firmada de manera manuscrita por correo electrónico deberá estar con firma legalizada por el representante asignado por la persona jurídica o por el suscriptor.
- De manera remota en una comunicación directa con la EC, mediante un control de acceso o contraseña brindados al suscriptor en el momento de la solicitud de emisión del certificado.

Para todos los demás actores, diferentes a los suscriptores y titulares, la solicitud deberá ser de manera presencial en las instalaciones de la ER PERÚ MEDIA SECURITY SAC.

La EC no requerirá realizar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato o en caso sea necesario por revocación del certificado de la EC. La EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su Declaración de Prácticas de Certificación y se encuentren de acuerdo con la legislación vigente.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER PERÚ MEDIA SECURITY SAC, utilizando un certificado digital reconocido por el INDECOPI.

10.2.5 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

10.2.6 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso de que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

10.2.7 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

11 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

11.1 RECHAZO DE LA SOLICITUD DE REVOCACIÓN EMISIÓN DE UN CERTIFICADO

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su

vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de AC CAMERFIRMA PERÚ S.A.C., puede decidir establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

11.2 APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por la ER PERÚ MEDIA SECURITY SAC realizará lo siguiente:

a) Comunicar a la EC su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC.

b) Una copia de dicha solicitud firmada será enviada a la EC o almacenada en la ER PERÚ MEDIA SECURITY SAC.

11.3 REGISTRO DE DOCUMENTOS

La ER PERU MEDIA SECURITY SAC registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de la misma a la EC de AC CAMERFIRMA PERÚ S.A.C., sus suscriptores y los terceros que confían.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad. En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

11.4 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER PERÚ MEDIA SECURITY SAC enviará a la respectiva EC la autorización de la revocación del certificado de manera inmediata.

El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación de la EC de AC CAMERFIRMA PERÚ S.A.C.

11.5 REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

12 GESTIÓN DE LA SEGURIDAD

Las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los servicios de registro son señaladas en la Política de Seguridad de LA ER PERU MEDIA SECURITY SAC.

12.1 AUTENTICACION DE OPERADORES DE REGISTRO

Los operadores de registro se autentican en los sistemas de registro mediante un certificado digital que se encuentra dentro de un token digital y mediante mecanismos de autenticación en doble factor, antes de tener acceso a solicitar la emisión, reemisión y revocación de certificados.

12.2 REGISTROS DE AUDITORÍA

Los sistemas de registro generarán registros de auditoría sobre las solicitudes de emisión, re-emisión y revocación de certificados, indicando el personal que hizo la solicitud, y el resultado positivo o fallido de la misma.

12.2.1 Tipos de eventos registrados

Los sistemas de información sensible son provistos por la EC, por lo que PERU MEDIA SECURITY SAC. en calidad Entidad de Registro de AC CAMERFIRMA PERU S.A.C. sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC.

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 PERU MEDIA SECURITY SAC. 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.

12.2.2 Frecuencia del procesamiento del registro

Los registros de auditoría son 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 incluye la verificación de que dichos registros no hayan sido manipulados.

12.2.3 Periodo de conservación del registro de auditorías

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

12.2.4 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.

12.2.5 Copia de seguridad del registro de auditoría

Todas las solicitudes y contratos físicos son generados con copia y los documentos electrónicos tiene una copia por los Operadores de Registro. Las copias son almacenadas en lugares diferentes como contingencia, protegidas contra acceso no autorizado por el Responsable de PERU MEDIA SECURITY SAC. en calidad Entidad de Registro de AC CAMERFIRMA PERU S.A.C.

12.2.6 Auditorías

Establecen los objetivos de las auditorías. Su frecuencia y sistemas implicados. PERU MEDIA SECURITY SAC cuenta con los siguientes documentos relacionados a las auditorias:

- PROCEDIMIENTO DE AUDITORÍAS INTERNAS (PAI)
- FORMATO DE AUDITORÍA INTERNA

12.2.7 Notificación al titular que causa un evento

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

12.2.8. Valoración de vulnerabilidad

Los sistemas de registro son administrados por cada EC, por lo que la protección perimetral de redes corresponde a cada EC.

