ENTIDAD DE CERTIFICACIÓN

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN V1.0

Nombre del documento	Declaración de Prácticas de Certificación
Realizado por	GIRASOL PE SCRL
Aprobado por	Responsable de la EC
Código del documento	EC-DPC-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 utilizadas 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	Declaración de Prácticas 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	20/10/2024
Clasificación de seguridad	Público
OID	**1.3.6.1.4.1.61580.0.0: DPC**
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. 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

4. USOS DEL CERTIFICADO

4.1. 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.

4.2. 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.

5. ADMINISTRACIÓN DE LA DPC

5.1. 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.

5.2. 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

5.3. FRECUENCIA DE REVISIÓN

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

5.4. PROCEDIMIENTO DE APROBACIÓN

Esta DPC 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.

5.5. 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.

6. 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.

7. PUBLICACIÓN Y RESPONSABILIDAD DEL REPOSITORIO

7.1. REPOSITORIOS

Los repositorios de GIRASOL.PE para la publicación de la información de certificación están disponibles las 24 horas del día, los 7 días de la semana.

En caso de fallo de sistema o cualquier factor que no esté bajo el control de GIRASOL.PE, GIRASOL.PE realizará los esfuerzos necesarios para asegurar que estos repositorios no se encuentren inaccesibles durante más de 24 horas.

Descripción	Link

Declaración de Prácticas de Certificación	www.girasol.pe
Política de Certificación	www.girasol.pe
Certificado CA Raíz FirmEasy RootCA	www.girasol.pe
Certificado CA Subordinada FirmEasy SubCA	www.girasol.pe
ARL: Lista de certificados de CA Revocados (CRL emitida por la CA Raíz FirmEasy Root CA)	www.girasol.pe
CRL: Lista de certificados de Entidad Final Revocados (CRL emitida por la CA FirmEasy SubCA)	www.girasol.pe
Servicio de Validación de certificados de CA - OSCP	www.girasol.pe

7.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

7.2.1. Políticas y Prácticas de Certificación

La versión actual de la DPC, así como todos los documentos normativos estarán disponibles en formato PDF en la web de GIRASOL.PE.

7.2.2 Términos y Condiciones

El responsable, y el Suscriptor y/o Titular, reciben información sobre los Términos y Condiciones que deben aceptar antes de la emisión del certificado.

7.2.3 Difusión de los certificados

GIRASOL.PE pone a disposición del público los certificados de la CA Raíz Y CA Subordinada propiedad de GIRASOL.PE bajo esta DPC.

De igual manera pone a disposición del público la CRL y OCSP propiedad de GIRASOL.PE bajo esta DPC.

7.3. FRECUENCIA DE PUBLICACIÓN

La información de la Entidad de Certificación, incluyendo la Declaración de Prácticas de Certificación, así como sus documentos normativos, se publican en cuanto se encuentren disponibles.

Los cambios generados en cada nueva versión de está DPC serán previamente informados al INDECOPI y publicados en la página web de

GIRASOL.PE. La auditoría anual de seguimiento por parte del INDECOPI validará estos cambios y emitirá la resolución de cumplimiento.

Los certificados Raíz y Subordinada se publicarán y permanecerán en la página web de GIRASOL.PE, durante todo el tiempo en que se estén prestando servicios de certificación digital.

GIRASOL.PE, publicará en su página web, la lista de certificados revocados (CRL).

7.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página web de GIRASOL.PE antes mencionados en el apartado 7.1, es de libre acceso al público en general.

8. IDENTIFICACIÓN Y AUTENTICACIÓN

8.1. REGISTRO DE NOMBRES

La información de la Entidad de Certificación, incluyendo la Declaración de Prácticas de Certificación, así como sus documentos normativos, se publican en cuanto se encuentren disponibles.

8.1.1. Tipos de nombres

La versión actual de la DPC, así como todos los documentos normativos estarán disponibles en formato PDF en la web de GIRASOL.PE.

8.1.2 Necesidad de que los nombres sean significativos

El responsable, y el Suscriptor y/o Titular, reciben información sobre los Términos y Condiciones que deben aceptar antes de la emisión del certificado.

8.1.3 Uso de seudónimos

GIRASOL.PE no emite certificados con uso de seudónimos

8.1.4 Reglas para la interpretación de varias formas de nombre

GIRASOL.PE atiende en todo caso a lo marcado por el estándar x.500 de referencia en la RFC 5280.

8.1.5 Singularidad de los nombres

El nombre distinguido (DN) de los certificados emitidos será único para cada Suscriptor y/o Firmante. Los atributos del DN que contienen el código identificativo del Suscriptor y/o el código identificativo del Firmante se usan

para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

8.1.6 Reconocimiento, autenticación y papel de las marcas reconocidas

La CA no asume compromisos en la emisión de certificados respecto al uso por los Suscriptores de una marca comercial. GIRASOL.PE no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Suscriptor. Sin embargo, la CA no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

8.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

8.2.1. Método de prueba de posesión de la clave privada

- **Generación de claves por parte de la EC:**

Software: Las claves se entregan al responsable a través de ficheros protegidos utilizando el estándar PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso al fichero PKCS#12 que posibilita la instalación de éste en las aplicaciones, es entregado por un medio distinto al utilizado en la recepción del fichero.

-

Hardware: La generación de claves de la AC se realiza en un módulo criptográfico que cumple con el estándar FIPS 140-2 nivel 3, el cual es realizado por personal de confianza de GIRASOL.PE.

- **Generación de claves por parte del suscriptor:**

El suscriptor dispone de un mecanismo de generación de claves en software. La prueba de posesión de la clave privada en estos casos es la petición recibida por la EC en formato PKCS#10.

Las claves privadas serán provistas directamente al suscriptor sin generar copias de las mismas,

8.2.2 Autenticación de la identidad de una organización

Los solicitantes deberán acreditar la existencia y vigencia de personas jurídicas mediante documentos públicos o normativa legal correspondiente, y mediante los correspondientes documentos de vigencia emitidos por los

organismos públicos de registro, o mediante normativa legal que especifique la constitución de las personas jurídicas correspondientes.

