



**ENTIDAD DE CERTIFICACIÓN**  
**POLÍTICA DE CERTIFICACIÓN V1.0**

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

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

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

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

## ÍNDICE

1. INTRODUCCIÓN Y ALCANCE DEL SERVICIO	10
1.1. PRESENTACIÓN	10
1.2. OBJETIVO	11
1.3. OBJETO DE LA ACREDITACIÓN	11
1.4. NOMBRE O IDENTIFICACIÓN DEL DOCUMENTO	11
2. PARTICIPANTES DE LA PKI	11
2.1. ENTIDAD DE CERTIFICACIÓN (EC - GIRASOL.PE)	11
2.2. ENTIDAD DE REGISTRO (GIRASOL.PE)	12
2.3. TITULAR	13
2.4. SUSCRIPTOR	13
2.5. SOLICITANTE	13
2.6. TERCERO QUE CONFÍA EN LOS CERTIFICADOS	13
2.7. ENTIDAD A LA QUE SE ENCUENTRA VINCULADO EL TITULAR	14
3. TIPOS DE CERTIFICADOS	14
4. USOS DEL CERTIFICADO	15
4.1. USOS APROPIADOS DE LOS CERTIFICADOS	15
4.2. USOS PROHIBIDOS DE LOS CERTIFICADOS	15
5. ADMINISTRACIÓN DE LA POLÍTICA	15
5.1. ORGANIZACIÓN RESPONSABLE	15
5.2. PERSONA DE CONTACTO	15
5.3. FRECUENCIA DE REVISIÓN	16
5.4. PROCEDIMIENTO DE APROBACIÓN	16
5.5. PROCEDIMIENTO DE QUEJAS Y DISPUTAS	16
6. DEFINICIONES Y ACRÓNIMOS	16
7. PUBLICACIÓN Y RESPONSABILIDAD DEL REPOSITORIO	19
7.1. REPOSITORIOS	19
7.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN	19
7.2.1. Políticas y Prácticas de Certificación	19
7.2.2. Términos y Condiciones	20
7.2.3. Difusión de los certificados	20
7.3. FRECUENCIA DE PUBLICACIÓN	20
7.4. CONTROLES DE ACCESO A LOS REPOSITORIOS	20
8. IDENTIFICACIÓN Y AUTENTICACIÓN	20
8.1. REGISTRO DE NOMBRES	20
8.1.1. Tipos de nombres	21
8.1.2. Necesidad de que los nombres sean significativos	21
8.1.3. Uso de seudónimos	21
8.1.4. Reglas para la interpretación de varias formas de nombre	21

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

8.1.5 Singularidad de los nombres	21
8.1.6 Reconocimiento, autenticación y papel de las marcas reconocidas	21
8.2. VALIDACIÓN INICIAL DE LA IDENTIDAD	21
8.2.1. Método de prueba de posesión de la clave privada	21
8.2.2 Autenticación de la identidad de una organización	22
8.2.3 Autenticación de la identidad de una persona natural	22
8.2.4 Validación de correo electrónico	22
8.2.5 Validación de la Autoridad	23
8.2.6 Criterios para la interoperación	23
8.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN	23
8.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN	23
9. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS	24
9.1. SOLICITUD DEL CERTIFICADO	24
9.1.1 Quién puede solicitar un certificado	24
9.1.2 Proceso de solicitud de certificados	24
9.2. PROCESAMIENTO DE LA SOLICITUD DE CERTIFICADOS	24
9.2.1 Ejecución de las funciones de identificación y autenticación	24
9.2.2 Aprobación o rechazo de la solicitud	24
9.2.3 Plazo para resolver la solicitud	25
9.3. EMISIÓN DE CERTIFICADOS	25
9.3.1 Acciones de la EC durante el proceso de emisión	25
9.3.2 Notificación de la emisión al suscriptor	25
9.4. ENTREGA Y ACEPTACIÓN DEL CERTIFICADO	25
9.4.1 Forma en la que se acepta el certificado	25
9.4.2 Publicación del certificado	25
9.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO	25
9.5.1 Uso del certificado y la clave privada del suscriptor	25
9.5.2 Uso de la clave pública y del certificado por la parte que confía	25
9.6. RE-EMISIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES DE GIRASOL.PE	26
9.7. RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES	26
9.8. MODIFICACIÓN DE CERTIFICADOS	26
9.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS	26
9.9.1 Circunstancia para la revocación	26
9.9.2 Quién puede solicitar una revocación	27
9.9.3 Procedimiento de solicitud de revocación	27
9.9.4 Periodo de gracia de la solicitud de revocación	27
9.9.5 Plazo en la que la EC debe procesar la solicitud de revocación	28
9.9.6 Requisitos de verificación de las revocaciones por los terceros que	

