ENTIDAD DE CERTIFICACIÓN

POLÍTICA DE CERTIFICACIÓN V1.0

Nombre del documento	Política de Certificación
Realizado por	GIRASOL PE SCRL
Aprobado por	Responsable de la EC
Código del documento	EC-PC-20102024
Versión	1.0
Fecha	20/10/2024

FirmEasy
PAGANO FAUSTINO GUILLERMO FOSHLEN
Fecha: 21/10/2024 13:01
Firmado por Firmeasy.legal

HISTORIAL DE VERSIÓN		
Versión	**Fecha**	**Descripción**
1.0	20/10/2024	Documento inicial

ÍNDICE

1. INTRODUCCIÓN Y ALCANCE DEL SERVICIO

1.1. PRESENTACIÓN

GIRASOL PE SCRL a la que denominaremos "GIRASOL.PE", es una empresa peruana establecida en 2019, dedicada a brindar servicios de Gestión Documental, Trámite Documentario Electrónico, Seguridad Digital, Certificados Digitales y Firma Electrónica.

En el año 2020 GIRASOL.PE logró acreditarse como Entidad de Registro ante la Autoridad Administrativa Competente como Entidad de Registro para brindar a sus clientes servicios de registro o verificación, incluidos representantes legales, empleados o agentes automatizados.

En el año 2023 GIRASOL.PE logró acreditar su software de firma digital Firmeasy - Firma Digital versión 1.0 ante la Autoridad Administrativa Competente desde donde se puede firmar documentos PDF con validez jurídica.

En el año 2024 GIRASOL.PE logró acreditarse como Entidad de Certificación ante la Autoridad Administrativa Competente para proveer servicios de emisión, re-emisión y revocación de certificados digitales.

Los tipos de certificados digitales que proporciona GIRASOL.PE son:

- Certificados digitales de Persona Natural.
- Certificados digitales de Profesional Independiente.
- Certificados digitales de Persona Jurídica.
- Certificados digitales de Agente Automatizado.
- Certificados digitales de Profesional vinculado a una empresa.
- Certificados digitales de facturación electrónica firmada en XML requeridos por la SUNAT de Perú.

GIRASOL.PE adecua sus servicios de certificación digital de acuerdo a las siguientes normativas:

- Guía de Acreditación de Entidades de Registro o Verificación, Entidad de Certificación Digital y Software de Firma Digital del INDECOPI.
- Ley 27269 - Ley de firmas y certificados digitales.
- Decreto Supremo N. 052 - 2008 - PCM Reglamento de la Ley de firmas y Certificados Digitales.
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures).

La estructura de este documento está basada en la especificación del estándar RFC 3647- Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

1.2. OBJETIVO

Este documento tiene como objetivo describir las operaciones y prácticas, los perfiles, los tipos de usuarios y usos definidos por GIRASOL.PE como Entidad de Certificación en el marco del cumplimiento de los requisitos de las "Guías de Acreditación de Entidades de Certificación Digital (EC)" establecida por INDECOPI.

1.3. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital de GIRASOL.PE.

1.4. NOMBRE O IDENTIFICACIÓN DEL DOCUMENTO

Nombre del documento	Política de Certificación
Código del documento	EC-DPC-20102024
Versión	1.0
Descripción	Declaración de Prácticas de Certificación de GIRASOL.PE bajo las jerarquías de FirmEasy Root CA y FirmEasy SubCA
Fecha de publicación	27/06/2024
Clasificación de seguridad	Público
OID	**1.3.6.1.4.1.61580.0.1.0: PC**
Repositorio	www.girasol.pe

2. PARTICIPANTES DE LA PKI

2.1. ENTIDAD DE CERTIFICACIÓN (EC - GIRASOL.PE)

GIRASOL.PE, como entidad certificadora autorizada, es una entidad jurídica privada que proporciona los servicios de emisión, reemisión y revocación de certificados digitales.

Bajo esta DPC, GIRASOL.PE gestiona las siguientes jerarquías de EC:

- **Autoridad de Certificación Raíz:** Se denomina Autoridad de Certificación Raíz (CA Root) a la entidad dentro de la jerarquía que emite certificados a otras Autoridades de Certificación, y cuyo certificado de clave pública ha sido autofirmado.

