**ENTIDAD DE CERTIFICACIÓN**

# POLÍTICA DE SEGURIDAD DE LA EC V1.0

| | |
|---|---|
| **Nombre del documento** | Política de Seguridad de la EC |
| **Realizado por** | GIRASOL PE SCRL |
| **Aprobado por** | Responsable de la EC |
| **Código del documento** | EC-POL-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 la descripción de operaciones y prácticas de seguridad que utiliza GIRASOL.PE para garantizar la autenticidad e integridad del servicio 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.

## 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. 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);<br>b)que la persona que firma los datos es quien dice ser (identificación); y<br>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. |

## 4. ALCANCE

La presente política es de cumplimiento obligatorio para el personal y terceros subcontratados por GIRASOL.PE, quienes participen de las operaciones críticas de los servicios de Entidad de Certificación conforme a las responsabilidades especificadas en las siguientes secciones.

## 5. RESPONSABILIDADES DE GIRASOL.PE

Las responsabilidades contractuales, garantías financieras y coberturas de seguro son brindadas por GIRASOL.PE de acuerdo con su Declaración de Prácticas de Certificación.

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. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

GIRASOL.PE tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de certificación. Esto implica controles de acceso a las aplicaciones, verificación de estado de certificado, generación de registros de eventos, evaluación de vulnerabilidades de las aplicaciones y asimismo se somete ante el INDECOPI, en su calidad de Autoridad Administrativa Competente de la IOFE a auditorías anuales.

## 6.1. ORGANIZACIÓN

El Responsable de la EC y el Oficial de Seguridad de la Información son los encargados de velar por el cumplimiento de lo establecido en la presente política.

## 6.2. GESTIÓN DE RIESGOS

GIRASOL.PE administra los riesgos relacionados con la infraestructura física y de comunicaciones.

## 6.3. GESTIÓN DE ACTIVOS

GIRASOL.PE protege los activos críticos de la EC, de acuerdo a la clasificación y controles especificados por el Oficial de Seguridad de la Información de la EC.

# 7. 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.

## 7.1. 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.

### 7.1.1 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.

### 7.1.2 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.

### 7.1.3 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.

#### 7.1.4 Exposición al agua

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

#### 7.1.5 Protección y prevención de incendios

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

#### 7.1.6 Sistema de almacenamiento

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

#### 7.1.7 Eliminación de residuos

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

#### 7.1.8 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.

### 7.2. CONTROLES PROCEDIMENTALES

#### 7.2.1 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.

### 7.2.2 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.

### 7.2.3 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.

### 7.2.4 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.

## 7.3. CONTROLES DEL PERSONAL

### 7.3.1 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.

### 7.3.2 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.

### 7.3.3 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.

### 7.3.4 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.

### 7.3.5 Frecuencia y secuencia de rotación de tareas

Sin estipulación adicional.

### 7.3.6 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.

### 7.3.7 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.

### 7.3.8 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.

## 7.4. PROCEDIMIENTO DE REGISTRO DE EVENTOS

### 7.4.1 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.

### 7.4.2 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.

### 7.4.3 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.

### 7.4.4 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.

### 7.4.5 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.

### 7.4.6 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.

### 7.4.7 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.

### 7.4.8 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.

## 7.5. ARCHIVO DE REGISTROS

### 7.5.1 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

### 7.5.2 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.

### 7.5.3 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.

### 7.5.4 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.

### 7.5.5 Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable vía NTP.

### 7.5.6 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.

### 7.5.7 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.

## 7.6. RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE

### 7.6.1 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.

### 7.6.2 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

### 7.6.3 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.

### 7.6.4 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.

## 7.7. 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.

### 7.7.1 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.

## 7.8. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

### 7.8.1 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.

### 7.8.2 Controles de gestión de seguridad

#### 7.8.2.1 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.

#### 7.8.2.2 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.

#### 7.8.2.3 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.

#### 7.8.2.4 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.

#### 7.8.2.5 Planificación del sistema

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

#### 7.8.2.6 Reporte de incidencias y respuestas

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

#### 7.8.2.7 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.

#### 7.8.2.8 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.

### 7.8.3 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.

### 7.9. 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.

### 7.10. 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”.

## 8. AUDITORÍAS DE CONFORMIDAD

### 8.1. 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.

### 8.2. CALIFICACIÓN DEL AUDITOR

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

### 8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Los auditores son independientes de GIRASOL.PE.

### 8.4. 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.

### 8.5. 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.

### 8.6. COMUNICACIÓN DE RESULTADOS

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

## 9. RESPONSABILIDADES

El Oficial de Seguridad y Datos Personales de GIRASOL.PE gestiona la implementación y vela por el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

# 10. ORGANIZACIÓN QUE ADMINISTRA LA POLÍTICA DE SEGURIDAD

## 10.1. 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.

## 10.2. PERSONA DE CONTACTO

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

## 10.3. FRECUENCIA DE REVISIÓN

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

## 10.4. PROCEDIMIENTO DE APROBACIÓN

Esta política 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 política 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.

## 11. CONFORMIDAD

Esta Política de Seguridad 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.

## 12. 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.