MINISTERIO
DE TRABAJO, MIGRACIONES
Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

Gerencia de Informática
de la Seguridad Social

Declaración de Prácticas de Certificación

Autoridad de Certificación de la Gerencia de Informática de la Seguridad Social (ACGISS)

V 2.0.3
(Agosto 2018)

Gerencia de Informática de
la Seguridad Social
c/ Doctor Tolosa Latour s/n
28041 Madrid

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
2.0	Revisión completa por actualización de la PKI para su adaptación al Reglamento eIDAS	20-06-2016
2.0.1	Revisión: corrección de erratas y aclaraciones de redacción	22-02-2017
2.0.2	Revisiones de redacción.	31-05-2017
2.0.3	Cambios debidos a revisión anual interna, adaptación al RGPD y recomendaciones de auditoría eIDAS	03-08-2018

Índice

1. INTRODUCCIÓN

1.1. Presentación

La Gerencia de Informática de la Seguridad Social (en adelante GISS) es un Servicio Común con nivel orgánico de subdirección general, adscrito a la Secretaría de Estado de la Seguridad Social. Como parte de sus funciones proporciona servicios informáticos 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 (Autoridad de Certificación de la Gerencia de Informática de la Seguridad Social) que expide certificados electrónicos y proporciona diversos servicios de confianza.

La Infraestructura de Clave Pública (PKI) de la GISS ha sido diseñada y es gestionada teniendo en cuenta los requisitos establecidos en el Reglamento (UE) nº 910/2014 del Parlamento Europeo, y es conforme con la Ley 59/2003 de Firma Electrónica.

Esta declaración describe las características de los servicios prestados por ACGISS como Autoridad de Certificación, así como las prácticas y procedimientos utilizados para la prestación de dichos servicios.

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

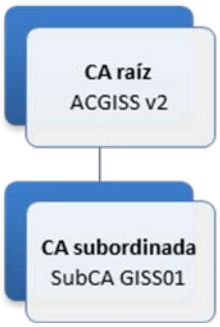
1.2. Identificación del documento

Nombre del documento	ACGISS. Declaración de Prácticas de Certificación
Versión	2.0.3
Estado del documento	Aprobado
Fecha de emisión	3 de agosto de 2018
OID ACGISS	2.16.724.1.4.2.2
Localización	http://www.seg-social.es/ACGISS

Significado de OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) ACGISSv2 (2)

1.3. Participantes de la PKI

1.3.1. Jerarquía de Autoridades de Certificación



A nivel jerárquico la arquitectura general de la PKI se compone de:

- Una Autoridad de Certificación raíz que constituye el punto de confianza de todo el sistema y que garantiza en última instancia la identidad del prestador. Es la encargada de expedir los certificados para las AC subordinadas que se creen.
- Una Autoridad de Certificación subordinada que se encargará de la emisión de los distintos certificados.

En adelante se utilizará indistintamente AC o CA para referirse a las Autoridades de Certificación (o Certification Authorities).

La jerarquía anterior permite distribuir riesgos permitiendo que la AC subordinada gestione las claves en un entorno on-line ágil, protegiendo a su vez la clave de la AC raíz en un entorno seguro desconectado.

1.3.1.1. Autoridad de certificación raíz ACGISS v2

Los datos fundamentales de la AC raíz son los siguientes:

Subject	CN = RAIZ ACGISSv2 SERIALNUMBER = Q2827003A OU = GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL O = TESORERIA GENERAL DE LA SEGURIDAD SOCIAL L = MADRID C = ES
OID	2.16.724.1.4.2.2
Número de Serie	57 62 68 ed
Período de validez	Desde jueves, 16 de junio de 2016 10:23:07 Hasta lunes, 16 de junio de 2036 10:53:07
Huella (SHA-1)	90 5d 3a 6f b1 49 64 b9 da cf 41 91 a4 1a 0c 0b 6a 2a 02 57
Longitud de clave	4096
Algoritmo de firma	SHA256RSA

1.3.1.2. Autoridades de certificación subordinadas

Las AC subordinadas son autoridades intermedias que expiden certificados electrónicos a los usuarios finales. Actualmente existe una única AC Subordinada denominada SubCA GISS01 que emite todos los certificados finales de ACGISS.

Subject	CN = SUBCA GISS01 SERIALNUMBER = Q2827003A OU = GISS01 OU = GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL O = TESORERIA GENERAL DE LA SEGURIDAD SOCIAL L = MADRID C = ES
OID	2.16.724.1.4.2.2.1
Número de Serie	57 62 69 40
Período de validez	Desde jueves, 16 de junio de 2016 11:51:17 Hasta lunes, 16 de junio de 2031 12:21:17
Huella (SHA-1)	b4 9c 4d ff bb 41 dc 34 8b 1a 97 05 78 5e 59 4d db 9a 9a 45
Longitud de clave	4096
Algoritmo de firma	SHA256RSA

1.3.2. Autoridades de Registro

Las Autoridades 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. Realizan la tramitación de las solicitudes de certificados y facilitan a los usuarios la información mínima necesaria.

Actuarán como Autoridades 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. Suscriptores y usuarios finales

Los usuarios finales (o titulares de los certificados) son las entidades que utilizan certificados emitidos por la Seguridad Social.

