GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO E INMIGRACIÓN

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

GERENCIA DE INFORMÁTICA
DE LA SEGURIDAD SOCIAL

Centro de Calidad, Auditoría y Seguridad

Declaración de Prácticas de Certificación de la Gerencia de Informática de la Seguridad Social

CORREO ELECTRONICO

C/ Dr. Tolosa Latour, s/n
24041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

Control de cambios

Versión	Observaciones	Fecha
1.0	Versión inicial	10-12-2009
1.1	Asignación de los OIDs	15-12-2009
1.2	Modificación de las ramas internas de OIDs de la GISS	02-02-2010

Índice

1. INTRODUCCIÓN 1
1.1. PRESENTACIÓN 1
1.1.1. Tipos y clases de certificados 2
1.1.2. Relación entre la declaración de prácticas de certificación y otros documentos 2
1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 2
1.3. PARTICIPANTES DE LA PKI 3
1.3.1. Autoridad de certificación 3
1.3.2. Entidades de Registro 3
1.3.3. Usuarios finales 3
1.3.4. Otros participantes 4
1.4. USO DE LOS CERTIFICADOS 4
1.4.1. Usos permitidos de los certificados 4
1.4.2. Aplicaciones prohibidas 4
1.5. ADMINISTRACIÓN DE LA DPC 4
1.5.1. Organización que administra la especificación 5
1.5.2. Datos de contacto de la organización 5
1.5.3. Persona que determina la conformidad de una DPC con la política 5
1.5.4. Procedimiento de aprobación 5
1.6. DEFINICIONES Y ACRÓNIMOS 6
1.6.1. Definiciones 6
1.6.2. Acrónimos 7
2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS 8
2.1. REPOSITORIOS 8
2.2. PUBLICACIÓN DE INFORMACIÓN DE LA ACGISS 8
2.3. FRECUENCIA DE PUBLICACIÓN 8
2.4. CONTROL DE ACCESO 9
3. IDENTIFICACIÓN Y AUTENTICACIÓN 9
3.1. GESTIÓN DE NOMBRES 9
3.1.1. Tipos de nombres 9
3.1.2. Necesidad de que los nombres sean significativos 10

3.1.3. Utilización de anónimos y seudónimos 10
3.1.4. Interpretación de formatos de nombres 10
3.1.5. Unicidad de los nombres 10
3.1.6. Resolución de conflictos relativos a nombres 10
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD 11
3.2.1. Prueba de posesión de clave privada 11
3.2.2. Autenticación de la identidad de una organización 11
3.2.3. Autenticación de la identidad de una persona física 11
3.2.4. Información de suscriptor no verificada 11
3.2.5. Facultades de representación 11
3.2.6. Criterios de interoperabilidad 11
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN 11
3.3.1. Validación para la renovación rutinaria de certificados 11
3.3.2. Validación para la renovación de certificados después de la revocación 12
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN 12

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 12
4.1. SOLICITUD DE EMISIÓN DE CERTIFICADO 12
4.1.1. Quién puede efectuar una solicitud de certificado 12
4.1.2. Proceso de registro y responsabilidades 12
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADO 12
4.2.1. Realización de las funciones de identificación y autenticación 12
4.2.2. Aprobación o denegación de las solicitudes 13
4.3. EMISIÓN DE CERTIFICADOS 13
4.3.1. Acciones de la ACGISS durante el proceso de emisión 13
4.3.2. Notificación de la emisión al suscriptor 13
4.4. ACEPTACIÓN DEL CERTIFICADO 13
4.4.1. Conducta que constituye aceptación del certificado 13
4.4.2. Publicación del certificado 13
4.4.3. Notificación de la emisión a terceros 14
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO 14
4.5.1. Uso por los suscriptores 14
4.5.2. Uso por el tercero que confía en certificados 14
4.6. RENOVACIÓN DE CERTIFICADOS SIN RENOVACIÓN DE CLAVES 14

4.7. RENOVACIÓN DE CERTIFICADO CON RENOVACIÓN DE CLAVES 14
4.7.1. Circunstancias para la renovación con cambio de claves de un certificado 15
4.7.2. Quién puede solicitar la renovación 15
4.7.3. Tramitación de las peticiones 15
4.7.4. Notificación de la emisión al suscriptor 15
4.7.5. Conductas que constituyen la aceptación del certificado con las nuevas claves 15
4.7.6. Publicación del certificado 16
4.7.7. Notificación de la emisión a otras entidades 16
4.8. MODIFICACIÓN DE CERTIFICADOS 16
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 16
4.9.1. Causas de revocación de certificados 16
4.9.2. Legitimación para solicitar la revocación 17
4.9.3. Procedimientos de solicitud de revocación 17
4.9.4. Período de gracia de la solicitud de revocación 17
4.9.5. Plazo máximo de procesamiento de la solicitud de revocación 17
4.9.6. Requisitos de verificación de revocación por terceros 17
4.9.7. Frecuencia de emisión de listas de revocación de certificados (CRLs) 18
4.9.8. Periodo máximo de publicación de CRLs 18
4.9.9. Disponibilidad de servicios online de comprobación de estado de certificados 18
4.9.10. Requisitos de comprobación online de la revocación 18
4.9.11. Otras formas de divulgación de información de revocación disponibles 18
4.9.12. Requerimientos especiales en caso de compromiso de la clave privada 18
4.9.13. Causas de suspensión de certificados 19
4.9.14. Quién puede solicitar la suspensión 19
4.9.15. Procedimientos de petición de suspensión 19
4.9.16. Plazo máximo de suspensión 19
4.10. SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS 19
4.10.1. Características de operación de los servicios 19
4.10.2. Disponibilidad de los servicios 19
4.10.3. Características adicionales 20
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN 20
4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES 20
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 20

5.1. CONTROLES DE SEGURIDAD FÍSICA 20
5.1.1. Localización y construcción de las instalaciones 21
5.1.2. Acceso físico 21
5.1.3. Electricidad y aire acondicionado 21
5.1.4. Exposición al agua 22
5.1.5. Protección y prevención de incendios 22
5.1.6. Almacenaje de soportes 22
5.1.7. Eliminación de soportes de información 22
5.1.8. Backup fuera de las instalaciones 22
5.2. CONTROLES DE PROCEDIMIENTOS 23
5.2.1. Principales perfiles 23
5.2.2. Número de personas por tarea 23
5.2.3. Identificación y autenticación para cada función 23
5.2.4. Roles que requieren separación de tareas 23
5.3. CONTROLES DE PERSONAL 24
5.3.1. Requisitos de historial, calificaciones, experiencia y autorización 24
5.3.2. Procedimientos de investigación de historial 24
5.3.3. Requisitos de formación 25
5.3.4. Requisitos y frecuencia de actualización formativa 25
5.3.5. Sanciones por acciones no autorizadas 25
5.3.6. Requisitos de contratación de profesionales 25
5.3.7. Suministro de documentación al personal 25
5.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD 25
5.4.1. Tipos de eventos registrados 25
5.4.2. Frecuencia de tratamiento de registros de auditoría 26
5.4.3. Periodo de conservación de registros de auditoría 26
5.4.4. Protección de los registros de auditoría 26
5.4.5. Procedimientos de backup 26
5.4.6. Localización del sistema de acumulación de registros de auditoría 26
5.4.7. Notificación de la realización de auditoría al causante del acontecimiento 26
5.4.8. Análisis de vulnerabilidades 27
5.5. ARCHIVO DE INFORMACIONES 27
5.5.1. Tipos de eventos registrados 27