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

confían	28
9.9.7 Frecuencia de emisión de CRL	28
9.9.8 Máxima latencia para la CRL	28
9.9.9 Disponibilidad de comprobación en línea de la revocación	28
9.9.10 Requisitos de comprobación de la revocación On-Line	28
9.9.11 Otras formas disponibles de divulgación de información de revocación	29
9.9.12 Requisitos especiales en relación con el compromiso de claves privadas	29
9.9.13 Circunstancias para la suspensión	29
9.9.14 Quién puede solicitar la suspensión	29
9.9.15 Procedimiento de solicitud de suspensión	29
9.9.16 Límites de periodo de suspensión	29
9.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS	29
9.10.1 Características operacionales	29
9.10.2 Disponibilidad del servicio.	30
9.11. FINALIZACIÓN DE LA SUSCRIPCIÓN	30
9.12. CUSTODIA Y RECUPERACIÓN DE CLAVES	30
10. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONES	30
10.1. CONTROLES FÍSICOS	30
10.1.1 Ubicación y construcción	31
10.1.2 Acceso físico	31
10.1.3 Alimentación eléctrica y aire acondicionado	31
10.1.4 Exposición al agua	31
10.1.5 Protección y prevención de incendios	31
10.1.6 Sistema de almacenamiento	32
10.1.7 Eliminación de residuos	32
10.1.8 Copia de respaldo externa	32
10.2. CONTROLES PROCEDIMENTALES	32
10.2.1 Roles de confianza	32
10.2.2 Número de personas requeridas por tarea	32
10.2.3 Identificación y autenticación para cada rol	33
10.2.4 Roles que requieren separación de tareas	33
10.3. CONTROLES DEL PERSONAL	33
10.3.1 Calificaciones, experiencia y requisitos de autorización	33
10.3.2 Procedimientos de comprobación de antecedentes	33
10.3.3 Requerimientos de formación	33
10.3.4 Requerimientos y frecuencia de la actualización de la formación	34
10.3.5 Frecuencia y secuencia de rotación de tareas	34
10.3.6 Sanciones por acciones no autorizadas	34
10.3.7 Requerimientos de contratación de personal	34

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

10.3.8 Documentación proporcionada al personal	34
10.4. PROCEDIMIENTO DE REGISTRO DE EVENTOS	34
10.4.1 Tipos de eventos registrados	34
10.4.2 Frecuencia de tratamiento de registros de auditoría	35
10.4.3 Periodos de retención para los registros de auditoría	35
10.4.4 Protección de los registros de auditoría	35
10.4.5 Procedimiento de copia de respaldo de los registros de auditoría	35
10.4.6 Sistema de recogida de información de auditoría	36
10.4.7 Notificación al sujeto causa del evento	36
10.4.8 Análisis de vulnerabilidades	36
10.5. ARCHIVO DE REGISTROS	36
10.5.1 Tipos de eventos archivados	36
10.5.2 Periodos de conservación de registros	38
10.5.3 Protección del archivo	38
10.5.4 Procedimiento de copia de respaldo del archivo	38
10.5.5 Requerimientos para el sellado de tiempo de los registros	38
10.5.6 Sistema de recogida de información de auditoría	38
10.5.7 Procedimiento para obtener y verificar información archivada	38
10.6. CAMBIO DE CLAVES	38
10.7. RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE	39
10.7.1 Procedimiento de Gestión de Incidencias y compromisos	39
10.7.2 Corrupción de recursos, aplicaciones o datos	39
10.7.3 Compromiso de la clave privada de la EC	39
10.7.4 Continuidad del negocio después de un desastre	39
10.8. TERMINACIÓN DE UNA EC O UNA ER	40
10.8.1 Entidad de Certificación	40
10.8.2 Entidad de Registro	40
10.9. CUSTODIA Y RECUPERACIÓN DE CLAVES	41
11. CONTROLES DE SEGURIDAD TÉCNICA	41
11.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	41
11.1.1 Generación del par de claves de la CA Raíz y CA Subordinada	41
11.1.1.1 Generación del par de claves del firmante	41
11.1.2 Envío de clave privada al firmante	41
11.1.3 Envío de clave pública al emisor del certificado	42
11.1.4 Distribución de la clave pública del prestador de servicios de certificación	42
11.1.5 Tamaño de claves	42
11.1.6 Generación de parámetros de clave pública	42
11.1.7 Comprobación de calidad de parámetros de clave pública	42