Al tratarse de una PKI que emite certificados para el desempeño de las funciones propias de Seguridad Social, los usuarios finales serán de forma general usuarios internos de la Secretaría de Estado de la Seguridad Social o colaboradores de la misma.

El suscriptor de los certificados será la Entidad que solicita la emisión de un certificado para el titular y puede coincidir o no con éste.

En cada Política específica se establecerá la lista concreta de suscriptores y usuarios finales a los que se destinan los diferentes tipos de certificados.

1.3.4. Terceras partes de confianza

Las terceras partes de confianza son aquellas que confían en los certificados emitidos por ACGISS.

1.3.5. 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 realiza una operación o transacción por medios electrónicos, con objeto de demostrar que una serie de datos han existido y no se han modificado desde ese momento.

  Este componente es un servicio gestionado por la Gerencia Informática de la Seguridad Social.

1.4. Uso de los certificados

1.4.1. Tipos y clases de certificados emitidos

La ACGISS emite diferentes tipos de certificados organizados fundamentalmente en tres grupos:

- Certificados de Actuación Automatizada: destinados a su uso por servidores y aplicaciones de la Seguridad Social.
- Certificados Personales: destinados al personal que presta servicios en el ámbito de la Secretaría de Estado de la Seguridad Social.
- Certificados asociados a Servicios de Confianza: relacionados con otros servicios de confianza proporcionados por el prestador, tales como los servicios de validación o sellado de tiempo.

Como caso particular, ACGISS emite certificados de Administración Pública, conformes con las normas aprobadas en la Administración General del Estado (AGE):

- Certificados de Empleado Público. Emitidos a empleados públicos (personal funcionario, laboral y eventual) de la Seguridad Social con propósito de identificación, firma electrónica 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 Sello Electrónico. Emitidos a organismos de la Seguridad Social con propósito de identificación y firma de documentos administrativos en el ámbito de sus funciones.

El resto de certificados emitidos se utilizan fundamentalmente en el ámbito interno de la Seguridad 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.

1.4.2. Uso de los certificados

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

1.4.2.1. 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 empleados. Los correspondientes a Administración Pública 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.

1.4.2.2. 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.

Los certificados emitidos con finalidad de prueba y especificados como tales en su nombre distintivo, no podrán utilizarse en ningún caso para los usos habituales establecidos.

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

1.5. Administración de la Normativa de Certificación

1.5.1. Especial referencia a la arquitectura anterior

Esta DPC se refiere a la Autoridad de Certificación de la GISS en su versión 2 (ACGISS v2).

La documentación relativa a la arquitectura anterior y a los certificados emitidos por ella, puede encontrarse en la página web del prestador. En el caso de la DPC, se aplicarían las condiciones establecidas hasta la versión 1.2. inclusive.

1.5.2. Organización de políticas y prácticas

La Normativa General de Certificación de la GISS se compone de las distintas Políticas de Certificación específicas definidas para cada certificado y de la Declaración de Prácticas de Certificación.

Este documento contiene la Declaración de Prácticas de Certificación (DPC) de la GISS como Prestador de Servicios de Confianza. Las políticas y prácticas generales establecidas en este documento son heredadas directamente por la AC subordinada existente.

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. En concreto incorpora los controles de seguridad física y técnica y las características

comerciales y legales del prestador, así como las disposiciones generales relativas a la gestión del ciclo de vida de los certificados.

Cada uno de los certificados que emita tendrá su correspondiente Política de Certificación que incluirá particularmente el método específico de identificación y autenticación, y los requisitos aplicables para su emisión, utilización y revocación.

1.5.3. Datos de contacto de la organización

Nombre	Gerencia de Informática de la Seguridad Social		
Dirección e-mail	acgiss.soporte.giss@seg-social.es		
Dirección	C/ Doctor Tolosa Latour s/n, 28041 Madrid		
Teléfono	91 390 27 03	**Fax**	91 460 40 72

1.5.4. Datos de contacto de la unidad responsable dentro de la organización

Nombre	Dirección de Seguridad, Innovación y Proyectos (Gerencia de Informática de la Seguridad Social)		
Dirección e-mail	acgiss.soporte.giss@seg-social.es buzon.giss-sscc.dsip@seg-social.es		
Dirección	c/ Doctor Tolosa Latour s/n, 28041 Madrid		
Teléfono	91 390 27 18	**Fax**	91 390 51 67

1.5.5. Procedimiento de aprobación

La DPC y las Políticas de Certificación están sometidas a un proceso de aprobación y revisión de acuerdo con los procedimientos internos establecidos al efecto.

1.6. Definiciones y acrónimos

1.6.1. Definiciones

Activación: es el procedimiento por el cual se desbloquean las condiciones de acceso a una 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: un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.

Certificado de firma electrónica (o certificado electrónico a efectos de esta DPC):una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.

Certificado cualificado de firma electrónica (o certificado electrónico cualificado a efectos de esta DPC): un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento UE nº 910/2014.

Certificado de Sello electrónico: una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona.

Certificado cualificado de sello electrónico: un certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento UE nº 910/2014.

Claves (pública y privada): son claves generadas por el prestador de servicios de confianza, denominadas habitualmente datos de creación de firma (clave privada) y datos de verificación de firma (clave pública). Están vinculadas entre sí de forma única y pertenecen a una determinada persona o entidad.

Dispositivo de creación de firma electrónica: un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

Dispositivo cualificado de creación de firma electrónica: un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento UE nº 910/2014.