5.5.2. Periodo de conservación de registros 27
5.5.3. Protección del archivo 27
5.5.4. Procedimientos de copia de respaldo 27
5.5.5. Requisitos de sellado de tiempo 28
5.5.6. Sistema de archivo 28
5.5.7. Procedimientos de obtención y verificación de información de archivo 28
5.6. RENOVACIÓN DE LAS CLAVES DE LA AC 28
5.7. COMPROMISO DE CLAVES Y RECUPERACIÓN ANTE DESASTRES 28
5.7.1. Procedimiento de gestión de incidencias y vulnerabilidades 28
5.7.2. Corrupción de recursos, aplicaciones o datos 28
5.7.3. Compromiso de la clave privada de la Entidad 29
5.7.4. Recuperación ante desastres 29
5.8. FINALIZACIÓN DEL SERVICIO 29
5.8.1. Entidad de Certificación 29
5.8.2. Entidad de Registro 30
6. CONTROLES DE SEGURIDAD TÉCNICA 30
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 30
6.1.1. Generación del par de claves 30
6.1.2. Envío de la clave privada al suscriptor 30
6.1.3. Envío de la clave pública al emisor del certificado 31
6.1.4. Distribución de la clave pública de la Autoridad de Certificación 31
6.1.5. Longitud de claves 31
6.1.6. Parámetros de generación de clave pública y verificación de calidad 31
6.1.7. Usos admitidos de las claves 31
6.2. PROTECCIÓN DE LA CLAVE PRIVADA 32
6.2.1. Estándares de módulos criptográficos 32
6.2.2. Control por más de una persona (n de m) sobre la clave privada 32
6.2.3. Repositorio de la clave privada 32
6.2.4. Backup de la clave privada 32
6.2.5. Introducción de la clave privada en el módulo criptográfico 32
6.2.6. Almacenaje de la clave privada en el módulo criptográfico 32
6.2.7. Método de activación de la clave privada. 32
6.2.8. Método de desactivación de la clave privada 33

6.2.9. Método de destrucción de la clave privada 33
6.2.10. Clasificación de los módulos criptográficos 33
6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 33
6.3.1. Archivo de la clave pública 33
6.3.2. Periodos de utilización de las claves pública y privada 33
6.4. DATOS DE ACTIVACIÓN 33
6.4.1. Generación e instalación de los datos de activación 33
6.4.2. Protección de los datos de activación 34
6.4.3. Otros aspectos de los datos de activación 34
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA 34
6.5.1. Requisitos técnicos específicos de seguridad informática 34
6.5.2. Evaluación del nivel de seguridad informática 35
6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA 35
6.6.1. Controles de desarrollo de sistemas 35
6.6.2. Controles de gestión de seguridad 35
6.6.3. Evaluación del nivel de seguridad del ciclo de vida 35
6.7. CONTROLES DE SEGURIDAD DE RED 35
6.8. SELLADO DE TIEMPO 36
7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS 36
7.1. PERFIL DE CERTIFICADO 36
7.2. PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS 36
8. AUDITORÍA DE CONFORMIDAD 36
8.1. FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD 36
8.2. IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR 37
8.3. RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA 37
8.4. RELACIÓN DE ELEMENTOS OBJETO DE AUDITORÍA 37
8.5. ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD 37
8.6. TRATAMIENTO DE LOS INFORMES DE AUDITORÍA 37
9. REQUISITOS COMERCIALES Y LEGALES 38
9.1. TARIFAS 38
9.2. CAPACIDAD FINANCIERA 38
9.2.1. Seguro de responsabilidad civil 38

9.2.2. Otros activos 38
9.3. CONFIDENCIALIDAD 38
9.3.1. Informaciones confidenciales 38
9.3.2. Informaciones no confidenciales 39
9.3.3. Responsabilidad para la protección de información confidencial 39
9.4. PROTECCIÓN DE DATOS PERSONALES 39
9.4.1. Plan de Protección de Datos Personales 39
9.4.2. Información considerada privada 39
9.4.3. Información no considerada privada 40
9.4.4. Responsabilidad correspondiente a la protección de los datos personales 41
9.4.5. Prestación del consentimiento en el uso de los datos personales 41
9.4.6. Divulgación de la información originada por procedimientos administrativos o judiciales 41
9.4.7. Otros supuestos de divulgación de la información 42
9.5. DERECHOS DE PROPIEDAD INTELECTUAL 42
9.5.1. Propiedad de los certificados e información de revocación 42
9.5.2. Propiedad de las políticas de certificación y Declaración de Prácticas de Certificación 42
9.5.3. Propiedad de la información relativa a nombres 42
9.5.4. Propiedad de claves 42
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL 43
9.6.1. Autoridad de Certificación ACGISS 43
9.6.2. Entidades de Registro 43
9.6.3. Suscriptores 44
9.6.4. Verificadores 44
9.7. RENUNCIAS DE GARANTÍAS 44
9.8. LIMITACIONES DE RESPONSABILIDAD 44
9.8.1. Limitaciones de responsabilidad del Prestador de Servicios de Certificación 44
9.8.2. Caso fortuito y fuerza mayor 45
9.9. INDEMNIZACIONES 45
9.10. PLAZO Y FINALIZACIÓN 45
9.10.1. Plazo 45
9.10.2. Finalización 45
9.10.3. Supervivencia 45

9.11. NOTIFICACIONES 45
9.12. MODIFICACIONES DE LA DPC 46
9.12.1. Procedimiento para las modificaciones 46
9.12.2. Periodo y mecanismos para notificaciones 46
9.12.3. Circunstancias en las que un OID tiene que ser cambiado 46
9.13. RESOLUCIÓN DE CONFLICTOS 46
9.13.1. Resolución extrajudicial de conflictos 46
9.13.2. Jurisdicción competente 46
9.14. LEGISLACIÓN APLICABLE 47
9.15. CONFORMIDAD CON LA LEGISLACIÓN APLICABLE 47
9.16. CLÁUSULAS DIVERSAS 47

1. INTRODUCCIÓN

1.1. Presentación

La Gerencia de Informática de la Seguridad Social (en adelante GISS) es un Servicio Común que proporciona servicios informático al conjunto de organismos que configuran la Seguridad Social. Dentro de la estrategia impulsada de adaptación a la legislación electrónica, con la intención de mejorar el servicio prestado a los ciudadanos y empresas, la GISS ha configurado una Autoridad de Certificación, denominada ACGISS (Entidad de Certificación de la Gerencia de Informática de la Seguridad Social) que expide certificados electrónicos.

Esta declaración determina las características de la ACGISS como Autoridad de Certificación, y es complementada por una Política de Certificación por cada uno de los tipos de certificados que emita.

Para la elaboración del presente documento se ha seguido el estándar RFC 3647 (*"Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framewok"*), del IETF (Internet Engineering Task Force), realizando las adaptaciones necesarias tanto para facilitar su lectura y análisis como para cumplir con la legislación española vigente.

En cuanto al marco legislativo, cabe destacar las siguientes normativas:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

Asimismo, se han tenido en cuenta los estándares europeos, entre los que cabe destacar los siguientes:

- ETSI 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- ETSI 101 862: Qualified Certificate Profile

1.1.1. Tipos y clases de certificados

La ACGISS emite diferentes tipos de certificados. En su comienzo emite cuatro tipos de certificados:

- Certificados de Empleado Público, que son emitidos a empleados públicos (personal funcionario, laboral y eventual) de la Seguridad Social y tienen con propósito de identificación, firma electrónica reconocida y cifrado de datos, para el desempeño de las funciones propias del puesto que ocupen o para relacionarse con otras Administraciones Públicas cuando éstas lo admitan.
- Certificados de Personal Externo, que son emitidos a trabajadores externos que prestan sus servicios en las oficinas de la Seguridad Social. Comparten funcionalidad y propósito con los certificados de Empleado Público.
- Certificados de sello. Emitidos a organismos de la Seguridad Social con propósito de firma de documentos administrativos en el ámbito de sus funciones.
- Certificados de sede. Emitido a la Seguridad Social y con propósito de su autenticación y cifrado de los canales de comunicación con la futura Sede Electrónica de la Segundad Social.

En el futuro, la ACGISS se reserva el derecho de emitir nuevos tipos de certificados o cesar en la emisión de los ya existentes.

1.1.2. Relación entre la declaración de prácticas de certificación y otros documentos

Este documento contiene la Declaración de Prácticas de Certificación (DPC) de la ACGISS, como Autoridad de Certificación de la GISS. Cada uno de los certificados que emita tendrá su correspondiente Política de Certificación.

Esta DPC incluye los procedimientos que aplica en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

1.2. Nombre del documento e identificación

Nombre del documento	ACGISS. Declaración de Prácticas de Certificación
Versión	1.2
Estado del documento	Aprobado
Fecha de emisión	02 de febrero de 2010
OID	2.16.724.1.4.2.1.1
Localización	www.seg-social.es

Significado del OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) ACGISS (1) DPC (1)

1.3. Participantes de la PKI

1.3.1. Autoridad de certificación

La Autoridad de Certificación es la ACGISS.