La información proporcionada por el solicitante será verificada consultando a la Superintendencia Nacional de los Registros Públicos del Estado.

Para una empresa registrada en el extranjero, su existencia y validez será verificada por el certificado de validez de la empresa u otros documentos equivalentes emitidos por la autoridad competente de su país de origen.

8.2.3 Autenticación de la identidad de una persona natural

La información proporcionada por el ciudadano peruano solicitante será verificada por el ER de GIRASOL.PE a través del mecanismo de consulta de la base de datos RENIEC.

Para las personas naturales con nacionalidad extranjera, se reconocerá su existencia y período de vigencia a través de su pasaporte o tarjeta de inmigración

8.2.4 Validación de correo electrónico

Las direcciones de correo electrónico incluidas en los certificados son validadas siempre por el Solicitante mediante su inclusión en las respectivas solicitudes del certificado firmadas por el Solicitante.

8.2.5 Validación de la Autoridad

La validación de la Entidad de Certificación GIRASOL.PE respecto a la propiedad de un dominio, se realiza a través de la comprobación de la existencia de un correo que contiene la dirección del dominio en cuestión y/o verificación de datos de registro de dominio respectivo.

8.2.6 Criterios para la interoperación

La Entidad de Certificación de GIRASOL.PE, únicamente emitirá certificados a ER Subordinadas, que estén directamente vinculadas o terceros con vínculo contractual los cuales se someten al cumplimiento de la presente DPC.

8.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN

La renovación 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). Un certificado no puede ser renovado después de su fecha de caducidad, y en su lugar se debe realizar una nueva emisión del certificado.

8.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

La identificación y autenticación de una solicitud de revocación se realiza, para cada uno de los procedimientos disponibles para los distintos tipos de certificados

GIRASOL.PE o cualquiera de sus ER afiliadas, puede, por iniciativa propia, solicitar la revocación de un certificado si:

- Tiene conocimiento o sospecha de que la clave privada del suscriptor ha sido comprometida.
- Tiene conocimiento o sospecha de cualquier otro evento que aconseje tomar dicha medida.

.

9. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

GIRASOL.PE emplea sus plataformas para la gestión del ciclo de vida de los certificados de entidad final bajo esta DPC.

Estas plataformas permiten realizar las acciones concernientes a la solicitud, la emisión, la aceptación, la reemisión y la revocación de los certificados de entidad final.

Los usuarios y solicitantes de los certificados digitales provistos por GIRASOL.PE son responsables de revisar la presente DPC así como los documentos normativos de GIRASOL.PE, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

9.1. SOLICITUD DEL CERTIFICADO

9.1.1 Quién puede solicitar un certificado

El certificado podrá ser solicitado por el Solicitante, con participación, en su caso, del Responsable, y/o del Suscriptor, y/o del Titular o la Entidad.

9.1.2 Proceso de solicitud de certificados

El Solicitante, deberá ponerse en contacto con la Entidad de Registro de GIRASOL.PE para gestionar la solicitud 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

9.2. 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

9.3. 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

9.4. 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

9.5. 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

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

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

9.7. 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.

9.8. 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.

9.9. 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.

9.9.1 Circunstancia para la revocación

Un certificado será revocado debido a:

- Uso indebido de la clave privada.
- Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- 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.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Decisión de la legislación respectiva.
- Falta de pago del certificado.
- La incapacidad sobrevenida o la muerte del Firmante o responsable del certificado.
- Resolución de la autoridad administrativa o judicial competente.

9.9.2 Quién puede solicitar una revocación

La revocación de un certificado puede ser solicitada por:

- El Responsable.
- El Titular.
- El Suscriptor.

- La Entidad.
- Un tercero autorizado.
- La ER a través del cual se emitió el certificado.
- La EC (GIRASOL.PE).
- Cualquier persona interesada puede notificar a la ER ó a la EC hechos que pueden indicar la necesidad de revocación de un certificado.

9.9.3 Procedimiento de solicitud de revocación

La solicitud de revocación puede realizarse por los titulares y suscriptores mediante las siguientes alternativas.

- Comunicación directa con GIRASOL.PE, mediante un código de revocación proporcionado durante el proceso de emisión del certificado.
- Una vez correctamente identificado el solicitante de la revocación y comprobada la causa comunicada, el operador procederá a tramitar la solicitud de revocación.

9.9.4 Periodo de gracia de la solicitud de revocación

La revocación del certificado es inmediata cuando el cliente lo solicita a través de los canales que GIRASOL.PE le brinda. El certificado revocado se mostrará como tal al validarlo en el servicio OCSP y, por otro lado, en la CRL con un plazo máximo de 24 horas. Se envía un correo al cliente como constancia de que el certificado ha sido revocado.

9.9.5 Plazo en la que la EC debe procesar la solicitud de revocación

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

9.9.6 Requisitos de verificación de las revocaciones por los terceros que confían

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la CRL o del servicio OCSP.

9.9.7 Frecuencia de emisión de CRL

- La CRL de los certificados de CA (ARL) se emite antes de que hayan transcurrido 180 días desde la emisión de la anterior CRL (antes de su fin de validez), o lo antes posible después de que se produzca una revocación (proceso manual).
- La CRL de los certificados de entidad final se emite cada 24 horas, o a más tardar 30 minutos después de que se produzca una revocación, con una validez de 7 días (proceso automático).

9.9.8 Máxima latencia para la CRL

- Una vez emitida la CRL de los certificados de CA (ARL), ésta se publica lo antes posible (proceso manual).
- Una vez emitida la CRL de los certificados de entidad final, ésta se publica a más tardar 1 hora después (proceso automático).

9.9.9 Disponibilidad de comprobación en línea de la revocación

GIRASOL.PE proporciona un servicio OCSP para la comprobación en línea de la revocación de los certificados emitidos, hasta la terminación de la EC por un motivo distinto al compromiso de su clave privada o hasta el cese de actividad como EC.