12.3 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, son borrados o

destruidos de manera irrecuperable. En el caso de ser un archivo de papel se usan máquinas trituradoras de papel; en el caso de que sean archivos electrónicos que se encuentren en computadoras servidores o en la nube se eliminan también todas las copias de respaldo de todos los dispositivos de almacenamiento asociados con la computadora o servidor, de copias en la nube y de dispositivos de almacenamiento asociados con la plataforma en línea.

13 GESTIÓN DE OPERACIONES

13.1 MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores es realizada en módulos criptográficos FIPS 140-2.

Los módulos criptográficos usados por los Operadores de Registro deben cumplen los requerimientos o son equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

13.2 RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

13.3 DEPÓSITO DE CLAVE PRIVADA

La ER PERÚ MEDIA SECURITY SAC no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

13.4 DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de PERÚ MEDIA SECURITY SAC, se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

14 CONTROLES DE SEGURIDAD COMPUTACIONAL

Los sistemas de registro utilizados por LA ER PERÚ MEDIA SECURITY SAC son provistos y administrados por AC CAMERFIRMA PERÚ S.A.C., reconocida por la IOFE. La ER sólo accede a estos sistemas vía web con acceso vía certificados digitales de los Operadores de Registro.

15 SEGURIDAD DEL PERSONAL

15.1 DEFINICIÓN DE ROLES

La ER debe define los roles y sus privilegios de acceso y facultades asignadas dentro de las operaciones de registro. Las responsabilidades de administrar los sistemas para solicitar la emisión, re-emisión o revocación de los certificados digitales son claramente asignadas. 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 obtiene constancia por escrito del conocimiento de las mismas.

15.2 VERIFICACIÓN DE ANTECEDENTES

El personal de la ER son verificados respecto de sus antecedentes penales, policiales y crediticios. A fin de reducir las posibilidades de que un personal autorizado pueda prestarse a remitir certificados de suplantación de identidad.

15.3 CUALIDADES, REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los responsables de administrar los sistemas para solicitar la emisión, re-emisión y revocación de los certificados digitales cuentan con experiencia y conocimiento en el uso de certificados digitales o seguridad de la información. LA ER PERÚ MEDIA SECURITY SAC declara los requisitos de experiencia y calificaciones que exige a sus empleados.

15.4 COMPROMISO CONTRACTUAL DE CONFIDENCIALIDAD

El personal de la ER firma términos contractuales respecto de la protección de la privacidad y confidencialidad de la información presentada por los clientes de LA ER PERÚ MEDIA

SECURITY SAC. Las ER establecer en su RPS los términos de confidencialidad y provisiones de no revelación que gobierna al mismo, así como la legislación que rige a las transacciones que se realizan bajo el marco de la IOFE, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante, de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 6 de la Guía de Acreditación de ER. Esta información es entregada por escrito a los empleados y contratistas, debiéndose obtener declaración por escrito por parte de estas personas respecto al conocimiento de toda esta información. Esta información es incorporada en todos los contratos de trabajo o servicio.

15.5 RESPONSABILIDADES CONTRACTUALES

Definir cláusulas contractuales respecto de las responsabilidades y las consecuencias laborales y penales en caso de ocurrir eventos de compromiso de las operaciones de LA ER PERÚ MEDIA SECURITY SAC, incluyendo casos de suplantación de identidad por intervención del personal.

15.6 COMPROMISO DE CUMPLIR LA POLÍTICA DE SEGURIDAD

Definir cláusulas contractuales respecto del cumplimiento de la política de seguridad de la ER por parte de su personal.

15.7 CAPACITACIÓN

El personal de la ER, que administra los sistemas para la solicitud, re-emisión y revocación, debe recibe una capacitación continua respecto:

- Certificados digitales
- Firma digital
- Regulación de la IOFE
- Política de registro
- Políticas de seguridad y privacidad de LA ER PERÚ MEDIA SECURITY SAC
- RPS
- Plan de contingencia
- Funciones respecto de su rol
- Seguridad de la Información.