La ACGISS proporciona servicios de expedición y gestión de certificados a usuarios finales. Los datos fundamentales de la AC son los siguientes:

Nombre Distintivo	cn=OU=SGI,O=Seg-Social,C=ES
Certificado pkcs1-sha1WithRSAEncryption	
Número de Serie	3e4ce218
Período de validez	Desde viernes, 14 de febrero de 2003 13:03:28 Hasta martes, 14 de febrero de 2023 13:33:28
Huella digital (SHA-1)	a6 7b 6a 93 09 70 66 93 cc be f0 7e b2 b1 59 c3 f4 bb d9 af
Algoritmo de firma	sha1RSA
Clave Pública	RSA(1024)

1.3.2. Entidades de Registro

Las Entidades de Registro son las encargadas de los trámites de identificación y autenticación de los usuarios que solicitan certificados electrónicos, cuando así se requiera en las correspondientes políticas de certificación.

Actuarán como entidades de registro las unidades, dependencias u oficinas de las Entidades Gestoras y Servicios Comunes de la Seguridad Social que se designen al efecto en cada Política de Certificación específica.

1.3.3. Usuarios finales

Los usuarios finales son las personas que obtienen y utilizan certificados emitidos por la Seguridad Social.

1.3.4. Otros participantes

- Autoridad de validación (AV)
  Es la encargada de comprobar el estado de los certificados emitidos por la Seguridad Social, mediante el uso del protocolo OCSP.

- Autoridad de sellado de tiempo.
  Su función es aportar evidencia de la fecha y la hora en la que se realizan los diferentes trámites de la PKI, de acuerdo a la legislación vigente.
  Este componente es un servicio común gestionado por la Gerencia Informática de la Seguridad Social.

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede utilizarse cada tipo de certificado, estableciendo limitaciones y prohibiendo algunas aplicaciones.

1.4.1. Usos permitidos de los certificados

Los certificados emitidos por ACGISS serán utilizados para dar cumplimiento a las funciones propias y legítimas de los organismos que conforman la Seguridad Social y sus trabajadores. Se emitirán de acuerdo con lo establecido en el artículo 11 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y se cumplirán las obligaciones determinadas en dicha Ley y en las normativas específicas vigentes en el ámbito de la Administración General del Estado.

El uso específico de cada uno de los certificados emitidos por ACGISS está referido en su correspondiente Política de Certificación.

1.4.2. Aplicaciones prohibidas

De forma general, no se permitirá el uso de los certificados para fines distintos de los establecidos como válidos en esta DPC y en las políticas de certificación existentes.

Las limitaciones y restricciones concretas en el uso de los certificados se establecerán en la Política de Certificación específica.

1.5. Administración de la DPC

La ACGISS da soporte a la elaboración, aprobación y conformidad de las presente DPC.

1.5.1. Organización que administra la especificación

Nombre	Gerencia de Informática de la Seguridad Social		
Dirección e-mail	eladio.quintanilla@giss.seg-social.es		
Dirección	C/ Albasanz nº 23, 28037 Madrid		
Teléfono	91 390 27 03	**Fax**	91 460 40 72

1.5.2. Datos de contacto de la organización

Nombre	Centro de Calidad, Auditoría y Seguridad (Gerencia de Informática de la Seguridad Social)		
Dirección e-mail	giss-ccas.solicitudes@giss.seg-social.es		
Dirección	C/ Albasanz nº 23, 28037 Madrid		
Teléfono	91 390 27 18	**Fax**	91 390 51 67

1.5.3. Persona que determina la conformidad de una DPC con la política

Nombre	Centro de Calidad, Auditoría y Seguridad (Gerencia de Informática de la Seguridad Social)		
Dirección e-mail	giss-ccas.solicitudes@giss.seg-social.es		
Dirección	C/ Albasanz nº 23, 28037 Madrid		
Teléfono	91 390 27 18	**Fax**	91 390 51 67

1.5.4. Procedimiento de aprobación

La DPC y las Políticas de Certificación están sometidas a un riguroso proceso de aprobación y revisión

En virtud del mismo, las versiones de estos documentos se envían a los centros de la GISS para su revisión y son finalmente publicadas en la Intranet para su general conocimiento y asunción.

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

Activación: es el procedimiento por el cual se desbloquean las condiciones de acceso a un clave y se permite su uso.

Actuación administrativa automatizada: Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

Autenticación: Acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos, y de la integridad y autoría de estos últimos.

Certificado electrónico: Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Certificado electrónico reconocido: Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Dispositivo seguro de creación de firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Firma electrónica: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Firma electrónica avanzada: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

1.6.2. Acrónimos

AC	Autoridad de Certificación
AV	Autoridad de Validación
ACGISS	Autoridad de Certificación de la Gerencia de Informática de la Seguridad Social
CCAS	Centro de Calidad, Auditoría y Seguridad (GISS)
CN	Common Name (Nombre común. Atributo del DN de un objeto)
CRL	Certificate Revocation List (Lista de Certificados Revocados)
CWA	CEN Workshop Agreement
DN	Distinguished Name (Nombre distintivo)
DPC	Declaración de Prácticas de Certificación
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
GISS	Gerencia de Informática de la Seguridad Social
HSM	Hardware Security Module (Modulo hardware de seguridad criptográfica)
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol (Protocolo ligero de acceso a directorios)
OCSP	Online Certificate Status Protocol
OID	Object Identifier (Identificador de objeto)
PC	Política de certificación
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure (Infraestructura de clave pública)
RFC	Request for Comments (IETF)
RSA	Rivest-Shimar-Adleman
SHA-1	Secure Hash Algorithm
TSL	Transport Layer Security

2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1. Repositorios

El servicio de repositorio de certificados está disponible durante las 24 horas de los 7 días de la semana.

Toda la información publicada estará disponible en la página Web de la Seguridad Social (www.seg-social.es)

2.2. Publicación de información de la ACGISS

La ACGISS publica las siguientes informaciones en su repositorio:

- Un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes, o si su vigencia ha sido suspendida o extinguida.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La política general de certificación, compuesta por la presente DPC y las Políticas de Certificación de los diferentes certificados emitidos.

Todo cambio en las especificaciones o condiciones del servicio se comunicará a los usuarios por la ACGISS a través del repositorio.

En todos los casos se hará una referencia explícita a los cambios en la página principal de la Web del servicio, a la que se accede a través del portal de la Seguridad Social “www.seg-social.es”

No se retira la versión anterior del documento objeto del cambio, sino que se indica que ha sido substituido por la versión nueva.

2.3. Frecuencia de publicación

La información de la ACGISS se publicará cuando se encuentre disponible y en especial, de forma inmediata cuando se emitan las menciones relativas a la vigencia de los certificados.

Los cambios en este documento se rigen por lo establecido en la sección correspondiente. La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones correspondientes.

Al cabo de 15 días desde la publicación de la nueva versión, se retirará la referencia al cambio de la página principal y se insertará en el repositorio.

Las versiones antiguas de la documentación son conservadas durante 15 años por la ACGISS, pudiendo ser consultadas por causa razonada por los interesados.

2.4. Control de acceso

La ACGISS no limita el acceso de lectura a las informaciones establecidas en la sección correspondiente, pero establece controles para mantener la integridad del directorio actualizado de los certificados expedidos y la protección de la integridad y autenticidad de la información de estado de revocación.

La ACGISS utiliza sistemas fiables para el Repositorio, de manera tal que:

- Se pueda comprobar la autenticidad de los certificados.
- Las personas no autorizadas no pueden alterar los datos.
- Los certificados solamente están accesibles en los supuestos o a las personas que el firmante indique.
- Detecte cualquier cambio técnico que afecte a los requisitos de seguridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Gestión de nombres

En esta sección se establecen requisitos relativos a los procedimientos de identificación y autenticación que se utilizan durante el registro de los suscriptores, que tiene que realizarse con anterioridad a la emisión y entrega de certificados.

3.1.1. Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN).

Se incluye en estos certificados la siguiente información:

- Country: ES (corresponde al código ISO de país, correspondiente al Estado Español).

- Organizational Unit Name: El nombre del tipo de servicio de certificación que se presta.
- Organizational Unit Name: Es la dirección Web de las condiciones generales de uso del certificado
- Surname: Los apellidos del suscriptor, autorizado por la Entidad de Registro
- Given Name: El nombre del suscriptor, autorizado por la Entidad de Registro
- Serial Number: DNI., del suscriptor, autorizado por la Entidad de Registro
- Common Name: El nombre en texto libre del suscriptor, autorizado por la Entidad de Registro

3.1.2. Necesidad de que los nombres sean significativos

Las reglas mencionadas en el apartado anterior, garantizan que los nombres utilizados en los certificados son suficientemente significativos.