9.9.10 Requisitos de comprobación de la revocación On-Line

Para el uso del sistema de comprobación de revocación en línea por CRL, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar el estado de revocación del certificado de entidad final en la última CRL emitida y publicada por la EC Subordinada de GIRASOL.PE, que podrá descargarse en la dirección URL contenida en el propio certificado, en su extensión CRL Distribution Points.

Para el uso del sistema de comprobación de revocación en línea por OCSP, se debe considerar lo siguiente:

- Se deberá comprobar el estado de revocación del certificado de entidad final en el servicio OCSP de la CA Subordinada de Firma, cuya dirección URL de acceso está contenida en el propio certificado, en su extensión Authority Information Access.

9.9.11 Otras formas disponibles de divulgación de información de revocación

Cuando se produce la revocación de un certificado de usuario final, se envía un comunicado mediante correo electrónico al suscriptor especificando la fecha y hora y el motivo de la revocación.

9.9.12 Requisitos especiales en relación con el compromiso de claves privadas

Cualquier parte que detecte el compromiso de claves privadas asociadas a certificados activos emitidos bajo esta DPC, o que sospeche de dicho compromiso, puede notificarlo a GIRASOL.PE enviando un correo electrónico a la dirección soporte@girasolpe.com con el asunto "Notificación de compromiso de claves", identificando los certificados asociados a las claves privadas comprometidas.

9.9.13 Circunstancias para la suspensión

GIRASOL.PE no brinda el servicio de suspensión de certificados de usuario final.

9.9.14 Quién puede solicitar la suspensión

GIRASOL.PE no brinda el servicio de suspensión de certificados de usuario final.

9.9.15 Procedimiento de solicitud de suspensión

GIRASOL.PE no brinda el servicio de suspensión de certificados de usuario final.

9.9.16 Límites de periodo de suspensión

GIRASOL.PE no brinda el servicio de suspensión de certificados de usuario final.

9.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

9.10.1 Características operacionales

La información sobre el estado de los certificados emitidos está disponible a través de CRL y servicios OCSP, sin restricciones de acceso y es de acceso gratuito.

9.10.2 Disponibilidad del servicio.

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana y un tiempo programado de inactividad máxima de 0.5 % anual.

9.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

La suscripción del certificado finalizará en el momento de expiración o revocación del certificado.

9.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

GIRASOL.PE no custodia las claves privadas, ni copias de respaldo de las claves privadas, ni ofrece servicios de recuperación de las claves privadas.

10. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONES

GIRASOL.PE tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentren los sistemas y

los equipamientos empleados para las operaciones de emisión y gestión de certificados.

10.1. CONTROLES FÍSICOS

La política de seguridad física y ambiental aplicable a los servicios de generación y revocación de certificados ofrece protección frente:
Accesos físico no autorizados

- Desastres naturales
- Incendios
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura
- Inundaciones
- Robo
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año.

10.1.1 Ubicación y construcción

Las instalaciones contratadas por GIRASOL.PE están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, y ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una jaula de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

10.1.2 Acceso físico

El acceso físico a las instalaciones contratadas de GIRASOL.PE donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar.

10.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones contratadas de GIRASOL.PE disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

10.1.4 Exposición al agua

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

10.1.5 Protección y prevención de incendios

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

10.1.6 Sistema de almacenamiento

Cada medio de almacenamiento se mantiene solo al alcance de personal autorizado.

10.1.7 Eliminación de residuos

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga:

10.1.8 Copia de respaldo externa

GIRASOL.PE realiza una copia de seguridad de las claves de la EC donde se requieren al menos dos personas autorizadas expresamente para el acceso.

10.2. CONTROLES PROCEDIMENTALES

10.2.1 Roles de confianza

Los roles de confianza garantizan una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación.

- Oficial de Seguridad y Privacidad (Security Officer): Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Operador de Registro (Registration Officer): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final, así como las oportunas verificaciones en certificados de autenticación web.
- Administradores del sistema de certificación (System Administrators): Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- Titular de las claves de EC: Responsables de activar las claves de la EC en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.
- Responsable de la EC: Responsable de dirigir las operaciones de la EC conforme a la normatividad vigente.

10.2.2 Número de personas requeridas por tarea

La CA garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

- La generación de la clave de las CA's.
- La recuperación y back-up de la clave privada de las CA's.
- La emisión de certificados de las CA's.
- Activación de la clave privada de las CA's.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la root CA.

10.2.3 Identificación y autenticación para cada rol

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

10.2.4 Roles que requieren separación de tareas

El oficial de seguridad es incompatible con cualquier otro rol.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría.

10.3. CONTROLES DEL PERSONAL

10.3.1 Calificaciones, experiencia y requisitos de autorización

Todo el personal está calificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza se encuentra libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

GIRASOL.PE asegura que el personal de registro es personal confiable para realizar las tareas de registro.

10.3.2 Procedimientos de comprobación de antecedentes

GIRASOL.PE se encarga de realizar las investigaciones pertinentes antes de la contratación de cualquier persona.

GIRASOL.PE realiza una inspección de los antecedentes policiales, penales y crediticios de los roles de confianza.

10.3.3 Requerimientos de formación

GIRASOL.PE forma al personal de confianza que incluye los siguientes contenidos:

- Versiones de hardware y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

10.3.4 Requerimientos y frecuencia de la actualización de la formación

GIRASOL.PE realiza los cursos necesarios a sus empleados y a los operadores de registro para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

10.3.5 Frecuencia y secuencia de rotación de tareas

Sin estipulación adicional.

10.3.6 Sanciones por acciones no autorizadas

Cuando un empleado realice acciones no autorizadas, GIRASOL.PE tiene la potestad de sancionar o incluso ser retirado de la empresa. La decisión será tomada por el Responsable de la EC de GIRASOL.PE.

10.3.7 Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables deberán firmar con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por la CA.

Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

10.3.8 Documentación proporcionada al personal

GIRASOL.PE pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

10.4. PROCEDIMIENTO DE REGISTRO DE EVENTOS

10.4.1 Tipos de eventos registrados

GIRASOL.PE registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la CA.

Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la CA a través de la red.
- Intentos de accesos no autorizados a la red interna de la CA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la Autoridad de Certificación.
- Encendido y apagado de la aplicación de la CA.
- Cambios en los detalles de la CA y/o sus claves.

- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico de la CA.

10.4.2 Frecuencia de tratamiento de registros de auditoría

Se revisarán los logs de auditoría cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

10.4.3 Periodos de retención para los registros de auditoría

Se almacenará la información de los logs de auditoría durante 10 años. GIRASOL.PE almacena la información de acuerdo a lo estipulado en las Guías de Acreditación del INDECOPI.

10.4.4 Protección de los registros de auditoría

Los logs de los sistemas están protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Solo el Administrador del Sistema de la EC tiene la posibilidad de acceder a los mismos.

10.4.5 Procedimiento de copia de respaldo de los registros de auditoría

Diariamente se genera un respaldo de todos los servicios y sistemas de la EC de GIRASOL.PE.

10.4.6 Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

10.4.7 Notificación al sujeto causa del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

10.4.8 Análisis de vulnerabilidades

GIRASOL.PE revisa de manera anual los procesos de gestión de riesgos y vulnerabilidades dentro del marco de acreditación del INDECOPI.

GIRASOL.PE corregirá cualquier incidencia reportada.

10.5. ARCHIVO DE REGISTROS

10.5.1 Tipos de eventos archivados

GIRASOL.PE, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado.

- Todos los datos de la auditoría.
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores y los datos relativos a su identificación.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos o publicados.
- CRL's emitidas o registros del estado de los certificados generados.
- La documentación requerida por los auditores.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y prácticas de certificación.
- Tipo de documento presentado en la solicitud del certificado.
- Claves públicas de la EC.

GIRASOL.PE es responsable del correcto archivo de todo este material y documentación.

- Generación de claves de la EC.
- Instalación Manual de Claves Criptográficas de EC y su resultado (con la identidad del operador).
- Respaldo de claves de EC.
- Almacenamiento de claves de EC.
- Recuperación de claves de EC.
- Actividades de repositorio de claves de EC.
- Uso de claves de la EC.

En cuanto al ciclo de vida de los dispositivos criptográficos, la EC debe registrar lo siguiente:

- Dispositivo del equipo e instalación.
- Colocar dentro o remover un dispositivo de almacenamiento.
- Activación y uso del dispositivo.
- Desinstalación del dispositivo.
- Designación de un dispositivo para el servicio y su reparación.
- Retiro del dispositivo

En cuanto ciclo de vida de las claves del suscriptor, la EC debe registrar lo siguiente:

- Generación de las claves.
- Archivo de las claves (si fuera aplicable).
- Destrucción de las claves.
- Identidad de la entidad que autoriza las operaciones de gestión de las claves .
- Compromiso de las claves,

La EC debe registrar o requerir a la ER el registro de la siguiente información para la solicitud de certificados:

- El método de identificación aplicados y la información usada para el cumplimiento de los requerimientos del suscriptor
- Registro de la data, números o combinación, única identificación o documentos de identificación.
- Locación de almacenamiento de las copias de los documentos de identificación y las solicitudes Identidad de la entidad que acepta las solicitudes.
- Método usado para validar documentos de identificación.
- Nombre de la EC que recibe o de la ER que solicita.
- Aceptación del suscriptor del Acuerdo del Suscriptor.
- El consentimiento para permitir a la EC o ER guardar registros de datos personales, pasar esta información a terceras partes especificadas, y publicación de certificados.

La EC debe registrar los siguientes eventos sensibles con respectos a la seguridad:

- Lectura o escritura de registros o archivos sensibles de seguridad, incluyendo los registros de auditoría por sí mismos.
- Acciones tomadas contra los datos sensibles de seguridad.
- Cambios de perfiles de seguridad.
- Uso de mecanismos de identificación y autenticación, considerando ambos casos exitosos y no exitosos (incluyendo múltiples intentos fallidos de autenticación).
- Fallos de los sistemas, del hardware y otras anomalías.
- Acciones tomadas por individuos en Roles de Confianza, operadores computacionales, administradores de sistemas, oficiales de seguridad de sistemas.
- Acceso a los sistemas de la EC y cualquiera de sus componentes

10.5.2 Periodos de conservación de registros

Los certificados, los contratos con los suscriptores y cualquier información indicada en el apartado Tipos de eventos archivados, serán conservados durante al menos diez (10) años.

10.5.3 Protección del archivo

GIRASOL.PE protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo.

GIRASOL.PE asegura la correcta protección de los archivos mediante la asignación de personal calificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

10.5.4 Procedimiento de copia de respaldo del archivo

GIRASOL.PE realiza copias de respaldo anuales de todos sus documentos electrónicos y realiza copias de respaldo completas para casos de recuperación de datos.

10.5.5 Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable vía NTP.

10.5.6 Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

10.5.7 Procedimiento para obtener y verificar información archivada

Los eventos registrados están protegidos contra manipulaciones no autorizadas.

Solo personal autorizado tiene acceso a los archivos para obtener y llevar a cabo verificaciones de integridad de dichos archivos.

10.6. CAMBIO DE CLAVES

Con anterioridad a que el uso de la clave privada de la EC caduque, será realizado un cambio de claves. La antigua EC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha EC. Se generará una nueva EC con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

10.7. RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE

10.7.1 Procedimiento de Gestión de Incidencias y compromisos

GIRASOL.PE ha desarrollado un Plan de continuidad, el cual contempla el compromiso de la clave raíz de la EC como un caso particular. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos del sector privado y público.

10.7.2 Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de GIRASOL.PE

10.7.3 Compromiso de la clave privada de la EC

En caso de compromiso de la clave privada de la EC, GIRASOL.PE:

- Notificará al INDECOPI tras tener conocimiento del compromiso.
- Informará del compromiso de la clave privada de la EC a todos los Suscriptores y Titulares, así como a otros clientes o entidades con los cuales tenga acuerdos u otro tipo de relación, mediante la publicación de un aviso en la página web.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave privada no son válidos.
- Cesará la actividad de la EC sin transferir la gestión de los certificados emitidos a otro PSC, pero pudiendo sustituir el certificado de la EC Subordinada con cambio de claves.