Dispositivo de creación de sello electrónico: un equipo o programa informático configurado que se utiliza para crear un sello electrónico.

Dispositivo cualificado de creación de sello electrónico: un dispositivo de creación de sellos electrónicos que cumple mutatis mutandis los requisitos enumerados en el anexo II del Reglamento UE nº 910/2014.

Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento UE nº 910/2014.

Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

Hash, huella o resumen: Es una operación matemática que se realiza sobre un conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. Es un método para generar claves que representen de manera unívoca a un documento o conjunto de datos.

Identificación electrónica: el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

Infraestructura de clave pública (PKI): es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Listas de Revocación de Certificados o Listas de Certificados Revocados (CRLs): lista donde figuran las relaciones de certificados revocados o suspendidos.

Medios de identificación electrónica: una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.

Módulo de Seguridad Hardware (HSM): es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas con un alto nivel de seguridad y suele aportar aceleración hardware para operaciones criptográficas.

OID: es una secuencia de números que se asignan jerárquicamente y permite identificar objetos en la red y que se registran en agencias especializadas. En el ámbito de un prestador de servicios de confianza se utilizan fundamentalmente para identificar de forma única las políticas y prácticas de certificación, así como diversos campos de los certificados.

Prestador de Servicios de Confianza: una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas.

Prestador Cualificado de Servicios de Confianza: un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación

Sello electrónico: datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

Sello electrónico avanzado: un sello electrónico que cumple los requisitos contemplados en el artículo 36 del Reglamento UE nº 910/2014.

Sello electrónico cualificado: un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

Sello de tiempo electrónico: datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

Sello cualificado de tiempo electrónico: un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 del Reglamento UE nº 910/2014.

Servicio de confianza: el servicio electrónico consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;

Servicio de confianza cualificado: un servicio de confianza que cumple los requisitos aplicables establecidos en el Reglamento UE nº 910/2014.

Validación: el proceso de verificar y confirmar la validez de una firma o sello electrónicos.

1.6.2. Acrónimos

AC	Autoridad de Certificación (CA – Certification Authority)
ARL	Lista de Revocación de Autoridades de Certificación
AV	Autoridad de Validación (VA – Validation Authority)
ACGISS	Autoridad de Certificación de la Gerencia de Informática de la Seguridad Social
CEN	Comité Europeo de Normalización
CN	Common Name (Nombre común. Atributo del DN de un objeto)
CRL	Certificate Revocation List (Lista de Certificados Revocados)
CWA	CEN Workshop Agreement
DCCF	Dispositivo cualificado de creación de firma electrónica
DCCS	Dispositivo cualificado de creación de sello electrónico
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
LAECSP	Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007)
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	Secure Hash Algorithm
SSL	Secure Socket Layer
SUBCA	Autoridad de Certificación Subordinada
TSL	Transport Layer Security

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. Repositorios

La GISS dispone de un repositorio de información pública en la página http://www.seg-social.es/ACGISS disponible durante las 24 horas de los 7 días de la semana.

2.2. Publicación de información de la ACGISS

La ACGISS proporciona acceso público a las siguientes informaciones:

- Los certificados emitidos por ACGISS que constituyen la cadena de confianza de la PKI.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La normativa general de certificación, compuesta por la presente DPC y las Políticas de Certificación de los diferentes certificados cualificados emitidos.
- Cualquier otra información relativa a los servicios ofrecidos que se considere de interés para las terceras partes de confianza.

Todo cambio en las especificaciones o condiciones del servicio se comunicará a los usuarios 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.

ACGISS mantiene un histórico de las versiones publicadas, de forma que se puedan consultar los documentos con posterioridad al cambio de versión.

2.3. Frecuencia de publicación

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

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en este documento.

Los cambios en este documento se rigen por lo establecido en las secciones correspondiente. Al cabo de 15 días desde la publicación de la nueva versión, se podrá retirar la referencia al cambio de la página principal del prestador. Las versiones antiguas de la documentación son conservadas al menos durante 15 años por la ACGISS para su consulta por los interesados.

2.4. Control de acceso

La ACGISS no limita el acceso de lectura a las informaciones establecidas en la sección pública correspondiente, pero establece controles para mantener la protección de la integridad y autenticidad de la información publicada.

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 autorice.
- Se detecta cualquier cambio técnico que afecte a los requisitos de seguridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Gestión de nombres

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).

De forma general, se incluye en los certificados la siguiente información:

- C - *Country*: ES (corresponde al código ISO de país, correspondiente al Estado Español).
- O – *Organization*: La organización suscriptora del certificado.
- OU –*Organizational Unit Name*: El nombre del tipo de certificado de que se trata.
- SN – *Serial Number*: NIF/CIF del suscriptor y/o titular del certificado.
- CN –*Common Name*: El nombre en texto libre del suscriptor y/o titular.

En el caso de certificados cualificados emitidos a personas físicas se incluirá además:

- *Surname*: Apellidos del titular
- *Given Name*: Nombre del titular

Asimismo se permitirá utilizar campos adicionales que faciliten la gestión e identificación de los distintos certificados y que serán descritos en la correspondiente Política de Certificación.

Adicionalmente se utiliza en ocasiones el campo *Subject Alternative Name* para incluir información que pueda utilizarse para la identificación del usuario y para facilitar la interoperabilidad en dicha identificación para el caso de certificados de Administración Pública.