La frecuencia de las capacitaciones es de al menos una vez antes de operar en LA ER PERÚ MEDIA SECURITY SAC y luego de manera anual.

15.8 SANCIONES POR ACCIONES NO AUTORIZADAS

La ER establecer cláusulas contractuales respecto de las sanciones que pueden ejecutarse en caso de ocurrir ACCIONES no autorizadas o que pongan en riesgo la autenticidad de las operaciones de registro. Así como acciones penales en caso de participación en hechos de suplantación de identidad. Como mínimo, en el caso de una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona es inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

15.9 ROTACIÓN EN EL TRABAJO

No se implementará rotación de los trabajadores.

16 MATERIAS DE NEGOCIO Y LEGALES

16.1 TARIFAS

Las tarifas por los servicios de registro y certificación digital se indican en la sección 3.5. Tarifas.

16.2 POLÍTICAS DE REEMBOLSO

PERU MEDIA SECURITY SAC ofrece reembolso y/o cambio dentro de los 07 (siete) días calendarios después de tu compra, mientras no se haya iniciado el proceso de validación de identidad con nosotros. Si han transcurrido 07 días desde tu compra, no se ofrecerá un reembolso y/o cambio de ningún tipo. Tampoco hay reembolso, por problemas que el suscriptor (cliente) pueda tener directamente con SUNAT, SMV u otros agentes privados del mercado, donde el Certificado Digital no tenga relación.

Elegibilidad para reembolsos y cambios

- El proceso de validación no se haya iniciado, es decir, no se haya completado ningún dato personal en el portal de https://firmas.perusecurity.pe ya que el simple hecho de hacerlo, inicia dicho proceso de validación, lo que implica acciones y operaciones de validación de datos que pueden ser aprobados o rechazados en primera instancia.
- Recibo o comprobante de pago.
- Los reembolsos de los certificados sólo se pueden realizar al titular del mismo (suscriptor), y no de terceros.

Las solicitudes de reembolso elegibles y aceptadas, serán procesadas dentro de los 10 días hábiles siguientes.

16.3 COBERTURA DE SEGURO

PERU MEDIA SECURITY SAC proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil adquirida de manera independiente de AC CAMERFIRMA PERÚ S.A.C.

16.4 PROVISIONES Y GARANTÍAS

Las garantías por los servicios de registro y certificación digital serán definidas en los contratos de titulares, en relación con errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales acordes con La Ley nº29733 de Protección de Datos Personales y su Reglamento (Decreto Supremo 003-2013 JUS).

16.5 EXCEPCIONES DE GARANTÍAS

La ER PERÚ MEDIA SECURITY SAC no se responsabiliza en casos de compromiso de la clave en manos del suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento.

16.6 OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.

En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación de sus certificados en casos de compromiso de su clave privada.

16.7 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

16.8 INDEMNIZACIÓN

La ER podrá indemnizar al Titular/Suscriptor por el servicio que se presta de acuerdo al monto establecido en la normativa vigente.

16.9 NOTIFICACIONES

Los medios de notificación serán definidos en los contratos de titulares y suscriptores.

16.10 ENMENDADURAS Y CAMBIOS

Las enmendaduras y cambios serán comunicados al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

16.11 RESOLUCIÓN DE DISPUTAS

Para la resolución de disputas el titular/suscriptor escribe desde el correo electrónico que brindó a la ER con los argumentos de la disputa en mención al correo electrónico entidad.registro@perusecurity.com.pe para su revisión y del ser del ámbito será atendido brindando respuesta al titular/suscriptor.

De llegar a alguna disputa o incumplimiento entre las partes, los costos incluido el honorario de abogados será asumida por cada parte.