3.1.3. Utilización de anónimos y seudónimos

No se pueden utilizar anónimos ni seudónimos.

3.1.4. Interpretación de formatos de nombres

La regla utilizada para interpretar los nombres distintivos de los certificados es ISO/ IEC 9595 (X.500) Distinguished Name (DN).

3.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada servicio de generación de certificados operado por la ACGISS y para cada tipo de certificado.

No se podrá volver a asignar un nombre de suscriptor que ya haya estado ocupado a un suscriptor diferente.

3.1.6. Resolución de conflictos relativos a nombres

La resolución de conflictos relativos a los nombres se realizará de acuerdo a lo estipulado en este documento en relación con la resolución general de conflictos y la jurisdicción aplicable.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Debido a que el procedimiento de generación del par de claves depende del tipo de certificado emitido, la prueba de posesión de la clave privada se describirá en cada política de certificación específica.

3.2.2. Autenticación de la identidad de una organización

Dependiendo del certificado reconocido en concreto, la autenticación se especifica en la correspondiente Política de Certificación.

3.2.3. Autenticación de la identidad de una persona física

Dependiendo del certificado reconocido en concreto, la autenticación se especifica en la correspondiente Política de Certificación.

3.2.4. Información de suscriptor no verificada

No estipulado.

3.2.5. Facultades de representación

Para la comprobación de las facultades de representación de personas físicas o jurídicas, se atenderá a lo dispuesto en la legislación vigente.

3.2.6. Criterios de interoperabilidad

No se contempla la interrelación de la PKI con entidades externas.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

Este apartado es dependiente del certificado reconocido en particular y está recogido en su correspondiente Política de Certificación.

3.3.2. Validación para la renovación de certificados después de la revocación

La renovación de certificados después de la revocación no es posible, sino que es necesaria la emisión de un nuevo certificado.

3.4. Identificación y autenticación de la solicitud de revocación

Este apartado es dependiente del certificado reconocido en particular y está recogido en su correspondiente Política de Certificación.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. Solicitud de emisión de certificado

4.1.1. Quién puede efectuar una solicitud de certificado

Puesto que los usuarios finales a los que se emiten los certificados dependen del tipo de certificado de que se trate, este apartado se establecerá en la política específica correspondiente.

4.1.2. Proceso de registro y responsabilidades

Al igual que en el apartado anterior, se establecerá en la política específica del certificado correspondiente.

4.2. Tramitación de la solicitud de certificado

4.2.1. Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación las realizará el personal destinado al efecto en las Entidades de Registro existentes.
Para cualquier aspecto específico de la identificación y autenticación de los usuarios se remite a la política correspondiente de cada certificado.

4.2.2. Aprobación o denegación de las solicitudes

Las condiciones para la aprobación o denegación de las solicitudes de certificados, se establecerán en las políticas de certificación correspondientes.

4.3. Emisión de certificados

4.3.1. Acciones de la ACGISS durante el proceso de emisión

Después de la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone el certificado a disposición del suscriptor.

Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados, ya que ésta implica la emisión de un nuevo certificado.

La ACGISS:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.
- Toma medidas contra la falsificación de certificados.

Las características particulares de las acciones de la ACGISS se especifican en la correspondiente Política de Certificación.

4.3.2. Notificación de la emisión al suscriptor

No estipulado.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye aceptación del certificado

Este apartado depende del tipo en particular de certificado y se especifica en su correspondiente Política de Certificación

4.4.2. Publicación del certificado

Este punto no es aplicable.

4.4.3. Notificación de la emisión a terceros

No estipulado.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por los suscriptores

Los suscriptores podrán utilizar las claves y los certificados para los usos autorizados en la presente DPC y en las correspondientes Políticas de Certificación.

Este uso debe cesar tras la extinción de la vigencia o la revocación del certificado del titular.

Se distinguen las siguientes finalidades de los certificados emitidos por la PKI:
- Certificado de autenticación: Permite garantizar la identidad del usuario.
- Certificado de firma electrónica: Permite la firma electrónica de documentos.
- Certificado de cifrado: Se utilizará para el cifrado de datos y documentos electrónicos.

El uso concreto por los suscriptores depende del tipo de certificado y está especificado en la correspondiente Política de Certificación.

4.5.2. Uso por el tercero que confía en certificados

Los terceros que confíen en los certificados emitidos por la PKI, están obligados al cumplimiento de las condiciones de uso establecidas en la presente DPC y en las correspondientes Políticas de Certificación.

4.6. Renovación de certificados sin renovación de claves

No se realizará la renovación de certificados sin renovación de las claves

4.7. Renovación de certificado con renovación de claves

Las condiciones particulares de renovación dependen del certificado en concreto y están especificadas en la correspondiente Política de Certificación.

Una vez transcurrido el periodo de vigencia, si el certificado no ha sido renovado, quedará inutilizable, siendo necesaria la revocación del mismo para la emisión de uno nuevo.

En el caso de establecerse alguna modificación en las Políticas o Prácticas de Certificación que implicase un cambio en el periodo de validez de las claves del certificado, no afectaría a los certificados ya existentes, sino solamente a los emitidos después de dicha modificación.

4.7.1. Circunstancias para la renovación con cambio de claves de un certificado

Todas las renovaciones de certificado se realizarán con cambio de claves.

El período de validez de cada tipo de certificado será el que se disponga en las correspondientes Políticas de Certificación, transcurrido el cual, el certificado quedará inutilizable, siendo necesaria la revocación del mismo para la emisión de uno nuevo.

Se podrán dar los siguientes casos de renovación de un certificado:

- Renovación de los certificados por deterioro del soporte, en su caso, o por variación de los datos recogidos en ellos.
- Renovación de los certificados por pérdida del anterior.
- Renovación por caducidad de los certificados sin que cambie el soporte.

4.7.2. Quién puede solicitar la renovación

La renovación se realizará de oficio por la AC o de forma voluntaria y por iniciativa del usuario final.
En caso de que existan condiciones específicas para cada tipo de certificado, se establecerán en las correspondientes Políticas de Certificación.

4.7.3. Tramitación de las peticiones

En los casos en los que exista un procedimiento de renovación concreto, se establecerá en su correspondiente Política de Certificación.

4.7.4. Notificación de la emisión al suscriptor

No estipulado.

4.7.5. Conductas que constituyen la aceptación del certificado con las nuevas claves

Se consideran las mismas condiciones que para el caso de la emisión inicial de certificados, señaladas en el apartado correspondiente.

4.7.6. Publicación del certificado

No estipulado.

4.7.7. Notificación de la emisión a otras entidades

No estipulado.

4.8. Modificación de certificados

No se permitirá la modificación de los certificados emitidos.

4.9. Revocación y suspensión de certificados

4.9.1. Causas de revocación de certificados

La revocación conlleva la pérdida de validez de un certificado electrónico. Son causas de dicha revocación:

- Expiración del período de validez que figura en el certificado.
- Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación, o utilización indebida de dichos datos por un tercero.
- Resolución judicial o administrativa que lo ordene.
- Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
  Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- Por renovación o expedición de un nuevo certificado que sustituya al actual, en cuyo caso se realiza una revocación automática del anterior.

Además de estas condiciones, cada uno de los certificados puede tener sus condiciones particulares de revocación especificadas en su correspondiente Política de Certificación.

4.9.2. Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- El suscriptor a nombre del que el certificado fue emitido.
- La Entidad de Registro que intervino en la emisión.
- La ACGISS.

4.9.3. Procedimientos de solicitud de revocación

El procedimiento depende de cada certificado y está especificado en la correspondiente Política de Certificación.

4.9.4. Período de gracia de la solicitud de revocación

Las solicitudes de revocación se remiten de forma razonablemente inmediata cuando se tenga conocimiento de la causa de revocación, por lo que no existe ningún período de gracia asociado a este proceso.

4.9.5. Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación será procesada en el mínimo plazo posible, siempre dentro de los horarios de oficina del Prestador de Servicios de Certificación.

En caso de encontrarse fuera de horas de oficina, el suscriptor solicita la suspensión cautelar del certificado.

4.9.6. Requisitos de verificación de revocación por terceros

Los usuarios deberán comprobar el estado de aquellos certificados en los que deseen confiar.

El procedimiento ordinario de comprobación de la validez de los certificados será mediante consulta a la Autoridad de Validación, mediante el uso del protocolo OCSP.