10.7.4 Continuidad del negocio después de un desastre

GIRASOL.PE restablecerá los servicios críticos (revocación, y publicación de información de estado de certificados) de acuerdo con el plan de continuidad de negocio.

10.8. TERMINACIÓN DE UNA EC O UNA ER

10.8.1 Entidad de Certificación

Antes de la terminación de su actividad GIRASOL.PE realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios, mediante un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.

- Informará a los suscriptores, titulares y terceros que confían del término de sus actividades por lo menos treinta (30) días calendario de anticipación.
- Las claves privadas de la EC serán destruidas o deshabilitadas para su uso.
- GIRASOL.PE mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Comunicará al INDECOPI de la terminación de sus actividades como EC y el destino que vaya a dar a los certificados, especificando, en su caso, si va transferir la gestión.

10.8.2 Entidad de Registro

Antes de la terminación de sus actividades, la ER de GIRASOL.PE informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

- GIRASOL.PE dejará de emitir certificados a través de la ER.
- GIRASOL.PE revocará todos los certificados activos emitidos a través de esa ER, excepto que exista un acuerdo entre la EC y la ER para mantenerlos activos.
- La ER entregará a la EC la información y documentación que ha sido necesaria para la emisión y gestión de los certificados a través de la ER. La ER proporcionará a la EC toda la información existente acerca de las solicitudes de certificados en curso y todavía no validadas, para que la EC pueda validarlas una vez comprobado el cumplimiento de los requisitos aplicables.
- La ER garantizará que mantendrá, de forma indefinida, la confidencialidad a la que ha estado obligada en virtud del contrato con la EC.

10.9. CUSTODIA Y RECUPERACIÓN DE CLAVES

GIRASOL.PE no custodia las claves privadas, ni copias de respaldo de las claves privadas, ni ofrece servicios de recuperación de las claves privadas de sus usuarios finales.

11. CONTROLES DE SEGURIDAD TÉCNICA

11.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

11.1.1 Generación del par de claves de la CA Raíz y CA Subordinada

La generación de las claves de la CA Raíz y CA Subordinada de GIRASOL.PE se realiza, de acuerdo con el "Procedimiento de Generación de Claves", por personal autorizado según los roles de confianza con un control dual, dentro de un centro de procesamiento de datos, en un módulo de seguridad de hardware (HSM) con certificación FIPS 140 -2, en presencia de testigos y un notario certificado.

La clave raíz se genera y gestiona en un equipo fuera de línea dentro del centro de procesamiento de datos.

AC	Longitud de claves	Algoritmo de firma	Creación	Caducidad
FirmEasy Root CA	4096	SHA 256	16/10/2024	13/10/39
FirmEasy Sub CA	4096	SHA 256	16/10/2024	08/10/39

11.1.1.1 Generación del par de claves del firmante

Las claves del firmante son creadas por él mismo en formato software PKCS#12.

Las claves tienen una longitud mínima de 2048 bits (RSA).

11.1.2 Envío de clave privada al firmante

La clave privada del firmante se genera y se almacena en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que en este caso no existe envío de clave privada, garantizando el control exclusivo de la clave por parte del usuario

11.1.3 Envío de clave pública al emisor del certificado

El método de envío de la clave pública al prestador de servicios electrónicos de confianza es PKCS#10.

11.1.4 Distribución de la clave pública del prestador de servicios de certificación

Las claves públicas de GIRASOL.PE son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en la página web.

Los usuarios pueden acceder a la página web www.girasol.pe para obtener las claves públicas de la Autoridad de Certificación Raíz y Subordinada.

11.1.5 Tamaño de claves

- La longitud de las claves de la Autoridad de Certificación raíz es de 4096 bits.
- La longitud de las claves de las Autoridad de Certificación subordinadas es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de 2048 bits.

11.1.6 Generación de parámetros de clave pública

La clave pública de la Autoridades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

11.1.7 Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096 bits.
- Algoritmo de generación de claves: RSA.
- Funciones criptográficas de Resumen: SHA256.

11.1.8 Usos admitidos de la clave (campo key usage de X.509 v3)

Todos los certificados emitidos por GIRASOL.PE incluyen las extensiones Key Usage y Extended Key Usage, indicando los usos habilitados de las claves.

- Los usos admitidos para los certificados de la CA Raíz y la CA Subordinada de GIRASOL.PE son firma de certificados y firma de CRL.
- Los usos admitidos de la clave para cada tipo de certificado de Suscriptores son autenticación, firma y no repudio.

11.2. PROTECCIÓN DE LA CLAVE PRIVADA

11.2.1 Estándares de módulos criptográficos

Los módulos criptográficos empleados para generar y proteger las claves de la Autoridad de Certificación Raíz y Autoridad de Certificación Subordinada (HSM) de GIRASOL.PE están certificados con la norma FIPS-140-2 nivel 3.

11.2.2 Control por más de una persona (n de m) sobre la clave privada

El acceso a la clave privada de la CA Raíz de GIRASOL.PE requiere la participación simultánea de 2 de 3 de los roles de confianza, con uso de sus respectivos usuario y PIN.

El acceso a la clave privada de la CA Subordinada de GIRASOL.PE requiere la participación simultánea de 2 de 3 de los roles de confianza, con uso de sus respectivos usuario y PIN.

11.2.3 Depósito de la clave privada

La clave privada de la CA Raíz de GIRSOL.PE está custodiada en un dispositivo criptográficos hardware (HSM) certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado en el apartado 11.2.2, con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

La clave privada de la CA Subordinada de GIRASOL.PE está custodiada en un dispositivo criptográficos hardware (HSM) certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación de la clave privada requiere el control multipersona detallado en el apartado 11.2.2.