  Su función es firmar el certificado de las otras EC pertenecientes a la jerarquía de Certificación.

CN	FirmEasy Root CA
VALIDEZ	Desde el 16 de octubre del 2024 hasta el 13 de octubre del 2039
TIPO DE CLAVE	RSA 4096 bits - SHA256

- **Autoridad de Certificación Subordinada:** Se denomina Autoridad de Certificación Subordinada (CA Sub) a las Entidades dentro de la jerarquía de certificación que emiten certificados de usuario final y cuyo certificado de clave pública ha sido firmado digitalmente por la Autoridad de certificación Raíz.

  Su función es emitir certificados a personas naturales y jurídicas, conforme a lo establecido en las Guías de Acreditación de Entidad de Certificación del INDECOPI.

CN	FirmEasy SUBCA
VALIDEZ	Desde el 16 de octubre del 2024 hasta el 08 de octubre del 2039
TIPO DE CLAVE	RSA 4096 bits - SHA256

2.2. ENTIDAD DE REGISTRO (GIRASOL.PE)

GIRASOL.PE presta los servicios de una entidad de registro que se encarga de verificar la identidad y los poderes de representación del solicitante, para acreditar la validez de la información proporcionada por el solicitante del certificado digital.

Podrán actuar como ER de GIRASOL:

- GIRASOL.PE directamente.
- Cualquier Entidad de Registro debidamente acreditada ante el INDECOPI que llegue a un acuerdo con GIRASOL.PE para la emisión de certificados a personas naturales o jurídicas.
-

2.3. TITULAR

Es la persona natural o jurídica cuyo nombre se expide en un certificado digital y por tanto actúa como responsable del mismo, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la DPC.

2.4. SUSCRIPTOR

Según IOFE, el suscriptor es responsable de utilizar la clave privada, que está específicamente vinculada a un documento electrónico que se firma digitalmente con su clave privada.

Si el titular del certificado digital es una persona natural, la responsabilidad del suscriptor recaerá sobre él. Si la persona jurídica es la titular del certificado digital, la responsabilidad del suscriptor correrá a cargo del representante legal designado por la entidad.

Si el certificado está diseñado para ser utilizado por un agente automatizado, la propiedad del certificado y la firma digital generada a partir del certificado corresponderá a la persona jurídica.

A tal efecto, la atribución de la responsabilidad del suscriptor corresponde a la misma persona jurídica.

2.5. SOLICITANTE

Se entenderá por solicitante a la persona natural o jurídica que haya obtenido un certificado emitido bajo esta DPC. Si se trata de un certificado de persona natural, puede coincidir con la identidad del titular.

2.6. TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Son las personas jurídicas o naturales que deciden optar por el servicio de validación y de registro de la ER DE GIRASOL PE, así como los certificados digitales emitidos por la EC de GIRASOL.PE, el tercero que confía, a su vez puede ser o no el titular.

2.7. ENTIDAD A LA QUE SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización que tenga una relación cercana con el titular a través de la relación acreditada en el certificado.

3. CARACTERÍSTICAS DE LOS CERTIFICADOS

3.1. PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los certificados de GIRASOL.PE tendrán un periodo de validez de hasta 3 años.

3.2. TIPOS DE SOPORTE

Los certificados de GIRASOL.PE se emiten en formato PKCS#10.

3.3. USO PARTICULAR DE LOS CERTIFICADOS

3.3.1 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados emitidos por GIRASOL.PE se usan para los siguientes propósitos:

- Autenticación del suscriptor. El Suscriptor del certificado puede autenticar 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 no fue alterado o modificado después de la firma del suscriptor.
- No repudio de origen: Con el uso de este certificado también se garantiza que la persona que firma el documento no puede repudiar, es decir, el suscriptor que ha firmado no puede negar la autoría o la integridad del mismo.