16.12 CONFORMIDAD CON LA LEY APLICABLE

La ER PERÚ MEDIA SECURITY SAC se compromete a cumplir la ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

16.13 CUMPLIMIENTO DE LA LEY APLICABLE

Este subcomponente se relaciona con los requisitos establecidos de que los participantes cumplan con la ley aplicable, por ejemplo, leyes relacionadas con hardware y software criptográfico que pueden estar sujetos a las leyes de control de exportaciones de una jurisdicción determinada. El CP o CPS podría pretender imponer dichos requisitos o puede exigir que tales disposiciones aparezcan en otros acuerdos.

16.14 SUBROGACIÓN

La ER PERÚ MEDIA SECURITY SAC no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes son especificados en este documento.

16.15 FUERZA MAYOR

La Entidad limita su responsabilidad en caso fortuito y en caso de fuerza mayor en las condiciones generales de emisión y uso del certificado.

16.16 VIGENCIA Y CONCLUSIÓN

La ER puede incluir el período de tiempo en el que una RPS sigue vigente y las circunstancias en que el documento, partes del documento, o su aplicabilidad a una determinada participante puede terminarse. Además, o alternativamente, la RPS puede indicar que los requisitos que cierta duración y cláusulas de terminación aparecen en los acuerdos, como los acuerdos de suscriptor o terceros de confianza acuerdos. En particular, tales condiciones pueden incluir:

- El término de un documento o acuerdo, es decir, cuando el documento se hace efectivo y cuando expira si no es capitulado primero.

- Disposiciones de terminación que indica las circunstancias bajo las cuales los

documentos, ciertas partes del mismo, o su aplicación a un participante en particular deja de permanecer en vigor.

- Las consecuencias de la terminación del documento. Por ejemplo, ciertas disposiciones de un acuerdo pueden sobrevivir a su terminación y permanecerá en vigor. Los ejemplos incluyen los reconocimientos de derechos de propiedad intelectual y disposiciones sobre confidencialidad. Además, la terminación puede desencadenar la responsabilidad de las partes en devolver información confidencial a la parte que la divulgó.

16.17 OTRAS PROVISIONES

La ER incluirá en su RPS o en los contratos otras disposiciones donde las responsabilidades y los términos que no encajan perfectamente dentro de uno de las secciones anteriores pueden ser impuestas a los participantes de la PKI.

17 FINALIZACIÓN DE LA ER PERÚ MEDIA SECURITY SAC

En caso de finalizar su actividad, la ER PERÚ MEDIA SECURITY SAC informará del cese de sus operaciones a las siguientes personas y autoridades:

- INDECOPI,
- Suscriptores y titulares
- Terceros que confían
- Entidades de Certificación

La referida comunicación se realizará por escrito por correo electrónico a la dirección de correo electrónico entidad.registro@perusecurity.com.pe con un periodo de anticipación de al menos sesenta (60) días.

Asimismo, se publicará la noticia en la página web de PERÚ MEDIA SECURITY SAC.

En caso de transferencia de actividad a otra Entidad de Registro, se ofrecerá a los suscriptores la posibilidad de mantener el contrato o desistir de ello. En caso de aceptar la

transferencia a otra Entidad de Registro, ésta deberá cumplir con los requerimientos de acreditación exigidos por el INDECOPI y se trasladará los expedientes de solicitudes y contratos a la nueva entidad para su gestión y custodia. En caso contrario, se podrán trasladar a la Entidad de Certificación emisora de los certificados o a otro Prestador designado por INDECOPI.

18 CONFORMIDAD

Este documento ha sido aprobado por la Autoridad de la ER PERÚ MEDIA SECURITY SAC, y tiene carácter normativo sobre todos los servicios de certificados digitales, 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/EC	Autoridad de Certificación / Entidad de Certificación
AR/ER	Autoridad de Registro / Entidad 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 Internacionalde 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 IntNet y un servidor.*

ANEXO II. DEFINICIONES

Autoridad de Certificación / Entidad 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 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	El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confi rmando su identidad.
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.ertificación 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 ocontraseñas 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	La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
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

PERU MEDIA SECURIT

Carlos Torres A
Gerente General