11.2.4 Copia de respaldo de la clave privada

Existen unos dispositivos que permiten la restauración de las claves privadas de la CA Raíz y la CA Subordinada de GIRASOL.PE, que son almacenados de forma segura y sólo son accesibles por personal autorizado, usando al menos un control dual en un medio físico seguro. Las claves privadas de la CA Raíz y la CA Subordinada de GIRASOL.PE se pueden restaurar por un proceso que requiere la utilización de 2 de 3 roles de confianza.

11.2.5 Archivo de la clave privada

GIRASOL.PE no archivará la clave privada de la CA Raíz Y CA Subordinada después de la expiración de todos los certificados autofirmados que contienen la correspondiente clave pública.

11.2.6 Introducción de la clave privada en el módulo criptográfico.

Las claves privadas de la CA Raíz y la CA Subordinada de GIRASOL.PE se crean en el interior de los HSM.

La introducción de la clave en el HSM se realizará al menos con la participación de 2 de 3 personas autorizadas.

Existe un documento de Generación de claves de la CA Raíz y CA Subordinada donde se describe el proceso de generación y almacenamiento de las claves privadas por los módulos criptográficos empleados.

11.2.7 Método de activación de la clave privada

La clave privada de la CA Raíz de GIRASOL.PE se activa en el HSM por un proceso que requiere la participación de 2 de 3 personas autorizadas, los cuales, junto a sus respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.

La clave privada de la CA Subordinada de GIRASOL.PE se activa en el HSM por un proceso que requiere la participación de 2 de 3 personas autorizadas, los cuales, junto a sus respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.

El acceso a la clave privada del firmante se realiza por medio de una clave de activación que conocerá solamente el suscriptor y que GIRASOL.PE recomienda no tener por escrito.

11.2.8 Método de desactivación de la clave privada

Para la desactivación de la clave privada de la CA Raíz y CA Subordinada se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

11.2.9 Método de destrucción de la clave privada

La destrucción de la clave privada de la CA Raíz o la CA Subordinada de GIRASOL.PE se realiza, de acuerdo con un procedimiento documentado de destrucción de claves, por personal autorizado según los roles de confianza,

y en presencia de testigos y un auditor interno o externo. Se realizará un borrado seguro de la clave privada de la CA, utilizando las funciones que proveen los dispositivos criptográficos hardware empleados (HSM). Asimismo, se realizará un borrado seguro de todas las copias de seguridad de la clave privada de la CA.

11.2.10 Clasificación de módulos criptográficos

Según lo especificado en el apartado 11.2.1.

11.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

11.3.1 Archivo de la clave pública

Los certificados emitidos por GIRASOL.PE, y por tanto las claves públicas se conservarán durante al menos 10 años desde su expiración.

11.3.2 Periodo de uso para las claves públicas y privadas

El periodo operativo de un certificado y el periodo de uso de su par de claves estarán determinados por el periodo de validez o por la revocación del certificado. En caso de que la seguridad del algoritmo utilizado para la creación del par de claves llegue a ser insuficiente antes del fin del periodo de validez del certificado, se comunicará a los suscriptores y terceras partes interesadas. La clave privada no debe ser usada después del periodo de validez o la revocación del certificado. La clave pública no debe ser usada después del periodo de validez o la revocación del certificado, excepto por los terceros que confían en los certificados para verificar datos históricos.

11.4. DATOS DE ACTIVACIÓN

11.4.1 Generación e instalación de los datos de activación

Los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada de GIRASOL.PE fueron generados de forma segura durante la ceremonia de claves.

11.4.2 Protección de los datos de activación

Sólo el personal autorizado tiene acceso a los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada de GIRASOL.PE. Para los certificados de los suscriptores, una vez se ha hecho entrega de los datos de activación de la clave privada, es responsabilidad del Firmante mantener la confidencialidad de estos datos.

11.5. CONTROLES DE SEGURIDAD INFORMÁTICA

GIRASOL.PE emplea sistemas fiables para ofrecer los servicios de certificación. Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal autorizado en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de usuarios y permisos.
- Configuración de eventos de log.
- Plan de backup y recuperación.
- Configuración de antivirus.
- Requerimientos de tráfico de red.

La documentación técnica y de configuración de GIRASOL.PE detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

11.5.1 Requerimientos técnicos de seguridad específicos

El servidor de GIRASOL.PE incluye las siguientes funcionalidades:

- Control de acceso a los servicios de EC y ER y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del Firmante, la EC y la ER y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Mecanismos de recuperación de claves y del sistema de EC y ER.

11.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

11.6.1 Controles de desarrollo de sistemas

Las plataformas de la EC y ER poseen un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

11.6.2 Controles de gestión de seguridad

11.6.2.1 Gestión de seguridad

GIRASOL.PE desarrolla las actividades precisas para la formación y concientización de los empleados en materia de seguridad.

GIRASOL.PE exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

11.6.2.2 Clasificación y gestión de información y bienes

GIRASOL.PE mantiene un inventario de activos y documentación, y un procedimiento para garantizar el correcto uso y gestión de este material. GIRASOL.PE dispone de procedimientos documentados de gestión de la información donde se clasifica según su nivel de confidencialidad.

GIRASOL.PE dispone de procedimientos documentados de gestión de altas y bajas de usuarios y política de acceso.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

11.6.2.3 Operaciones de Gestión

GIRASOL.PE dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

GIRASOL.PE dispone de cajas de seguridad para el almacenamiento de soportes físicos.

GIRASOL.PE tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

11.6.2.4 Tratamiento de los soportes de seguridad

Los soportes que contengan datos sensibles serán destruidos de manera segura si no van a volver a ser requeridos.

11.6.2.5 Planificación del sistema

GIRASOL.PE mantiene un registro de las capacidades de los equipos.

11.6.2.6 Reporte de incidencias y respuestas

GIRASOL.PE dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas.