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.

Los valores de los campos se corresponderán con la información oficial de las entidades y usuarios suscriptores de los certificados, tal como aparece registrada en las bases de datos de la Seguridad Social.

3.1.3. Utilización de anónimos y seudónimos

No se permitirá la utilización de anónimos ni seudónimos.

3.1.4. Interpretación de formatos de nombres

Las reglas utilizadas para interpretar los nombres distintivos de los certificados se encuentran en los estándares ISO/IEC 9594– ITU-T X.500, así como la parte aplicable del estándar ETSI EN 319 412.

3.1.5. Unicidad de los nombres

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

No se podrá volver a asignar un DN a un certificado que ya haya sido utilizado por otro.

3.1.6. Resolución de conflictos relativos a nombres

Dado que se utiliza la información oficial de las entidades y usuarios presente en las bases de datos de la Seguridad Social, y teniendo en cuenta la garantía existente en cuanto a la unicidad de los nombres, no se contemplan en principio conflictos relativos a los nombres empleados en los certificados.

No obstante lo anterior, de presentarse conflictos relativos a los nombres su resolución 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

Las claves privadas de la AC raíz y de la AC subordinada se generan de forma segura en el interior de un Módulo de Seguridad Hardware (HSM), que proporciona adicionalmente mecanismos de protección de las claves para evitar su salida del mismo.

En cuanto a los certificados finales, 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

Los suscriptores/titulares son usuarios internos a la organización, disponiéndose ya de su dirección física y otros medios de contacto.

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

La información utilizada para la identificación de los titulares en los certificados se basa en los mecanismos de identificación oficiales en España y su inclusión en los certificados se hace de acuerdo con los estándares internacionales aplicables, lo que garantiza la interoperabilidad con terceros.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

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

4. REQUISITOS OPERACIONALES DEL 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, el proceso de registro y las responsabilidades concretas se establecerán en la Política específica de cada tipo de certificado.

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 y las herramientas tecnológicas existentes en la GISS.

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.

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

En todo caso 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 las medidas oportunas contra la falsificación de certificados.

4.3.2. Notificación de la emisión al suscriptor/titular

ACGISS notifica al suscriptor/titular la emisión del certificado por distintos medios, en función del tipo de certificado, por lo que este extremo se recogerá también en la Política de Certificación específica.

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.

4.4.2. Publicación del certificado

La publicación se realiza a nivel interno en la Seguridad Social.

4.4.3. Notificación de la emisión a terceros

La GISS notificará la emisión de aquellos certificados utilizados en servicios y comunicaciones con sistemas de terceros cuando sea necesario para la interoperabilidad y para la autorización de las transacciones.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por los suscriptores del par de claves

Los suscriptores o titulares podrán utilizar las claves y los certificados para los usos autorizados en la presente DPC y en las correspondientes PC. Este uso debe cesar tras la extinción de la vigencia o la revocación del certificado del titular.

En todo caso se atenderá a lo establecido en la presente DPC en relación con el uso de los certificados y las obligaciones de los suscriptores/titulares.

Se distinguen las siguientes finalidades de los certificados emitidos por la PKI:

- Autenticación: Permite garantizar la identidad del usuario.
- Firma electrónica: Permite la firma electrónica de documentos y garantizar su integridad.
- Cifrado: Se utilizará para garantizar la confidencialidad de los documentos electrónicos.

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 PC.

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 emisión de uno nuevo.

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 o renovación 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.
- Renovación por cambios en la infraestructura o en las políticas de certificación, por ejemplo por modificaciones en los perfiles definidos.

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, siempre que se produzca alguna de las circunstancias descritas en el apartado anterior.

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/titular

La ACGISS notifica la emisión del certificado al suscriptor/titular por distintos medios según el tipo de certificado, por lo que este extremo se describirá en la correspondiente Política.

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

La publicación de los certificados se realiza a nivel interno en la Seguridad Social.

4.7.7. Notificación de la emisión a otras entidades

La GISS notificará la emisión de aquellos certificados utilizados en servicios y comunicaciones con sistemas de terceros cuando sea necesario para la interoperabilidad y para la autorización de las transacciones.

4.8. Modificación de certificados

No se permitirá la modificación de los certificados emitidos. Cualquier modificación implicará la emisión de un nuevo certificado.

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, un tercero autorizado o la persona física representante del titular.
- Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de confianza, o utilización indebida de dichos datos por un tercero.
- Resolución judicial o administrativa que lo ordene.
- Extinción de la personalidad jurídica del firmante 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 confianza salvo que la gestión de los certificados electrónicos expedidos por aquél sea transferida a otro prestador.
- Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, 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 o el titular a nombre del que el certificado fue emitido.
- La Autoridad 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 se atiende de forma inmediata y será procesada en el mínimo plazo posible según cada tipo de 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 CA Raíz emite una Lista de CAs Revocadas (ARL - http://crl.seg-social.gob.es/arl.crl), como mínimo una vez al año y teniendo en cuenta la periodicidad establecida en la propia ARL, o extraordinariamente, cuando se produzca la revocación de un certificado de autoridad.

La CA Subordinada emite una CRL al menos cada 24 horas y de forma inmediata cuando se produce la revocación de alguno de los certificados emitidos. 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 se renuevan como máximo cada 24 horas y se publican de forma razonablemente inmediata tras su generación debido a una revocación, teniendo en cuenta las especificaciones técnicas de los sistemas utilizados.