4.9.7. Frecuencia de emisión de listas de revocación de certificados (CRLs)

La ACGISS emite una CRL al menos cada hora, o bien de forma inmediata cada vez que se produce la revocación de al menos uno de sus certificados.

Se indica en la CRL el momento programado de emisión de una nueva CRL, si bien se puede emitir una CRL antes del plazo indicado en la CRL anterior.

4.9.8. Periodo máximo de publicación de CRLs

Las CRLs no se publicarán en repositorios de acceso libre.

4.9.9. Disponibilidad de servicios online de comprobación de estado de certificados

Los usuarios pueden consultar el estado de los certificados emitidos por la ACGISS a través de la Autoridad de Validación que está disponible las 24 horas de los 7 días de la semana.

En caso de error de los sistemas de comprobación del estado de los certificados por causas fuera del control de la ACGISS, ésta realiza sus mayores esfuerzos para asegurar que este servicio se mantenga inactivo el mínimo tiempo posible. La ACGISS suministrará información a los usuarios sobre el funcionamiento del servicio de información del estado de los certificados.

4.9.10. Requisitos de comprobación online de la revocación

Para ella comprobación online del estado de los certificados, se deberá disponer de un software capaz de operar con el protocolo OCSP.

4.9.11. Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.9.12. Requerimientos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de la ACGISS es notificado, en la medida posible, a todos los participantes en el dominio del Prestador de Servicios de Certificación.

4.9.13. Causas de suspensión de certificados

No estipulado.

4.9.14. Quién puede solicitar la suspensión

No estipulado.

4.9.15. Procedimientos de petición de suspensión

No estipulado.

4.9.16. Plazo máximo de suspensión

No estipulado.

4.10. Servicios de comprobación del estado de los certificados

4.10.1. Características de operación de los servicios

Para la validación de los certificados se dispone de una Autoridad de Validación que proporciona información de los certificados emitidos por la ACGISS.

Se trata de un servicio online que implementa el protocolo OCSP (On-Line Certificate Status Protocol) siguiendo la RFC 2560. Para la consulta del estado, se envía una petición a la AV, la cual ofrece una respuesta vía HTTP.

4.10.2. Disponibilidad de los servicios

Los sistemas de consulta en línea del estado de los certificados están disponibles las 24 horas de los 7 días de la semana.

En caso de fallo de los sistemas de comprobación del estado de certificados por causas fuera del control de la ACGISS, ésta realizará sus mayores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible. La ACGISS detallará en este documento el periodo máximo de tiempo en el que el servicio tendrá que volver a operar.

El Prestador de Servicios de Certificación suministra información a los titulares de sus certificados sobre el funcionamiento del servicio de información de estado de certificados.

4.10.3. Características adicionales

No estipulado.

4.11. Finalización de la suscripción

La extinción de la validez de los certificados emitidos por la ACGISS se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas enumeradas en este documento.
- Caducidad de la vigencia del certificado.

4.12. Custodia y recuperación de claves

No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

5.1. Controles de seguridad física

La ACGISS ofrece a sus suscriptores un nivel adecuado de seguridad física para la realización de las tareas imprescindibles en la generación y gestión de los certificados.

De esta forma dispone de instalaciones con diversos perímetros de seguridad alrededor de los servicios de generación de certificados, de los dispositivos criptográficos y de la gestión de revocación

Así la ACGISS controla la seguridad física y ambiental de las instalaciones y los sistemas que se encuentran en dichas instalaciones, con las siguientes medidas:

- Controles de acceso físico.
- Protección ante desastres naturales.
- Medidas de protección ante incendios.
- Fallo de los sistemas de soporte (energía eléctrica, telecomunicaciones, etc.).
- Derribo de la estructura.

- Inundaciones.
- Protección antirrobo.
- Conformidad y entrada no autorizada.
- Recuperación ante un desastre.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativas a componentes utilizados para los servicios de la ACGISS.

5.1.1. Localización y construcción de las instalaciones

La localización de las instalaciones permite la presencia de fuerzas de seguridad en un plazo de tiempo razonable desde que una incidencia les sea notificada (en el caso de no contar con presencia física permanente de personal de seguridad de la ACGISS).

La existencia de un perímetro de protección que garantice unos niveles de protección adecuados ante intrusiones por fuerza bruta.

5.1.2. Acceso físico

El Prestador de Servicios de Certificación establece niveles de seguridad con restricción de acceso diferentes a los perímetros y barreras físicas definidas.

Para el acceso a las dependencias del Prestador de Servicios de Certificación, donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, es necesaria autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

La generación de claves criptográficas del Prestador de Servicios de Certificación, así como su almacenaje, se realiza en dependencias específicas para estas finalidades, y requieren de acceso y permanencia dobles.

5.1.3. Electricidad y aire acondicionado

Los equipos informáticos del Prestador de Servicios de Certificación están convenientemente protegidos ante fluctuaciones o cortes de suministro eléctrico, que puedan dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el subministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos están ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

5.1.4. Exposición al agua

Existen las medidas de detección adecuadas para prevenir la exposición al agua de los equipos y el cableado del Prestador de Servicios de Certificación.

5.1.5. Protección y prevención de incendios

Todas las instalaciones y activos del Prestador de Servicios de Certificación cuentan con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos y soportes que almacenen claves del Prestador de Servicios de Certificación, cuentan con un sistema específico y adicional al resto de la instalación, para la protección ante el fuego.

5.1.6. Almacenaje de soportes

El almacenaje en soportes de información se realiza de forma que se garantice tanto su integridad como su confidencialidad y cumpliendo los requisitos mínimos establecidos por la legislación de protección de carácter personal vigente.

Se cuenta para ello con dependencias o armarios ignífugos y robots automatizados de tratamiento de cintas.

5.1.7. Eliminación de soportes de información

La eliminación de soportes se realiza mediante un contrato con una empresa, con métodos seguros.

5.1.8. Backup fuera de las instalaciones

La ACGISS dispone de un centro de respaldo remoto en el que la infraestructura de la PKI está incluida.

5.2. Controles de procedimientos

La ACGISS garantiza que sus sistemas se operan de forma segura, y por esto establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

El personal al servicio de la ACGISS realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de la ACGISS.

5.2.1. Principales perfiles

Se distinguen los siguientes perfiles en la gestión de de la PKI:

- Administradores de Sistema: Usuarios autorizados para realizar las tareas relacionadas con la instalación, configuración y mantenimiento de los sistemas de la PKI.
- Auditores de sistemas: Encargados de la consulta de las trazas y logs de los sistemas de la PKI.
- Responsable de seguridad. Usuarios responsables de la definición, verificación, administración e implementación de las políticas, normas y procedimientos de seguridad.
- Responsables de registro. Son los responsables de llevar a cabo las tareas relacionadas con la identificación y autenticación de los suscriptores de los certificados, así como de la solicitud en su nombre de la emisión/revocación de los mismos.
- Operadores de sistemas: Serán los usuarios encargados de realizar las tareas básicas relativas a los sistemas involucrados en la PKI, incluyendo los procesos de backup y recuperación.

5.2.2. Número de personas por tarea

Las funciones básicas de la PKI de la ACGISS están soportadas por más de una persona, en grupos de trabajo activos y de respaldo, dentro de un plan que garantizan una disponibilidad inmediata en caso de contingencia grave en sus instalaciones.

5.2.3. Identificación y autenticación para cada función

La ACGISS tiene implantados unos estrictos sistemas de autenticación y autorización, de forma que su personal sólo accede a aquellos servicios que deba para realizar estrictamente sus funciones. De esta forma se preserva la integridad, confidencialidad y disponibilidad de la información manejada por el Prestador.

5.2.4. Roles que requieren separación de tareas

Las prácticas de trabajo en la ACGISS siguen el principio de que las tareas principales de administración y operación de los sistemas son realizadas por más un trabajador, en ocasiones de

departamentos diferentes, para minimizar el riesgo de actuaciones ilegítimas por parte de alguno de sus trabajadores.

5.3. Controles de personal

La ACGISS tiene en cuenta, en cuanto a los controles de personal, los siguientes aspectos:

- Se mantiene confidencialidad de la información, asignando los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones y, fuera del ámbito laboral, en aquello referente a la seguridad de las infraestructuras.
- Se es diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en este documento.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen soportes de información a niveles de seguridad inferiores.
- Se utilizan los activos de la infraestructura para las finalidades que les han sido encomendadas.
- Se exige documentación escrita que marque sus funciones y medidas de seguridad a las que está sometido.
- El responsable de seguridad vela porque el punto anterior sea ejecutado, proporcionando a los responsables de área toda la información que fuera necesaria.
- No se instalan en ninguno de los sistemas de la infraestructura software o hardware que no sea expresamente autorizado por escrito por el responsable de sistemas de información.
- No se accede voluntariamente, ni se elimina o altera información no destinada a su persona o perfil profesional.