11.6.2.7 Procedimientos operaciones y responsabilidades

GIRASOL.PE define actividades asignadas a personas con un rol de confianza distinto, para las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

11.6.2.8 Gestión del sistema de acceso

GIRASOL.PE realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

A. Gestión general de la EC y ER:

- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- Se dispone de procedimientos documentados de gestión de altas y bajas de usuarios y política de acceso.
- Se dispone de un procedimiento para asegurar que las operaciones se realizan respetando los roles establecidos.
- Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.
- El personal será responsable de sus actos, por ejemplo, por retener logs de eventos.

B. Generación del certificado:

- Las instalaciones están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular.
- La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n para la activación de la clave privada de la CA Raíz y CA Subordinada.

C. Gestión de revocación:

- Las instalaciones de las plataformas de la EC y la ER están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular al sistema de revocaciones.
- La revocación se refiere a la pérdida de efectividad de un certificado de forma permanente. La revocación se realizará mediante autenticación por certificado a las aplicaciones por un operador autorizado (Responsable de revocación). Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de la EC.

D. Estado de la revocación

- La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificado para evitar el intento de modificación de la información del estado de revocación.

11.6.3 Gestión del ciclo de vida del hardware criptográfico

GIRASOL.PE asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación

GIRASOL.PE registra toda la información pertinente de los dispositivos para añadir al catálogo de activos

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Los dispositivos criptográficos solo son manipulados por personal confiable. Las claves privadas de firma de las CA almacenadas en el hardware criptográfico se eliminarán una vez que se hayan retirado los dispositivos. La configuración del sistema de las CA así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de la Entidad de Certificación y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizan al menos por dos personas confiables.

11.7. CONTROLES DE SEGURIDAD DE RED

GIRASOL.PE protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL.

11.8. FUENTES DE TIEMPO

En el caso de la plataforma de la CA, el tiempo se obtiene mediante una sincronización y consulta a INACAL, siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en la RFC 5905 “Network Time Protocol”.

12. PERFILES DE CERTIFICADO, CRL Y OCSP

12.1. 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)

12.2. PERFIL DE CRL

El perfil de las CRL se corresponde con el perfil estándar de CRL X.509 de la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Las CRL son firmadas por la CA que ha emitido los certificados.

12.2.1 Número de versión

Las CRL emitidas por GIRASOL.PE siguen el estándar de CRL X.509 versión 2.

12.2.2 CRL y extensiones

Se soporta y se utilizan CRLs conformes al estándar X.509.

12.3. PERFIL DE OCSP

El Servicio de Validación de Certificados se basa en el uso del protocolo OCSP sobre HTTP, definido en la norma RFC 6960 “Online Certificate Status Protocol – OCSP”.

Los servicios de OCSP cumplen con la norma IETF RFC 6960.

13. AUDITORÍAS DE CONFORMIDAD

13.1. FRECUENCIA DE LAS AUDITORÍAS

GIRASOL.PE lleva a cabo auditorías internas y externas. La auditoría interna se llevará a cabo una vez al año. Así mismo, las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y/o cada vez que el INDECOPI lo requiera.

13.2. CALIFICACIÓN DEL AUDITOR

INDECOPI se encarga de enviar un listado de auditores siendo decisión de GIRASOL.PE la selección del auditor de dicha lista.

13.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Los auditores son independientes de GIRASOL.PE.

13.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

Las auditorías verifican los siguientes principios:

- Que la EC haga público sus documentos normativos.
- Que la EC mantenga la integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.
- Que la DPC, se ajusta a lo establecido con la normativa vigente.
- Que la EC gestione de forma adecuada la seguridad de sus sistemas de información.

13.5. ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE INCIDENCIAS

En caso de que sean detectadas incidencias o no-conformidades, se tomarán las medidas oportunas para su resolución en el menor tiempo posible.

13.6. COMUNICACIÓN DE RESULTADOS

La comunicación de resultados se realiza al Responsable de la Entidad de Certificación.

14. ASPECTOS LEGALES Y OTROS ASUNTOS

14.1. TARIFAS

14.1.1 Tarifa de emisión de certificados

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

14.1.2 Tarifa de acceso a los certificados

El acceso a los certificados raíz e intermedias es gratuito.

14.1.3 Tarifa de acceso a la información relativa al estado de los certificados o los certificados revocados

No se establece ninguna tarifa para la revocación de certificados.

GIRASOL.PE provee un acceso gratuito a la información relativa al estado de los certificados, por medio de la publicación de las correspondientes CRL y del servicio OCSP.

14.1.4 Tarifa de otros servicios

El acceso al contenido de la presente DPC será gratuito.

14.1.5 Política de reintegros

La EC dispondrá de una política de reintegros que se encuentra descrita en los contratos con los suscriptores.

14.2. RESPONSABILIDADES ECONÓMICAS

La EC dispondrá en todo momento de una póliza de seguro en los términos que marque la legislación vigente. La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los Suscriptores y de los terceros que confíen en los certificados.

14.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

14.3.1 Ámbito de la información confidencial

GIRASOL.PE considerará confidencial toda la información que esté catalogada expresamente como confidencial. No se difundirá información declarada como confidencial sin el consentimiento expreso por escrito de la persona, entidad u organización que le haya otorgado el carácter de confidencial, a no ser que ello sea requerido por una autoridad administrativa o judicial.

14.3.2 Información no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.
- La contenida en la Política de Certificación.
- La información contenida en los certificados, puesto que para su emisión el Suscriptor y, en su caso, el Firmante otorgan previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de certificados revocados (CRL), así como las restantes informaciones de estado de revocación.
- Cualquier otra información cuya publicidad sea impuesta normativamente.

14.3.3 Responsabilidad en la protección de la información confidencial

Es responsabilidad de GIRASOL.PE establecer medidas adecuadas para la protección de la información confidencial.

14.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

14.4.1 Plan de Privacidad

GIRASOL.PE cumple con la normativa vigente en materia de protección de datos personales, concretamente con lo dispuesto por la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas, en los ámbitos legales, regulatorios y contractuales.

14.4.2 Información tratada como privada

La información personal sobre un individuo que no está públicamente disponible en los contenidos de un certificado o CRL se considera privada.