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 vía OCSP (http://ocsp.seg-social.gob.es/) 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 GISS protege los sistemas asociados a la validación del estado de los certificados con las medidas de seguridad organizativas y técnicas descritas en este documento con el fin de garantizar la validez y la disponibilidad de la información proporcionada. Adicionalmente garantiza la autenticidad e integridad de dicha información mediante la firma de las respuestas OCSP y las CRLs facilitadas a terceros.

La información del estado de revocación está disponible más allá del período de validez de los certificados. También estará disponible tras el cese del prestador de acuerdo con lo previsto en el correspondiente plan de terminación.

4.9.10. Requisitos de comprobación online de la revocación

Para la comprobación online del estado de los certificados se utilizará preferentemente el servicio OCSP, para lo que se deberá disponer de un software capaz de operar con dicho protocolo.

Asimismo se proporciona un mecanismo de consulta pública de CRLs mediante HTTP.

4.9.11. Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.9.12. Requerimientos especiales en caso de compromiso de las claves privadas

En caso de compromiso de las claves privadas se actuará conforme a lo establecido en este documento.

Tras el compromiso, se revoca el certificado y se discontinúa el uso de la clave privada del sujeto de manera inmediata y permanente.

4.9.13. Condiciones relativas a la suspensión de certificados

No estipulado.

4.10. Servicios de comprobación del estado de los certificados

La comprobación del estado de los certificados se podrá realizar por dos métodos diferentes: vía OCSP o mediante descarga de las CRLs.

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 y ofrece una respuesta vía HTTP.

Las CRLs se facilitan con la periodicidad establecida en este documento mediante protocolo 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. Para ello los sistemas involucrados en la prestación del servicio así como la

información relativa al estado de los certificados se encuentran replicados en un centro de respaldo que permite garantizar la continuidad de los servicios de validación.

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

La custodia y recuperación de claves se realizarán con las medidas de seguridad especificadas en este documento y en la correspondiente Política de Certificación.

5. CONTROLES DE SEGURIDAD FÍSICA, GESTIÓN Y OPERACIONES

5.1. Controles de seguridad física

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

Para ello establece controles en sus dependencias relativas a:

- Ubicación física de las instalaciones y condiciones específicas de la edificación.
- Acceso físico del personal autorizado.
- Medidas de protección relativas a la alimentación eléctrica y condiciones térmicas de los equipos.
- Medidas de protección frente a inundaciones e incendios.
- Condiciones de seguridad del almacenamiento.
- Procedimientos de eliminación de soportes de información.
- Configuración del respaldo fuera de las instalaciones.

5.1.1. Localización y construcción de las instalaciones

La GISS se encuentra ubicada en un perímetro protegido que garantiza la seguridad de las operaciones realizadas en los edificios comprendidos en él. Concretamente dispone de:

- Control de acceso físico al perímetro en el que están ubicadas sus instalaciones.
- Circuito cerrado de vigilancia en todo el perímetro, incluyendo las áreas de acceso restringido.
- Control de acceso a edificios y zonas protegidas.
- Protección de sistemas críticos en áreas dedicadas y con controles de seguridad adicionales.
- Sistemas de protección ante desastres y accidentes conformes a la legislación vigente.

5.1.2. Acceso físico

El Prestador establece adecuados niveles de seguridad de acceso a los edificios y diferentes perímetros.

Las instalaciones están protegidas dentro de un perímetro de seguridad con barreras arquitectónicas y de seguridad suficientes para detectar accesos no autorizados. Se cuenta con personal propio dedicado al control de acceso a las dependencias de la GISS.

El acceso a los edificios por parte del personal se realiza mediante tarjetas criptográficas o mediante identificación por personal de seguridad. Se requiere que todo el personal porte estas tarjetas en lugar visible a modo de identificación.

Se dispone de un sistema de control de autorizaciones, junto con procedimientos asociados, que garantizan que el acceso sólo está permitido a personal autorizado. El personal ajeno a la GISS se encuentra continuamente supervisado mientras trabaja en sus instalaciones.

Todos los accesos son registrados y filmados por circuito cerrado de vigilancia.

Adicionalmente, los sistemas involucrados en la emisión de certificados, en concreto las CAs y los módulos criptográficos que contienen las claves privadas, se encuentran ubicados en una localización aislada protegida con control de acceso físico independiente para las personas autorizadas.

5.1.3. Electricidad y aire acondicionado

Los equipos informáticos de la GISS 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 suministro 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 garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

5.1.4. Exposición al agua

La GISS dispone de las medidas de detección adecuadas para prevenir la exposición al agua de los equipos y el cableado.

5.1.5. Protección y prevención de incendios

Todas las instalaciones y activos de la GISS cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6. Almacenamiento y backup

El almacenamiento de información se realiza de forma que se garantice tanto su integridad como su confidencialidad, en caso de que así lo requiera, y cumpliendo los requisitos mínimos establecidos por la legislación de protección de carácter personal vigente.

Los datos almacenados se encuentran protegidos ante accesos no autorizados y disponen de las medidas de seguridad física especificadas en este documento.

5.1.7. Eliminación de soportes de información

La destrucción de soportes se realiza de acuerdo a los procedimientos internos de la GISS.