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

11.1.8 Usos admitidos de la clave (campo key usage de X.509 v3)	42
11.2. PROTECCIÓN DE LA CLAVE PRIVADA	43
11.2.1 Estándares de módulos criptográficos	43
11.2.2 Control por más de una persona (n de m) sobre la clave privada	43
11.2.3 Depósito de la clave privada	43
11.2.4 Copia de respaldo de la clave privada	43
11.2.5 Archivo de la clave privada	44
11.2.6 Introducción de la clave privada en el módulo criptográfico.	44
11.2.7 Método de activación de la clave privada	44
11.2.8 Método de desactivación de la clave privada	44
11.2.9 Método de destrucción de la clave privada	45
11.2.10 Clasificación de módulos criptográficos	45
11.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES	45
11.3.1 Archivo de la clave pública	45
11.3.2 Periodo de uso para las claves públicas y privadas	45
11.4. DATOS DE ACTIVACIÓN	45
11.4.1 Generación e instalación de los datos de activación	45
11.4.2 Protección de los datos de activación	46
11.5. CONTROLES DE SEGURIDAD INFORMÁTICA	46
11.5.1 Requerimientos técnicos de seguridad específicos	46
11.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	47
11.6.1 Controles de desarrollo de sistemas	47
11.6.2 Controles de gestión de seguridad	47
11.6.2.1 Gestión de seguridad	47
11.6.2.2 Clasificación y gestión de información y bienes	47
11.6.2.3 Operaciones de Gestión	47
11.6.2.4 Tratamiento de los soportes de seguridad	47
11.6.2.5 Planificación del sistema	47
11.6.2.6 Reporte de incidencias y respuestas	48
11.6.2.7 Procedimientos operaciones y responsabilidades	48
11.6.2.8 Gestión del sistema de acceso	48
11.6.3 Gestión del ciclo de vida del hardware criptográfico	49
11.7. CONTROLES DE SEGURIDAD DE RED	49
11.8. FUENTES DE TIEMPO	50
12. PERFILES DE CERTIFICADO, CRL Y OCSP	50
12.1. PERFIL DE LOS CERTIFICADOS	50
12.1.1 Número de versión	51
12.1.2 Extensiones de los certificados	51
12.1.3 Identificadores de objeto OID de los algoritmos utilizados	51
12.1.4 Formatos de nombres	52

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

12.1.5 Restricciones de los nombres	52
12.1.6 Identificador de objeto OID de la política de certificación	52
12.2. PERFIL DE CRL	53
12.2.1 Número de versión	53
12.2.2 CRL y extensiones	53
12.3. PERFIL DE OCSP	53
13. AUDITORÍAS DE CONFORMIDAD	53
13.1. FRECUENCIA DE LAS AUDITORÍAS	53
13.2. CALIFICACIÓN DEL AUDITOR	53
13.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA	53
13.4. ASPECTOS CUBIERTOS POR LOS CONTROLES	53
13.5. ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE INCIDENCIAS	54
13.6. COMUNICACIÓN DE RESULTADOS	54
14. ASPECTOS LEGALES Y OTROS ASUNTOS	54
14.1. TARIFAS	54
14.1.1 Tarifa de emisión de certificados	54
14.1.2 Tarifa de acceso a los certificados	54
14.1.3 Tarifa de acceso a la información relativa al estado de los certificados o los certificados revocados	54
14.1.4 Tarifa de otros servicios	54
14.1.5 Política de reintegros	55
14.2. RESPONSABILIDADES ECONÓMICAS	55
14.3. CONFIDENCIALIDAD DE LA INFORMACIÓN	55
14.3.1 Ámbito de la información confidencial	55
14.3.2 Información no confidencial	55
14.3.3 Responsabilidad en la protección de la información confidencial	55
14.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL	56
14.4.1 Plan de Privacidad	56
14.4.2 Información tratada como privada	56
14.4.3 Información no calificada como privada	56
14.4.4 Responsabilidad de la protección de los datos de carácter personal	56
14.4.5 Comunicación y consentimiento para usar datos de carácter personal	56
14.4.6 Revelación en el marco de un proceso judicial	56
14.4.7 Otras circunstancias de publicación de información	56
14.5. DERECHOS DE PROPIEDAD INTELECTUAL	57
14.6. OBLIGACIONES Y RESPONSABILIDADES	57
14.6.1 Obligaciones de la Entidad de Certificación	57
14.6.2 Obligaciones de la Entidad de Registro	57
14.6.3 Obligaciones del Solicitante	58

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

14.6.4 Obligaciones del Suscriptor	58
14.6.5 Obligaciones del Tercero que confía	58
14.6.6 Obligaciones de la entidad	59
14.7. RESOLUCIÓN DE DISPUTAS	59
14.8. INDEMNIZACIONES	59
14.9. PERIODO DE VALIDEZ	60
14.10. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES	60
14.11. CAMBIOS EN DPC Y PC	60
14.12. CUMPLIMIENTO DE LA NORMATIVA APLICABLE	60
15. BIBLIOGRAFÍA	61

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

## 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).

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

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

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

## 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:

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

- **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:

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

- 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.