14.4.3 Información no calificada como privada

La siguiente información no está calificada como privada:

- La información contenida en los certificados, puesto que para su emisión el Suscriptor otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de certificados revocados (CRL), así como las restantes informaciones de estado de revocación.

14.4.4 Responsabilidad de la protección de los datos de carácter personal

Es responsabilidad del responsable del tratamiento proteger adecuadamente la información privada.

14.4.5 Comunicación y consentimiento para usar datos de carácter personal

Antes de entablar una relación contractual, GIRASOL.PE ofrecerá a los interesados la información previa acerca del tratamiento de sus datos personales y ejercicio de derechos, y en su caso, recabará el consentimiento preceptivo para el tratamiento diferenciado del tratamiento principal para la prestación de los servicios contratados.

14.4.6 Revelación en el marco de un proceso judicial

Los datos de carácter personal podrán ser revelados por GIRASOL.PE sin el previo consentimiento del usuario cuando sea requerida para ello por una autoridad administrativa o judicial.

14.4.7 Otras circunstancias de publicación de información

No se ceden datos personales a terceros salvo obligación legal.

14.5. DERECHOS DE PROPIEDAD INTELECTUAL

GIRASOL.PE es titular de los derechos de propiedad intelectual sobre estas DPC.

GIRASOL.PE será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita si no se acuerda explícitamente lo contrario.

14.6. OBLIGACIONES Y RESPONSABILIDADES

14.6.1 Obligaciones de la Entidad de Certificación

GIRASOL.PE se encuentra obligada a cumplir con lo dispuesto por la normativa vigente y además a:

- Respetar lo dispuesto en esta DPC.
- Proteger sus claves privadas de forma segura.
- Emitir certificados conforme a esta DPC y a los estándares de aplicación.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados.
- Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- Revocar los certificados según lo dispuesto en esta DPC y publicar las mencionadas revocaciones en la CRL.
- Informar a los Suscriptores de la revocación de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
- Publicar esta DPC correspondiente en su página web.
- Informar sobre las modificaciones de la Política y Declaración Prácticas de Certificación de GIRASOL.PE, a los suscriptores.
- No almacenar ni copiar los datos de creación de firma del Suscriptor.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

14.6.2 Obligaciones de la Entidad de Registro

La ER de GIRASOL.PE se encuentra obligada a cumplir con lo dispuesto por la normativa vigente y además a:

- Respetar lo dispuesto en esta DPC.
- Comprobar la identidad de los solicitantes de certificados.

- Verificar la exactitud y autenticidad de la información suministrada por el Suscriptor solicitante.
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor.
- Respetar lo dispuesto en los contratos firmados con la EC de GIRASOL.PE y con el Suscriptor.
- Informar a la EC las causas de revocación, siempre y cuando tomen conocimiento.

14.6.3 Obligaciones del Solicitante

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

- Suministrar a la ER la información necesaria para realizar una correcta identificación.
- Confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

14.6.4 Obligaciones del Suscriptor

El Suscriptor (ya sea persona natural o jurídica a través de un representante suficiente) de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Custodiar su clave privada de manera diligente.
- Usar el certificado según lo establecido en la presente Política de Certificación.
- Respetar lo dispuesto en el contrato firmado con la EC de GIRASOL.PE.
- En el caso de los certificados con alguna vinculación empresarial, informar de la existencia de alguna causa de revocación como, por ejemplo, el cese o la modificación de su vinculación con la Entidad.
- En el caso de los certificados con alguna vinculación empresarial, notificar cualquier cambio en los datos aportados para la creación del certificado durante su período de validez, como el cese o la modificación de su vinculación con la Entidad.

14.6.5 Obligaciones del Tercero que confía

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

14.6.6 Obligaciones de la entidad

En el caso de aquellos certificados que impliquen vinculación a una Entidad, la Entidad estará obligada a cumplir con lo dispuesto por la normativa vigente aplicable y además a:

- Proporcionar a la ER información y/o documentación exigida del Titular y/o de la Entidad.
- Proporcionar a la ER información y/o documentación exigida del Solicitante y/o del Responsable, conforme a la normativa vigente de protección de datos personales.
- Garantizar la exactitud y veracidad de la información y/o la documentación proporcionada.
- Informar a la ER o la EC de cualquier cambio en los datos aportados para la emisión del certificado y que consten en él, durante el periodo de validez del certificado.
- Solicitar a la ER o la EC lo antes posible la revocación del certificado cuando tenga conocimiento de la existencia de cualquier causa de revocación, en especial cuando el Titular cese la vinculación con la Entidad.

14.7. 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 de la ENTIDAD soporte@girasol.pe para su revisión. De llegar a alguna disputa o incumplimiento entre las partes, los costos incluido el honorario de abogados será asumida por cada parte.

14.8. INDEMNIZACIONES

El seguro se hará cargo de todas las cantidades que GIRASOL.PE resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad.

14.9. PERIODO DE VALIDEZ

- La DPC y PC entran en vigor en el momento de su publicación en la web de GIRASOL.PE
- La presente DPC y PC serán derogadas en el momento en que una nueva versión del documento sea publicada en la web de GIRASOL.PE. La nueva versión sustituirá íntegramente el documento anterior.

14.10. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

De modo general, se utilizará el sitio web de GIRASOL.PE para realizar cualquier tipo de notificación y comunicación.

En caso de problemas de seguridad o de pérdida de integridad que puedan afectar a una persona física o jurídica, GIRASOL.PE notificará a ésta dicha incidencia.

14.11. CAMBIOS EN DPC Y PC

El contenido de esta DPC y de la PC puede ser cambiado unilateralmente por GIRASOL.PE.

Todos los cambios en esta DPC y en la PC requerirán nuevas versiones de los documentos. Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

Las nuevas versiones aprobadas de esta DPC y de la PC serán enviadas al INDECOPI y publicadas en la página web de GIRAASOL.PE Aquellos cambios que puedan afectar sustancialmente a los Suscriptores, y/o a los Firmantes serán notificados a los interesados.

14.12. 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.

15. 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