3.3.2 USOS PROHIBIDOS DE LOS CERTIFICADOS

Los certificados emitidos por GIRASOL.PE no pueden ser utilizados para las siguientes circunstancias:

- Cuando contravengan la Ley de Firmas y Certificados Digitales – Ley 27269, las Guías de Acreditación del INDECOPI o sus anexos.

3.4. TARIFAS

Los precios de los servicios de certificación o otros servicios relacionados estarán disponibles en la página web de GIRASOL.PE.

4. PROCEDIMIENTOS OPERATIVOS

4.1. SOLICITUD DEL CERTIFICADO

4.2. PROCESAMIENTO DE LA SOLICITUD DE CERTIFICADOS

9.2.1 Ejecución de las funciones de identificación y autenticación

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

9.2.2 Aprobación o rechazo de la solicitud

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

9.2.3 Plazo para resolver la solicitud

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

4.3. EMISIÓN DE CERTIFICADOS

9.3.1 Acciones de la EC durante el proceso de emisión

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

9.3.2 Notificación de la emisión al suscriptor

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

4.4. ENTREGA Y ACEPTACIÓN DEL CERTIFICADO

9.4.1 Forma en la que se acepta el certificado

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

9.4.2 Publicación del certificado

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO

9.5.1 Uso del certificado y la clave privada del suscriptor

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

9.5.2 Uso de la clave pública y del certificado por la parte que confía

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de GIRASOL.PE, disponible en la siguiente página web: www.girasol.pe

4.6. RE-EMISIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES DE GIRASOL.PE

GIRASOL.PE no permite la re-emisión de certificados sin renovación de claves.

4.7. RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

La remisión de un certificado con cambio de claves es el proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado antes de su expiración, cuando su fecha de expiración está próxima o cuando deba ser sustituido (sin modificación de los datos esenciales).

GIRASOL.PE comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Si el suscriptor no solicita la re-emisión de certificado, el certificado expirará. Luego de ello, el suscriptor deberá realizar el proceso de validación de identidad desde la etapa inicial.

4.8. MODIFICACIÓN DE CERTIFICADOS

En caso de necesidad de modificar algún dato, GIRASOL.PE procederá a la revocación y a la emisión de un nuevo certificado.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible. Las revocaciones tienen efecto desde el momento en que aparecen publicadas en la CRL o en el servicio OCSP. No se contempla la suspensión de certificados. GIRASOL.PE no realiza suspensiones de certificados.

5. TIPOS DE CERTIFICADOS

La siguiente tabla muestra los tipos de certificados digitales emitidos por GIRASOL.PE.

Tipo de certificado	Descripción
Certificado de Persona Natural	Son certificados que permiten a la persona natural firmar electrónicamente documentos asegurando así su identidad.
Certificado de Profesional Independiente	Son certificados que identifican digitalmente a una persona y lo asocia a un colegio profesional específico, permitiendo al profesional ejercer legalmente su profesión.
Certificado de Persona Jurídica	Son certificados que identifican digitalmente a una persona jurídica y es vinculada a una entidad informando del cargo que desempeña en ella.
Certificado de Agente Automatizado	Son certificados para dispositivos informáticos, programas o aplicaciones dedicadas a firmar de forma automatizada en nombre de la Persona Jurídica en sistemas de firma.
Certificado de Profesional vinculado a una empresa	Son certificados que identifican digitalmente a una persona vinculada a una entidad y lo asocia a un colegio profesional específico, permitiendo al profesional ejercer legalmente su profesión.
Certificado de Facturación Electrónica	Son certificados que permiten la firma de facturas, boletas y otros documentos tributarios, cumpliendo con lo exigido por la SUNAT

6. PERFILES DE LOS CERTIFICADOS

6.1. PERFIL DE LOS CERTIFICADOS

El perfil de los certificados de GIRASOL.PE son conforme a los estándares IETF RFC 5280 e "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (TBSCertificate)

Campo del certificado		Descripción	Valor
version		N° de versión	v3
serialNumber		N° de serie	Número entero positivo único con respecto a la CA que emite el certificado
signature		Algoritmo de firma	OID y parámetros del algoritmo de firma
issuer		Emisor (DN)	DN de la CA que emite el certificado
validity	**notBefore**	Válido desde	Fecha y hora de inicio de validez del certificado, tiempo UTC
	notAfter	Válido hasta	Fecha y hora de fin de validez del certificado, tiempo UTC
subject		Asunto (DN)	DNI del suscriptor del certificado
subjectPublicKeyInfo		Clave pública	OID y parámetros del algoritmo y valor de la clave pública
extensions		Extensiones del certificado	Extensiones del certificado

12.1.1 Número de versión

Los certificados siguen el estándar de certificados X.509 versión 3.