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

El personal funcionario que trabaja en la ACGISS debe superar un proceso de selección previo antes de tomar posesión de su puesto de trabajo, además de pertenecer a cuerpos especializados en el desarrollo y operación de los sistemas informáticos, así como en la gestión de proyectos.

El personal de empresas externas está clasificado por categorías profesionales y debe acreditar conocimientos o experiencia en las materias que debe dominar en sus puestos de trabajo.

El personal en los puestos más críticos se encuentra libre de intereses personales que entren en conflicto con el desarrollo de la función que tenga encomendada.

5.3.2. Procedimientos de investigación de historial

No estipulado.

5.3.3. Requisitos de formación

La ACGISS se ocupa de formar al personal funcionario y de solicitar formación para el personal externo para lograr la calificación adecuada y saber responder ante situaciones de contingencia.

5.3.4. Requisitos y frecuencia de actualización formativa

Cuando es necesario se imparten cursos especializados, según los procedimientos que se establezca la GISS.

5.3.5. Sanciones por acciones no autorizadas

La ACGISS, en su condición de administración pública, está sometida a un régimen disciplinario para todos sus funcionarios. Por otra parte, garantiza que se aplican cláusulas disciplinarias en los contratos de soporte técnico con las empresas externas, de manera que la responsabilidad del trabajador externo se transfiera a su empresa en caso de conducta punible.

5.3.6. Requisitos de contratación de profesionales

El Prestador de Servicios de Certificación contrata profesionales cualificados para la ejecución efectiva de las funciones propias de certificación y de registro.

El perfil del personal contratado está especificado en las cláusulas de los pliegos de contratación de las empresas.

5.3.7. Suministro de documentación al personal

La ACGISS suministra la documentación que estrictamente necesite su personal en cada momento, con el fin de que sea adecuadamente competente en sus labores de administración de la PKI.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

La ACGISS guarda registro de los eventos más significativos relacionados con la seguridad de la entidad.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinan cuando existen sospechas o pruebas recabadas en otras fuentes de conductas punibles.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría también tienen que estar documentadas.

5.4.3. Periodo de conservación de registros de auditoría

Los registros de auditoría se retienen durante al menos un año después de procesarlos y a partir de ese momento se archivan de acuerdo con la sección correspondiente de este documento.

5.4.4. Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como eléctricos, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5.4.5. Procedimientos de backup

Se generan diariamente copias de soporte incrementales del registro de auditoría y semanalmente copias completas.

5.4.6. Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría es, al menos, un sistema interno de la ACGISS, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

5.4.7. Notificación de la realización de auditoría al causante del acontecimiento

No estipulado.

5.4.8. Análisis de vulnerabilidades

Los eventos en el proceso de auditoría son guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad son ejecutados, repasados y revisados por medio de un examen de estos eventos monitorizados.

Estos análisis son ejecutados de acuerdo con su definición en el Plan de Auditoría del Prestador de Servicios de Certificación.

5.5. Archivo de informaciones

La ACGISS garantiza que toda la información relativa a los certificados se guarda durante un periodo de tiempo apropiado.

5.5.1. Tipos de eventos registrados

La ACGISS conserva registrada por medios seguros toda la información y documentación relativa a los certificados generados y a las declaraciones de prácticas de certificación.

5.5.2. Periodo de conservación de registros

La ACGISS guarda los registros especificados en la sección correspondiente de este documento durante 15 años, contados desde el momento de la expedición del certificado.

5.5.3. Protección del archivo

El Prestador de Servicios de Certificación:

- Mantiene la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archiva los datos indicados anteriormente de forma completa y confidencial.
- Mantiene la privacidad de los datos de registro del suscriptor.

5.5.4. Procedimientos de copia de respaldo

La ACGISS realiza a diario copias incrementales de todos los datos que configuran su PKI. Además, realiza copias de soporte completas al menos una vez a la semana para casos de recuperación de datos.

Los datos así recogidos se almacenan en un sistema de jerarquía de soportes de copias de seguridad que garantiza la integridad y la confidencialidad de las copias, así como la aplicación de una política predefinida de respaldo.

5.5.5. Requisitos de sellado de tiempo

Se garantiza el instante de tiempo en el que se realizan las principales actuaciones de la PKI mediante la Autoridad de Sellado de Tiempo de la GISS.

5.5.6. Sistema de archivo

El sistema de archivo es interno dentro de la ACGISS. Además, la ACGISS tiene un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, así como se especifica en la sección correspondiente de este documento.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Solamente personas autorizadas por la ACGISS tienen acceso a los datos de archivo, sea en las mismas instalaciones de la ACGISS o en su ubicación externa.

5.6. Renovación de las claves de la AC

Los procedimientos para proporcionar la nueva clave de la AC serán los mismos que para proporcionar la clave pública en vigor.

5.7. Compromiso de claves y recuperación ante desastres

5.7.1. Procedimiento de gestión de incidencias y vulnerabilidades

El Prestador de Servicios de Certificación establece los procedimientos que aplica en la gestión de las incidencias y, muy especialmente, en los compromisos de la seguridad de las claves.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos, la ACGISS iniciará las gestiones necesarias para hacer que el sistema vuelva a su estado normal de funcionamiento

5.7.3. Compromiso de la clave privada de la Entidad

El plan de contingencia del Prestador de Servicios de Certificación considera el compromiso o sospecha de compromiso de la clave privada del Prestador de Servicios de Certificación como un desastre.

En caso de compromiso la ACGISS:

- Informará a todos los suscriptores y usuarios del compromiso.
- Indicará que los certificados y la información del estado de revocación entregados usando la clave de este Prestador de Servicios de Certificación ya no son válidos.

5.7.4. Recuperación ante desastres

La ACGISS desarrolla, mantiene, prueba y, si es necesario, ejecuta un plan de emergencia en el caso de desastre, ya sea por causas naturales o intencionadas, sobre las instalaciones, que indique cómo se restauran los servicios de los sistemas de información.

La ubicación de los sistemas de recuperación de desastres dispone de las protecciones físicas de seguridad detalladas en la documentación del proyecto de Centro de Respaldo.

La ACGISS es capaz de restaurar la operación normal de la PKI en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Revocación de certificados.
- Publicación de información de revocación.

La base de datos de recuperación de desastres utilizada por el Prestador de Servicios de Certificación está sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el Plan de Seguridad. Los equipos de recuperación de desastres de la ACGISS tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8. Finalización del servicio

5.8.1. Entidad de Certificación

La ACGISS asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios de la ACGISS y, en particular, asegura un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en procedimientos legales.

Antes de finalizar su actividad como prestador de Servicios de Certificación, la ACGISS realizará los siguientes procedimientos:

- Informará a todos los suscriptores y usuarios.
- En caso de emitir certificados para el público, deberá informar al menos dos meses antes al Ministerio de Ciencia y Tecnología del cese de su actividad.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los periodos de tiempo respectivos indicados al suscriptor y a los verificadores.
- Destruirá las claves privadas de la ACGISS o las retirará del uso.

La ACGISS transferirá los certificados, en los términos previstos el artículo 21 de la Ley 59/2003, de 19 de diciembre.

5.8.2. Entidad de Registro

No estipulado.

6. CONTROLES DE SEGURIDAD TÉCNICA

La ACGISS utiliza sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves del certificado raíz de la AC se genera en un módulo de hardware criptográfico HSM, que cumple con los requisitos de seguridad FIPS 140-1 nivel 3 o superior.

Las claves de los certificados emitidos se generarán según lo dispuesto en su correspondiente Política de Certificación.

6.1.2. Envío de la clave privada al suscriptor

El envío de la clave privada al titular se realizará de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

6.1.3. Envío de la clave pública al emisor del certificado

El procedimiento de envío de la clave pública depende del tipo de certificado, por lo que se especificará en la Política de Certificación correspondiente.

6.1.4. Distribución de la clave pública de la Autoridad de Certificación

Las claves públicas de la ACGISS como Autoridad de Certificación son comunicadas a los verificadores de sus certificados emitidos, asegurando la integridad de la clave y autenticando el origen.