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

## 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

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

#### 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](http://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](http://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](http://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](http://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](http://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](http://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](http://www.girasol.pe)

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

#### **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](http://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](http://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.

	<b>POLÍTICA DE CERTIFICACIÓN</b>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

## 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)

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

Campo del certificado		Descripción	Valor
version		Nº de versión	v3
serialNumber		Nº 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

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

		key CertSign, cRLSign Para los usuarios finales digital Signature, nonRepudiation
<b>Certificate Policies</b>	-	OID anyPolicy (2.5.29.32.0) URI de la DPC <a href="https://girasol.pe/">https://girasol.pe/</a> <sup>2</sup>
<b>Basic Constraints</b>	Sí	cA: TRUE pathLenConstraint: 0
<b>CRL Distribution Points</b>	-	URI de la CRL: <a href="https://girasol.pe/">https://girasol.pe/</a> <sup>2</sup>
<b>Authority Information Access</b>	-	URI del certificado de la CA Raíz: <a href="https://girasol.pe/">https://girasol.pe/</a> <sup>2</sup>
<b>Extended Key Usage</b>	-	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
<b>Country Name (C)</b>	País	PE <sup>1</sup>
<b>State or Province Name (ST)</b>	Estado/Provincia	<i>Departamento donde reside el suscriptor</i>
<b>Locality Name (L)</b>	Localidad	<i>Distrito donde reside el suscriptor</i>

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

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

#### 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.

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

## 7.2. PERSONA DE CONTACTO

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

## 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](http://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](mailto:soporte@girasolpe.com)

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

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

<b>Entidad de Certificación – EC:</b>	Entidad que brinda la emisión, revocación, renovación, modificación y suspensión de servicios de certificados digitales en el marco de la normativa establecida por IOFE.
<b>Entidad de Registro – ER:</b>	Entidades que realizan el proceso de verificación de identidad de solicitantes de servicios de certificación digital.
<b>Política de Certificación - PC:</b>	Un conjunto de reglas que indican el marco de aplicabilidad del servicio para la comunidad de usuarios definida.
<b>Certificado:</b>	Archivo que asocia la clave pública con datos del suscriptor y es firmado por la EC.
<b>Clave Pública:</b>	Valor matemático conocido públicamente y usado para la verificación de una firma digital.
<b>Clave Privada:</b>	Valor matemático usado únicamente por el suscriptor para la creación de una firma digital.
<b>Lista de Certificados Revocados - CRL:</b>	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.
<b>Declaración de Prácticas de Certificación - DPC:</b>	Conjunto de prácticas adoptadas por una Entidad de Certificación para la emisión, gestión, revocación y reemisión de certificados digitales.
<b>FIPS</b>	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

	<p>POLÍTICA DE CERTIFICACIÓN</p>	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

	<p>todas las agencias del gobierno no militares y por los contratistas del gobierno.</p>
<b>Firma Digital:</b>	<p>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:</p> <ul style="list-style-type: none"> <li>a) que los datos no han sido modificados (integridad);</li> <li>b) que la persona que firma los datos es quien dice ser (identificación); y</li> <li>c) que la persona que firma los datos no puede negar haberlo hecho.</li> </ul>
<b>HASH</b>	<p>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.</p>
<b>HSM:</b>	<p>Dispositivo Hardware que genera y protege claves criptográficas, y permite utilizarlas para realizar operaciones criptográficas de modo seguro.</p>
<b>OID:</b>	<p>Identificador numérico único registrado bajo la estandarización ISO y que se refiere a un objeto o clase de objeto determinado.</p>
<b>PKI</b>	<p>Conjunto de hardware, software, recursos humanos, procedimientos, etc, que componen un sistema usado para la creación y gestión de certificados de clave pública.</p>
<b>Suscriptor</b>	<p>Persona natural o jurídica a cuyo nombre se expide un certificado digital.</p>
<b>Titular:</b>	<p>Una entidad que requiere los servicios provistos por la EC y acepta los términos y condiciones del servicio descrito en este documento.</p>
<b>Tercero que confía:</b>	<p>Una persona que recibe documentos, registros o notificaciones firmados digitalmente y cree en la validez de las transacciones realizadas.</p>

	POLÍTICA DE CERTIFICACIÓN	Público
		Fecha de Emisión: 20/10/2024
		Versión: 1.0

## 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](http://WWW.GIRASOL.PE)