12.1.2 Extensiones de los certificados

Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Raíz, obtenido a partir del hash SHA-1 de la misma
Subject Key Identifier	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage	Sí	Para la CA

		key CertSign, cRLSign Para los usuarios finales digital Signature, nonRepudiation
Certificate Policies	-	OID anyPolicy (2.5.29.32.0) URI de la DPC https://girasol.pe/[2]
Basic Constraints	Sí	cA: TRUE pathLenConstraint: 0
CRL Distribution Points	-	URI de la CRL: https://girasol.pe/[2]
Authority Information Access	-	URI del certificado de la CA Raíz: https://girasol.pe/[2]
Extended Key Usage	-	Para los usuarios finales clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)

12.1.3 Identificadores de objeto OID de los algoritmos utilizados

OID	Nombre	Descripción
1.2.840.113549.1.1.11	sha256WithRSAEncryption	OID del algoritmo de firma
1.2.840.113549.1.1.1	rsaEncryption	OID de Clave pública

12.1.4 Formatos de nombres

Atributo del DN	Descripción	Valor
Country Name (C)	País	PE [1]
State or Province Name (ST)	Estado/Provincia	*Departamento donde reside el suscriptor*
Locality Name (L)	Localidad	*Distrito donde reside el suscriptor*

Street Address (STREET)	Dirección	*Dirección donde reside el suscriptor*
Serial Number (serialNumber)	Número de Serie	*TipoDoc-NumDoc* *TipoDoc*: *Tipo de documento de identificación del suscriptor DNI ó CE* *NumDoc*: *Número de documento de identificación del suscriptor*
Surname (SN)	Apellidos	*Apellidos del suscriptor*
Given Name (givenName)	Nombre de Pila	*Nombre del suscriptor*
Common Name (CN)	Nombre	*Nombre completo (nombre y apellidos) del suscriptor*

12.1.5 Restricciones de los nombres

Respecto a la codificación de los atributos de los DN de los certificados, siguiendo el estándar RFC 5280 ”Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”), se emplea la codificación UTF8String en todos los atributos, contengan o no caracteres especiales, excepto en los atributos en los que es obligatorio utilizar la codificación PrintableString (C, Country; Serial Number).

12.1.6 Identificador de objeto OID de la política de certificación

Los certificados de usuario final contienen un OID, que parte de la base 1.3.6.1.4.1.61580, que identifica la DPC de GIRASOL.PE.

Los certificados de Autoridad Raíz y Autoridad Subordinada, en general, contienen el OID de PC 2.5.29.32.0 (anyPolicy)

7. ADMINISTRACIÓN DE LA PC

7.1. ORGANIZACIÓN RESPONSABLE

GIRASOL.PE administra los documentos de Declaración de Prácticas de Certificación, Política de Certificación, Política de Seguridad, Política y Plan de Privacidad y todos los documentos normativos de la EC de GIRASOL.PE.

7.2. PERSONA DE CONTACTO

ORGANIZACIÓN RESPONSABLE	GIRASOL PE SCRL
PERSONA DE CONTACTO	Responsable de la Entidad de Certificación
CORREO ELECTRÓNICO	soporte@girasolpe.com
DIRECCIÓN	Jr. Túpac Yupanqui Nro. 143 Amarilis - Huánuco - Perú
TELÉFONO	+51 987 592 655
PÁGINA WEB	www.girasol.pe

7.3. FRECUENCIA DE REVISIÓN

Esta PC así como todos los documentos normativos serán revisadas y, si procede, actualizadas de manera anual.

