AN INFOCERT COMPANY

IN-2022-18-01

POLÍTICA Y PLAN DE PRIVACIDAD DE CAMERFIRMA PERÚ V.2.0

Firmado digitalmente por: XAVIER JOAQUIN URIOS HUIGENS
Rol: GERENTE GENERAL
Organización: CAMERFIRMA PERU S.A.C.
Unidad organizacional: GERENCIAIssued by AC CAMERFIRMA PER\xC3\x9A SAC ER [PE1]
Limitación de uso: Explicit Text: CERTIFICADO DE PERSONA FISICA CON VINCULACION A EMPRESA
Fecha: 22/08/2022 17:39:49

ÍNDICE

1. TRATAMIENTO DEL DOCUMENTO

1.1 CONTROL DE ACTUALIZACIONES

VERSIÓN	FECHA	ELABORADO	ACTUALIZACIÓN	BORRADOR	APROBADO
1.0	Abril 2017		Ramiro Muñoz		Ramiro Muñoz
2.0	Diciembre 2021		Ramiro Muñoz		Ramiro Muñoz
2.1	Junio 2022	Innovate DC (Consultor Externo)			Ramiro Muñoz

1.2 CONTROL DE CAMBIOS

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

1.3 MANTENIMIENTO DEL DOCUMENTO

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

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

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

- Aprobado por la Responsable de la Entidad de Registro.

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

1.4 VALIDEZ

Hasta su siguiente actualización.

1.5 TRATAMIENTO Y CONFIDENCIALIDAD

Documento de acceso al público.

1.6 DISTRIBUCIÓN

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

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

2. INTRODUCCIÓN

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

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

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

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

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

2.1 VISTA GENERAL

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

2.2 IDENTIFICACIÓN

Nombre de la Política:	Política y Plan de Privacidad de la Entidad de Registro de Camerfirma Perú
Descripción:	Define los criterios básicos a seguir por el prestador de servicios de certificación que ofrezca servicios de Entidad de Registro
Versión:	2.1
Fecha de Emisión:	Junio 2022
Localización:	http://www.camerfirma.com/

2.3 COMUNIDAD Y ÁMBITO DE APLICACIÓN

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

2.3.1 ENTIDAD DE CERTIFICACIÓN

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

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

2.3.2 ENTIDAD DE REGISTRO

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

2.3.3 PROVEEDOR DE SERVICIOS E INFRAESTRUCTURA

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

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

2.3.4 TITULAR

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

2.3.5 SUSCRIPTOR

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

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

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

2.3.6 PARTE USUARIA

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

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

2.3.7 SOLICITANTE

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

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

2.4 USOS DEL CERTIFICADO DIGITAL

2.4.1 ÁMBITO DE APLICACIÓN Y USOS

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

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

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

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

2.4.2 USOS PROHIBIDOS Y NO AUTORIZADOS

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

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

3. POLÍTICAS DE PRIVACIDAD DE DATOS PERSONALES DE LA ER

Camerfirma Perú garantiza la protección de datos personales de los suscriptores y titulares de los servicios de registro, en cumplimiento de la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación de Entidades de Registro o Verificación, en los ámbitos legales, regulatorios y contractuales.

Serán considerados como datos personales, la información de nombres, dirección, correo electrónico y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los contratos y solicitudes de los suscriptores y titulares. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de registro, a excepción que exista un previo consentimiento del titular de dichos datos o medie una orden judicial o administrativa que así lo determine.

Con este fin, se implementará un Plan de Privacidad con controles para la protección contra divulgación y uso no autorizado.

Es responsabilidad de los suscriptores garantizar que la información provista a la ER sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos.

4. PLAN DE PRIVACIDAD DE DATOS PERSONALES DE LA ER

4.1 INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de registro, Camerfirma Perú en calidad de ER recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.

- Contrato de solicitud de servicios.

4.2 TRATAMIENTO DE LOS DATOS PERSONALES

- Información no privada

Deberá considerarse como información no privada, la información personal públicamente disponible.

En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

- Información privada

Deberá considerarse como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.

- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de sellado de tiempo.

- En todos los casos, figurará en la Política de Privacidad que deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada únicamente será divulgada en caso que exista consentimiento previo y por escrito firmado para tales efectos por el titular de dicha información o medie una orden judicial o administrativa que así lo determine.

Cualquier violación a la privacidad de esta información por parte del personal de la ER de Camerfirma Perú o de los terceros subcontratados, será sujeto de sanción

4.3 FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular de transferir los datos personales contenidos en los certificados digitales a las locaciones de Camerfirma España, como prestador de servicios de Camerfirma Perú.

4.4 IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente documento adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

- Medidas preventivas

a) Se restringirá el acceso a los datos personales a los Operadores de Registro.
b) Estos datos serán protegidos contra acceso no autorizado.
c) Se concientizará al personal para no divulgar o exponer de manera accidental datos personales de los usuarios.
d) Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de los servicios de sellado de tiempo, las mismas que deben informar sobre:
   - El hecho de que se está recolectando información personal;
   - Los propósitos para los cuales se recolecta dicha información personal;
   - Los tipos de personas u organizaciones a las que dicha información podría ser revelada;
   - La identidad y ubicación del responsable de la información personal, incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal;
   - Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.
   - Deben tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.
e) Puede no resultar apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

- Limitaciones a la recolección

La recolección de información personal debe encontrarse limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información deberá ser obtenida de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

- Uso de la información personal

La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:

- Que exista consentimiento del individuo al que pertenece la información personal recolectada;
- Que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o
- Que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

- Elección

Cuando sea apropiado, se proveerá a los individuos mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin que puedan decidir respecto a la recolección, uso y revelación de su información personal. Puede no resultar necesario que los responsables de la información provean estos mecanismos en los casos de recolección de información que sea públicamente disponible.

- Integridad de la información personal

La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

- Salvaguardas a la seguridad

Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones y reevaluaciones periódicas.

- Acceso y corrección

a) Los individuos deben ser capaces de:
   - Obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne.
   - Comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible; y
   - Cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.

b) Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:
   - La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;
   - La información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
   - Se podría violar la privacidad de la información de personas diferentes al individuo.

Si una solicitud bajo el supuesto (a) o (b) es denegado, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

5. RESPONSABILIDAD

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

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

www.camerfirma.com

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

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

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

5.1 RESPONSABLE DE LOS DOCUMENTOS DE LA ER

Nombre: Xavier Urios

Cargo: Gerente General de Camerfirma Perú

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

5.2 RESPONSABLE DE PRIVACIDAD

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

6. CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

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

7. CONFORMIDAD

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

ANEXO I. ACRÓNIMOS

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

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

ANEXO II. DEFINICIONES

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

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

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