En caso de que contengan información confidencial, la eliminación de soportes se realiza mediante métodos seguros de acuerdo con la legislación vigente en materia de seguridad de la información y protección de datos de carácter personal.

5.1.8. Backup fuera de las instalaciones

La GISS dispone de un centro de respaldo remoto en el que se replica la infraestructura y la información básica utilizada en los procesos de la PKI. Este centro dispone también de las adecuadas medidas de seguridad.

5.2. Controles de procedimientos

La GISS garantiza que sus sistemas se operan de forma segura y establece procedimientos para las funciones que afecten a la provisión de sus servicios.

El personal al servicio de la ACGISS realiza las actuaciones definidas en los procedimientos y la gestión de la infraestructura de acuerdo con la política de seguridad de la GISS.

5.2.1. Principales perfiles

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

- Administradores de sistemas: 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 y la realización de auditorías de conformidad.
- Responsables de seguridad: Usuarios responsables de la definición, verificación, administración e implementación de las políticas, normas y procedimientos de seguridad.

- Responsables de registro: Responsables de llevar a cabo las tareas relacionadas con la identificación y autenticación de los solicitantes de los certificados, así como de la solicitud en su nombre de la emisión/revocación de los mismos.
- Operadores de sistemas: Usuarios encargados de realizar las tareas básicas relativas a los sistemas involucrados en la PKI, incluyendo los procesos de backup y recuperación.
- Custodios criptográficos: Responsables de la custodia del material criptográfico de la PKI.

5.2.2. Número de personas por tarea

Las funciones básicas de la PKI de la ACGISS están soportadas por más de una persona, dentro de un plan que garantiza una disponibilidad inmediata en caso de contingencia grave en sus instalaciones.

5.2.3. Identificación y autenticación para cada función

La GISS tiene implantados diversos sistemas de autenticación y autorización, tanto a nivel físico como lógico, de forma que se controle el acceso a los sistemas y los datos del prestador a las personas autorizadas para cada función.

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 de una persona, en ocasiones de departamentos diferentes, para minimizar el riesgo de actuaciones ilegítimas.

En concreto, los diferentes perfiles involucrados en la gestión de la PKI, definidos en el apartado 5.2.1, están desempeñados por personas y/o unidades diferentes dentro de la GISS.

5.3. Controles de personal

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

- Se selecciona al personal involucrado en la gestión de la PKI mediante procedimientos bien definidos y de acuerdo a su conocimiento y experiencia.
- Se garantiza la adecuada formación del personal, así como la disponibilidad de la documentación requerida para el desempeño de sus funciones.
- El personal involucrado debe respetar las políticas de uso de sistemas de información de la GISS y demás normativa interna aprobada en materia de seguridad de la información.
- Existen mecanismos de exigencia de responsabilidad en caso de incumplir las normas establecidas.
- Se utilizan mecanismos de contratación sujetos a la normativa aplicable a las entidades de derecho público, con requisitos y garantías específicas en caso de incumplimiento de las condiciones pactadas.
- Se asegura la inexistencia de conflictos de intereses en el personal de la organización que tenga roles de confianza.

- El personal es formalmente nombrado para funciones de confianza por la dirección de seguridad, requiriendo siempre el principio de "privilegio mínimo" al acceder o configurar los privilegios de acceso.

Todos los controles de personal especificados en este documento se entenderán aplicables también al personal de empresas externas contratado que interviene en la administración y operación de estos sistemas.

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

El personal propio que trabaja en la ACGISS supera un proceso específico de selección y pertenece a cuerpos especializados en el desarrollo y operación de los sistemas informáticos.

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

Todo el personal tiene establecidas sus funciones y dispone de los medios y autorizaciones acordes a dichas funciones.

5.3.2. Procedimientos de investigación de historial

El personal propio debe cumplir los requisitos establecidos en la legislación para el acceso a la Administración.

En caso de contratación externa, se aplican los procedimientos establecidos internamente al efecto y en la legislación sobre contratación en la Administración Pública.

5.3.3. Requisitos de formación

La GISS se ocupa de formar a su personal y de solicitar formación para el personal contratado, con el fin de lograr la cualificación y los conocimientos adecuados de todos los involucrados en los procedimientos de la PKI.

5.3.4. Requisitos y frecuencia de actualización formativa

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

5.3.5. Secuencia y frecuencia de rotación de personal

No estipulado.

5.3.6. Sanciones por acciones no autorizadas

La Seguridad Social, en su condición de Entidad de derecho público, está sometida a un régimen disciplinario para todo su personal. 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.

5.3.7. Requisitos de contratación de profesionales

El Prestador contrata profesionales cualificados para la ejecución efectiva de las funciones propias de la PKI.

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

5.3.8. Suministro de documentación al personal

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

En particular, existen manuales de operación y administración de los principales componentes a disposición de los roles de confianza de la PKI.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

La ACGISS guarda registro de los eventos de seguridad más significativos relacionados con la PKI, incluidos los cambios relacionados con la política de seguridad, arranque y apagado del sistema, fallos del sistema y fallos de hardware, actividades de firewall y routers e intentos de acceso al sistema de PKI.

Específicamente, se generan los relativos al ciclo de vida de los certificados y a las principales operaciones de administración de los sistemas de la PKI:

- Rastros de operación de los componentes SW y HW integrantes de la PKI.
- Datos relativos a la emisión, renovación y revocación de certificados.