7.4. PROCEDIMIENTO DE APROBACIÓN

Esta PC así como todos los documentos normativos son aprobados y firmados por el Responsable de la Entidad de Certificación antes de ser publicadas.

Las nuevas versiones aprobadas de esta DPC así como todos los documentos normativos serán enviadas al INDECOPI y publicadas en la página web de GIRASOL.PE www.girasol.pe

Los cambios realizados serán registrados en la tabla de “Historial de Versión”, a fin de evitar modificaciones y suplantaciones no autorizadas.

7.5. PROCEDIMIENTO DE QUEJAS Y DISPUTAS

Los solicitantes, suscriptores, terceros que confían o el público en general indicarán su consulta con respecto a los servicios de certificación digital ofrecidos por GIRASOL.PE enviando un correo electrónico a la siguiente dirección soporte@girasolpe.com

Las peticiones, quejas o reclamos serán registradas en nuestra plataforma de incidencias y atendidas por parte del personal responsable de GIRASOL.PE.

El usuario recibirá un mensaje de correo electrónico confirmando la recepción de la petición, queja o reclamo y cuando ésta sea resuelta.

8. DEFINICIONES Y ACRÓNIMOS

Entidad de Certificación – EC:	Entidad que brinda la emisión, revocación, renovación, modificación y suspensión de servicios de certificados digitales en el marco de la normativa establecida por IOFE.
Entidad de Registro – ER:	Entidades que realizan el proceso de verificación de identidad de solicitantes de servicios de certificación digital.
Política de Certificación - PC:	Un conjunto de reglas que indican el marco de aplicabilidad del servicio para la comunidad de usuarios definida.
Certificado:	Archivo que asocia la clave pública con datos del suscriptor y es firmado por la EC.
Clave Pública:	Valor matemático conocido públicamente y usado para la verificación de una firma digital.
Clave Privada:	Valor matemático usado únicamente por el suscriptor para la creación de una firma digital.
Lista de Certificados Revocados - CRL:	Archivo que contiene una lista de los certificados que han sido revocados en una fecha y hora determinada y que es firmada por la EC.
Declaración de Prácticas de Certificación - DPC:	Conjunto de prácticas adoptadas por una Entidad de Certificación para la emisión, gestión, revocación y reemisión de certificados digitales.
FIPS	Federal Information Processing Standards (FIPS; en español, Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de

	todas las agencias del gobierno no militares y por los contratistas del gobierno.
Firma Digital:	Resultado de la transformación de un mensaje, o cualquier tipo de datos, 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); y c) que la persona que firma los datos no puede negar haberlo hecho.
HASH	Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
HSM:	Dispositivo Hardware que genera y protege claves criptográficas, y permite utilizarlas para realizar operaciones criptográficas de modo seguro.
OID:	Identificador numérico único registrado bajo la estandarización ISO y que se refiere a un objeto o clase de objeto determinado.
PKI	Conjunto de hardware, software, recursos humanos, procedimientos, etc, que componen un sistema usado para la creación y gestión de certificados de clave pública.
Suscriptor	Persona natural o jurídica a cuyo nombre se expide un certificado digital.
Titular:	Una entidad que requiere los servicios provistos por la EC y acepta los términos y condiciones del servicio descrito en este documento.
Tercero que confía:	Una persona que recibe documentos, registros o notificaciones firmados digitalmente y cree en la validez de las transacciones realizadas.

9. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

GIRASOL.PE es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación para Entidades de Certificación Digital EC, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales – Ley 27269, para el reconocimiento legal de los servicios que brinda la EC de GIRASOL.PE bajo las directrices de nidas en el presente documento.

10. CONFORMIDAD

Esta Política de Certificación ha sido aprobada por el Responsable de la EC. Cada vez que se genere un cambio en este documento, se procederá a informar previamente a INDECOPI y al dar conformidad, será publicada en nuestra página web.

11. BIBLIOGRAFÍA

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo N° 052-2008-PCM, y sus modificatorias.
- Decreto Supremo N° 070-2011-PCM.
- Decreto Supremo N° 105-2012-PCM.
- Guía de Acreditación de Entidad de Certificación Digital - INDECOPI.

GIRASOL.PE