La clave pública de la GISS se publica en el Repositorio de la ACGISS, en forma de certificado auto firmado, junto a una declaración referente a que la clave permite autenticar a la ACGISS.

Los usuarios acceden al Repositorio para obtener las claves públicas de la Autoridad de Certificación.

6.1.5. Longitud de claves

Las claves de la ACGISS son al menos de 1.024 bits.

La longitud de las claves de los suscriptores de certificados, se especificarán en la correspondiente Política de Certificación.

6.1.6. Parámetros de generación de clave pública y verificación de calidad

Los parámetros de clave pública son generados conforme a la PKCS#1. El algoritmo usado para la generación de las claves es RSA.

La calidad de los parámetros está garantizada en el módulo criptográfico de la AC raíz, no existiendo acreditación de calidad de los parámetros para las tarjetas criptográficas.

6.1.7. Usos admitidos de las claves

Los usos admitidos de las claves para cada tipo de certificado emitido se definen en las correspondientes Políticas de Certificación.

La ACGISS incluye la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

Las claves privadas de la ACGISS se protegen utilizando hardware criptográfico que cumpla los requisitos establecidos para la especificación técnica FIPS 140-1 Nivel 3 o equivalente.

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

La clave privada de la AC raíz, se encuentra bajo control multipersonal.

Las claves privadas de los certificados están bajo el exclusivo control del titular del mismo.

6.2.3. Repositorio de la clave privada

Las claves privadas de la ACGISS se almacenan en espacios ignífugos y protegidos por controles de acceso físico doble.

6.2.4. Backup de la clave privada

Existe backup de la clave privada de la ACGISS y de los medios necesarios para acceder, en dependencia independiente de aquella donde se almacena habitualmente.

6.2.5. Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la ACGISS quedan almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes (de las que no pueden ser extraídas).

Estas tarjetas son utilizadas para introducir la clave privada en el módulo criptográfico.

6.2.6. Almacenaje de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos.

6.2.7. Método de activación de la clave privada.

La clave privada del suscriptor se activa mediante la introducción del PIN en la correspondiente aplicación de generación de firma.

6.2.8. Método de desactivación de la clave privada

Este punto se desarrollará en la correspondiente Política de Certificación

6.2.9. Método de destrucción de la clave privada

Las claves privadas son destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

6.2.10. Clasificación de los módulos criptográficos

Los módulos de la ACGISS obtienen o superan el nivel EAL 4 de Common Criteria (ISO 15408) con los aumentos que se determinen en la especificación técnica CEN CWA 14167.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

La ACGISS archiva sus claves públicas, de acuerdo con lo establecido en la sección correspondiente de este documento.

6.3.2. Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, y una vez transcurrido no se pueden continuar utilizando.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

La generación de los datos de activación dependerá de cada tipo de certificado, por lo que especificará en la correspondiente Política de Certificación.

6.4.2. Protección de los datos de activación

Se especifica en la Política de certificación de cada certificado

6.4.3. Otros aspectos de los datos de activación

Sin estipulación adicional.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

Se garantiza que el acceso a los sistemas está limitado a individuos debidamente autorizados. En particular:

- La ACGISS garantiza una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como de cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo la gestión de cuentas de usuario, auditoría y modificaciones o denegaciones de acceso oportunas.
- La ACGISS garantiza que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas del Prestador, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema esta restringido y estrechamente controlado.
- El personal de la Entidad está identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal de la Entidad es responsable y tiene que poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- Los sistemas de seguridad y monitorización permiten una rápida detección, registro y actuación ante intentos de acceso irregulares o no autorizados a sus recursos (por ejemplo, mediante un sistema de detección de intrusiones, monitorización y alarma).
- El acceso a los repositorios públicos de la información de la ACGISS (por ejemplo, certificados o información de estado de revocación) cuenta con un control de accesos para modificaciones o borrado de datos.

6.5.2. Evaluación del nivel de seguridad informática

Los procesos de gestión de la seguridad de la infraestructura soporte de la PKI son evaluados por la Gerencia Informática de la Seguridad Social de cara a detectar posibles debilidades, mediante la realización de auditorías internas y el establecimiento de los controles de seguridad necesarios.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizada en las aplicaciones del Prestador de Servicios de Certificación y de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

6.6.2. Controles de gestión de seguridad

La ACGISS mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.
La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección correspondiente de este documento.

Se realiza un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenaje para los activos informativos.

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

Existen controles de seguridad a lo largo del ciclo de vida de los sistemas que tengan impacto en la seguridad de la infraestructura de la PKI.

6.7. Controles de seguridad de red

Se garantiza que el acceso a las diferentes redes de la ACGISS es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles por medio de cortafuegos para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la ACGISS.

- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo los datos de registro del suscriptor).
- Se garantiza que los componentes locales de red (como direccionadores) se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.8. Sellado de tiempo

El sellado de tiempo se realizará a través de la Autoridad de Sellado de Tiempo de la GISS.

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

7.1. Perfil de certificado

Este punto se desarrollará en la correspondiente Política de Certificación.

7.2. Perfil de la lista de revocación de certificados

Este punto se desarrollará en la correspondiente Política de Certificación.

8. AUDITORÍA DE CONFORMIDAD

La ACGISS realizará auditorías periódicas de conformidad para comprobar que cumple, una vez esté en funcionamiento, los requisitos de seguridad y de operación especificados en esta DPC, en las Políticas de Certificación de los certificados y en la legislación aplicable.

La ACGISS podrá delegar la ejecución de las auditorías a empresa que cooperará con su personal para llevar a cabo este proyecto.

8.1. Frecuencia de la auditoría de conformidad

Se deberá realizar una auditoría anual de conformidad de la PKI.

8.2. Identificación y calificación del auditor

La ACGISS dispone de un departamento de auditoría interna, que será el encargado de o bien realizar o bien coordinar la auditoría de conformidad.

Si lo considera oportuno, la ACGISS podrá acudir a un auditor independiente externo, el cual tiene que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Prestadores de Servicios de Certificación y sus elementos relacionados.

8.3. Relación del auditor con la entidad auditada

Las auditorías serán realizadas por el departamento interno de la GISS anteriormente mencionado, aunque se podrá acudir a auditores independientes externos.

8.4. Relación de elementos objeto de auditoría

Los elementos objeto de auditoría serán los siguientes:

- Procesos de Autoridades de Certificación y elementos relacionados.
- Sistemas de información.
- Protección del centro de proceso.
- Documentación relacionada.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a término, la ACGISS discutirá con la entidad que ha ejecutado la auditoría las deficiencias encontradas y desarrollará y ejecutará un plan correctivo que las solucione.

Si la ACGISS auditada es incapaz de desarrollar o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, se realizará una de las siguientes acciones:

- Revocar la clave de la ACGISS, de la forma como se describe en esta DPC.
- Finalizar el servicio de la ACGISS, de la forma como se describe en esta DPC.

8.6. Tratamiento de los informes de auditoría

El equipo de auditor comunicará los resultados de la auditoría a todas las partes interesadas.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. Tarifas

No estipulado.

9.2. Capacidad financiera

9.2.1. Seguro de responsabilidad civil

La ACGISS dispone de una garantía de cobertura de su responsabilidad civil suficiente, en los términos previstos en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre.

9.2.2. Otros activos

Sin estipulación adicional.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por la ACGISS:

- Información de negocio suministrada por sus proveedores y otras personas con las que ACGISS tiene una obligación de guardar secreto, establecida legal o convencionalmente.
- Registros de transacciones, incluyendo los completos y los de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la ACGISS y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como ahora archivo, monitorización y otros de análogos.

9.3.2. Informaciones no confidenciales

Las siguientes informaciones no tienen carácter confidencial:

- La Declaración de Prácticas de Certificación de la ACGISS.
- La política de certificación de los certificados reconocidos emitidos por la ACGISS.
- Toda otra información identificada como “Pública”.

9.3.3. Responsabilidad para la protección de información confidencial

La ACGISS es responsable del establecimiento de las medidas apropiadas de protección de la información confidencial.

Estas medidas incluyen las cláusulas apropiadas de información confidencial en los instrumentos jurídicos con todas las personas.

9.4. Protección de datos personales

9.4.1. Plan de Protección de Datos Personales

La ACGISS desarrolla una política de confidencialidad, de acuerdo con la legislación de protección de datos personales vigentes en España.