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 quedarán también registradas.

5.4.3. Periodo de conservación de registros de auditoría

Los registros de auditoría se tratan de acuerdo a los procedimientos de auditoría y de comprobación de rastros de la GISS.

La información relativa a la emisión, renovación y revocación de certificados es archivada y se mantiene al menos durante 15 años.

5.4.4. Protección de los registros de auditoría

Los ficheros de los registros se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico. Estos accesos sólo podrán realizarse por personal específicamente designado al efecto.

5.4.5. Procedimientos de backup de registros de auditoría

Los backups se realizan de forma automática de acuerdo con la política de copias de seguridad establecida en la GISS.

5.4.6. Recolección y almacenamiento de registros de auditoría

El sistema de almacenamiento de registros de auditoría, ubicado internamente en la GISS, está compuesto por varios registros de aplicación, red y sistema, además de los datos manualmente generados, almacenados por el personal debidamente autorizado. La gestión de este sistema en su conjunto se realiza de acuerdo a los procedimientos internos de la GISS.

5.4.7. Notificación del evento al causante

No está contemplada una notificación automática del evento al origen del mismo.

5.4.8. Análisis de vulnerabilidades

La GISS dispone de sistemas y servicios de análisis de vulnerabilidades generales en sus sistemas.

Se sigue una metodología específica de análisis de riesgos, según la cual se realiza un análisis de riesgos que se revisa periódicamente, y se elabora un plan de tratamiento para mitigar los riesgos detectados.

De igual modo, se realizan evaluaciones de riesgos con el fin de estimar las necesidades de la organización y determinar los requisitos de seguridad que deben incluirse en la política de certificación.

Adicionalmente, se podrán realizar análisis de vulnerabilidades específicos en caso de sospecha en las operaciones de la PKI.

Cualquier vulnerabilidad crítica es corregida dentro de un plazo de 48 horas desde su detección.

5.5. Archivo de informaciones

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

5.5.1. Tipos de informaciones archivadas

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

5.5.2. Periodo de conservación del archivo

Los certificados, los contratos con los firmantes, las políticas y prácticas y la información relativa a la emisión, renovación y revocación de certificados se mantiene al menos durante 15 años.

5.5.3. Protección del archivo

Para la protección del archivo la GISS garantiza que:

- 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/titular de los certificados.

5.5.4. Procedimientos de copia de respaldo

La ACGISS realiza a diario copias de respaldo de acuerdo a la política establecida al efecto en la GISS.

Adicionalmente, la información crítica se replica en el Centro de Respaldo siguiendo los procedimientos y utilizando los medios indicados de forma general en la GISS.

5.5.5. Requisitos de marca de tiempo de los registros

Los sistemas de información empleados garantizan el registro del tiempo en que se realizan las operaciones de la ACGISS.

La fuente de tiempo utilizada se encuentra sincronizada con el Real Instituto y Observatorio de la Armada. El Real Instituto y Observatorio de la Armada, a través de la Sección de Hora, tiene como misión principal el mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala de “Tiempo Universal Coordinado”, considerada a todos los efectos como la base de la hora legal en todo el territorio nacional.

5.5.6. Sistema de archivo

El sistema de archivo es interno de la ACGISS y se opera de acuerdo a los procedimientos establecidos.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Solamente personal autorizado por la GISS tienen acceso a los datos de archivo, lo que se garantiza mediante la existencia de diversos controles de acceso físico y lógico.

5.6. Renovación de las claves de la AC

La renovación de las claves de la AC supone la renovación del certificado.

Los procedimientos para proporcionar las nuevas claves de las Autoridades de Certificación serán los mismos que para proporcionar la clave pública en vigor, incluyendo la publicación y notificación de las nuevas claves en el repositorio de información del Prestador.

5.7. Compromiso de claves y recuperación ante desastres

5.7.1. Procedimientos de gestión de incidentes y vulnerabilidades

El Prestador establece en su plan de continuidad los procedimientos que aplica en la gestión de los incidentes y, muy especialmente, en los compromisos de la seguridad de las claves.

Los procedimientos de notificación y respuesta de incidentes se emplean de tal manera que se minimizan los daños causados por incidentes de seguridad y mal funcionamiento.

La detección de los incidentes, especialmente los relacionados con el ciclo de vida de los certificados y con los controles de acceso a los sistemas y servicios, así como la realización de copias de seguridad de la información y los datos, se realizarán de acuerdo a lo estipulado en este documento.

Adicionalmente la GISS dispone de mecanismos y procedimientos internos de comunicación y resolución de incidencias técnicas que se produzcan en sus sistemas y servicios.

Concretamente, se dispone de procedimientos para responder rápidamente a los incidentes y notificar cualquier violación de seguridad a las partes apropiadas dentro de las 24 horas siguientes a su identificación.

Si la pérdida de integridad afecta a una persona natural o jurídica, la notificación se realiza lo antes posible desde la detección.

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.

La GISS dispone de diferentes procedimientos de recuperación y restauración para sus sistemas, incluyendo la disponibilidad de un centro de respaldo que replica la arquitectura de la PKI y los datos asociados.

5.7.3. Compromiso de la clave privada de la Entidad

El plan de continuidad de la GISS considera el compromiso o sospecha de compromiso de la clave privada del Prestador como un desastre.