Los datos recabados por la ACGISS para la prestación de los servicios de certificación detallados en el presente documento, son incorporados a un fichero registrado en la Agencia de Protección de Datos denominado CERTIFCADOS SILCON.

Este fichero dispone de su correspondiente Documento de Seguridad que se encuentra publicado a disposición de los empleados de la Seguridad Social.

El Prestador de Servicios de Certificación no divulga ni cede estos datos personales, excepto en los casos previstos, así como en la sección 5.8, en caso de finalización del Prestador de Servicios de Certificación.

9.4.2. Información considerada privada

De conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados en todo caso como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas o almacenadas por ACGISS.
- Toda otra información identificada como "Información privada".

La información confidencial de acuerdo con la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

9.4.3. Información no considerada privada

Esta información se trata de información personal que se incluye en los certificados y en el referido mecanismo de comprobación del estado de los certificados.

Dicha información, proporcionada en la solicitud de certificados en los términos que se prevén en el artículo 17.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, es incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados.

La información no tiene carácter privado, por imperativo legal ("datos públicos"), pero sólo se publica en el repositorio si lo consiente el suscriptor.

En todo caso, es considerada no confidencial la siguiente información:

- Los certificados.
- Los certificados emitidos o en trámite de emisión.
- La sujeción del suscriptor a un certificado emitido por la ACGISS.
- El nombre y los apellidos del suscriptor del certificado, así como cualesquiera otras circunstancias o datos personales del titular, en el supuesto que sean significativas en función de la finalidad del certificado, de acuerdo con esta política.
- La dirección electrónica del suscriptor del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.

- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como el resto de informaciones de estado de revocación.
- La información contenida en el Repositorio de la ACGISS.

9.4.4. Responsabilidad correspondiente a la protección de los datos personales

La ACGISS garantiza como mínimo el cumplimento de sus obligaciones legales como Autoridad de Certificación y por tanto responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, en el caso de incumplir, en lo que aquí interesa, las obligaciones contenidas en el artículo 17 de la Ley 59/2003, relativas a la protección de datos personales.

La ACGISS incluye en este documento su procedimiento de notificación, gestión y respuesta ante las incidencias relacionadas con los datos personales.

Este procedimiento contiene un registro en el que se hace constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, la persona a quien se comunica la notificación y los efectos que se derivan.
La ACGISS implanta medidas de identificación y autenticación, así como el necesario control de acceso del personal a los datos personales y de gestión de los soportes de datos personales y de sus backups.

9.4.5. Prestación del consentimiento en el uso de los datos personales

La expedición de certificados personales, obliga a las ACGISS a solicitar el consentimiento expreso a los suscriptores de los certificados, en los procesos de obtención de sus datos personales. La ACGISS pide únicamente los datos necesarios para la expedición y el mantenimiento del certificado, así como para la prestación de otros servicios en relación con la firma electrónica. Estos datos no pueden tratarse con finalidades diferentes sin consentimiento expreso del suscriptor.

La ACGISS informa a los suscriptores de la obtención de sus datos personales.

9.4.6. Divulgación de la información originada por procedimientos administrativos o judiciales

La ACGISS divulga la información confidencial en los casos legalmente previstos para este tema.

En concreto, la ACGISS está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas y en el resto de supuestos previstos en el artículo 11.2 de la LOPD donde así se requiera.

9.4.7. Otros supuestos de divulgación de la información

La ACGISS incluye, en la política de intimidad prevista en este documento, prescripciones para permitir la divulgación de la información del suscriptor, directamente a los mismos o a terceros.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

La ACGISS y las Entidades Gestoras y Servicios Comunes son las únicas entidades que disfrutan de los derechos de propiedad intelectual sobre los certificados que emita.

9.5.2. Propiedad de las políticas de certificación y Declaración de Prácticas de Certificación

La ACGISS y las Entidades Gestoras y Servicios Comunes son las únicas entidades que disfrutan de los derechos de propiedad intelectual sobre la Declaración de Prácticas de Certificación de sus correspondientes Políticas de Certificación.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor, conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (Distinguished Name) del certificado, sin perjuicio del derecho de terceros.

9.5.4. Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados. Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. Autoridad de Certificación ACGISS

La ACGISS responderá por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone la ley 59/2003, en los términos de su artículo 22.

De manera particular, responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

También asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

9.6.2. Entidades de Registro

9.6.2.1. Obligaciones y otros compromisos

La ACGISS puede delegar algunas funciones a Entidades de Registro, quien será responsable en el ámbito de las funciones atribuidas por la AC.

La Entidad de Registro queda obligada a registrar los datos del certificado y su aprobación en caso de ser correctos, así como al registro de los datos de este certificado, por el que realiza las comprobaciones que considere necesarias al respecto de la identidad y el resto de datos personales y complementarios de los suscriptores, y si fuera necesario, de los poseedores de claves.

Si la Entidad de Registro detectase errores en los datos que son incluidos en los certificados, o en los documentos que justificasen estos datos, está obligada a realizar los cambios que considere necesarios antes de la emisión del certificado, o a la paralización del proceso de emisión y a gestionar con el suscriptor la incidencia correspondiente.
En el caso que la Entidad de Registro corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, queda obligada a notificar los datos que finalmente se certifiquen al suscriptor en el momento de la entrega.
La Entidad de Registro se reserva el derecho a no aprobar la solicitud de emisión del certificado, cuando la justificación documental aportada por el solicitante sea insuficiente para la correcta identificación y/o autenticación del suscriptor.

9.6.3. Suscriptores

En general, la ACGISS obliga al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

9.6.4. Verificadores

No estipulado.

9.7. Renuncias de garantías

No estipulado.

9.8. Limitaciones de responsabilidad

9.8.1. Limitaciones de responsabilidad del Prestador de Servicios de Certificación

La ACGISS limita su responsabilidad en los términos del artículo 23 de la Ley 59/2003.

En particular, no es responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el suscriptor incurre en alguno de los siguientes supuestos:

- No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.
- La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.
- Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el la ACGISS le notifique la extinción o suspensión de su vigencia.
- Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

9.8.2. Caso fortuito y fuerza mayor

No estipulado.

9.9. Indemnizaciones

No estipulado.

9.10. Plazo y finalización

9.10.1. Plazo

La DPC y las Políticas de Certificado específicas entrarán en vigor desde el momento de su aprobación por la GISS y su publicación en la página Web de la Seguridad Social, y permanecerán vigentes hasta la aprobación de una nueva versión de las mismas.

9.10.2. Finalización

La DPC y las Políticas de Certificado serán sustituidas por las nuevas versiones que se aprueben.

9.10.3. Supervivencia

Las obligaciones y restricciones que establecen esta DPC y las correspondientes Políticas de Certificado, subsistirán tras su sustitución por una nueva versión en todo lo que no se oponga a ésta.

9.11. Notificaciones

La ACGISS establece, en sus instrumentos jurídicos vinculantes con los suscriptores, cláusulas de notificación.

En virtud de la cláusula de notificación se establece el procedimiento por el que las partes se notifiquen hechos mutuamente.

9.12. Modificaciones de la DPC

9.12.1. Procedimiento para las modificaciones

La ACGISS puede modificar, de forma unilateral, este documento, siempre que proceda según el siguiente procedimiento:

- La modificación tiene que estar justificada desde el punto de vista técnico, legal o comercial.
- La modificación propuesta por la ACGISS no puede ir en contra de las políticas de certificación establecidas por ella.
- Se establece un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplan los requisitos que se intentan cumplir y que dieron pie al cambio.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones.
- La nueva política tiene que ser aprobada por ACGISS.

9.12.2. Periodo y mecanismos para notificaciones

Las modificaciones de este documento se notifican a ACGISS, para su posterior aprobación.

9.12.3. Circunstancias en las que un OID tiene que ser cambiado

No estipulado.

9.13. Resolución de conflictos

9.13.1. Resolución extrajudicial de conflictos

La ACGISS establece, en sus instrumentos jurídicos con los suscriptores, los procedimientos de mediación y resolución de conflictos aplicables, tanto en vía administrativa como judicial, y se atiene a los procedimientos generales establecidos para la Administración Pública.

9.13.2. Jurisdicción competente

La jurisdicción competente será la correspondiente a la resolución de conflictos en las Administraciones Públicas.

9.14. Legislación aplicable

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

9.15. Conformidad con la legislación aplicable

La ACGISS manifiesta su conformidad con la legislación mencionada en el apartado anterior.

9.16. Cláusulas diversas

No estipulado.