En caso de compromiso de la clave privada de una CA, la ACGISS:

- Informará a todos los suscriptores y usuarios del compromiso, así como al organismo supervisor.
- Indicará que los certificados y la información del estado de revocación entregados usando dicha clave ya no son válidos.

- Revocará el certificado de la CA y publicará las correspondientes listas de revocación.
- Planificará la generación de nuevos certificados para las CAs, así como la emisión de nuevos certificados a los usuarios.
- Restablecerá tan pronto como sea posible el servicio.
- Estudiará las causas del compromiso y tomará las medidas oportunas para evitar su repetición.

En caso de compromiso de los algoritmos utilizados para la generación de los certificados, el prestador informará a los usuarios y planificará la emisión de nuevos certificados con algoritmos adecuados.

5.7.4. Recuperación ante desastres

La ACGISS desarrolla, mantiene y, si es necesario, ejecuta planes de contingencia y continuidad 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 GISS replica los sistemas y bases de datos de la PKI en su centro de respaldo. Las bases de datos de recuperación de desastres utilizadas por el Prestador están sincronizadas con las bases de datos de producción, dentro de los límites temporales especificados en los procedimientos establecidos. Los equipos de recuperación de desastres de la ACGISS disponen de medidas de seguridad físicas adecuadas.

La ACGISS es capaz de restaurar la mayoría de las operaciones de la PKI de forma razonablemente inmediata y al menos en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

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

5.8. Finalización del servicio

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 Confianza, la GISS realizará las siguientes actuaciones:

- Informará a todos los suscriptores y usuarios, así como al organismo supervisor, al menos 2 meses antes de la finalización de su actividad.
- Así mismo, informará a los anteriores actores del destino de los certificados, indicando además cualquier transferencia de la responsabilidad de archivo.
- Ejecutará, en caso necesario, 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.

- Garantizará la continuidad de los sistemas de consulta del estado de los certificados emitidos durante un tiempo apropiado (15 años) para asegurar la correcta validación de los mismos tras la finalización del servicio.

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 las CAs se generan en el interior de un módulo de hardware criptográfico HSM, que cumple con los requisitos necesarios para su protección. La generación se realiza dentro de las instalaciones de la GISS con las medidas de seguridad físicas y lógicas establecidas en el presente documento.

Las claves de las CAs se generan según un procedimiento definido de generación de claves que detalla los distintos roles involucrados y las funciones realizadas. Dicha ceremonia es realizada ante un auditor que garantiza que las actuaciones se han realizado conforme a dicho procedimiento.

Tanto el procedimiento de la generación del par de claves de la CA, como la posterior certificación de la clave pública, se llevan a cabo bajo al menos un control dual de roles de confianza, y manteniendo siempre este mínimo número de personal autorizado para desempeñar esta función.

Las claves de CAs se almacenan en diversas particiones dentro de los HSM, cada una de los cuales dispone de controles de acceso propios. Se utilizará una partición independiente, que se mantendrá offline, para la clave privada de la CA raíz.

La instalación y recuperación de los pares de claves de la CA requerirá el control simultáneo de al menos dos empleados de confianza.

La duración de los pares de claves de las CAs establecida en los certificados está condicionada a la seguridad de los algoritmos y mecanismos criptográficos utilizados. ACGISS garantiza que antes de su expiración se generarán nuevos certificados según los procedimientos establecidos en esta DPC. Esto se realizará con un margen de tiempo apropiado para permitir que los usuarios y las terceras partes de confianza sean conscientes del cambio y evitar la interrupción de las operaciones.

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

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.

6.1.3. Envío de la clave pública al emisor del certificado

El procedimiento de envío de la clave pública se realizará de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

6.1.4. Distribución de la clave pública de las Autoridades de Certificación

Las claves públicas de las CAs de ACGISS son comunicadas a los verificadores de sus certificados y al organismo supervisor, asegurando la integridad de la clave y la autenticidad del origen.

Estas claves públicas de las Autoridades de Certificación se publican adicionalmente en el Repositorio público, en forma de certificados auto-firmados.

6.1.5. Longitud de claves y algoritmos utilizados

Las claves de las Autoridades de Certificación de la ACGISS son al menos de 4.096 bits. Las claves de los certificados finales emitidos serán como mínimo de 2.048 bits.

Se utilizan algoritmo de firma RSA y algoritmos de hash SHA-2 para garantizar la seguridad y la autenticidad de los certificados emitidos.

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. La calidad de los parámetros de generación se garantiza a través de los sistemas y herramientas utilizadas en la gestión de los certificados.

6.1.7. Usos admitidos de las claves

La ACGISS incluye en los campos "*Key Usage"* y "*Extended Key Usage*" de los certificados, los usos permitidos de las correspondientes claves privadas.

Para las CAs los usos permitidos incluyen:

- Firma de claves de certificados ("*Key CertificateSignature*").
- Firma de las CRLs ("*CRL Signature*").

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

Se utiliza hardware criptográfico (HSM) certificado FIPS 140-2 Nivel 3 o superior y CC EAL 4+.

Los estándares aplicables a los módulos criptográficos utilizados en certificados finales se detallan en la correspondiente Política de Certificación.

El estado de certificación de los QSCD existentes es monitorizado hasta el fin del período de validez del certificado, y se toman medidas adecuadas en caso de modificación de este estado.

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

Las claves privadas de ACGISS, se encuentran bajo control multi personal, tanto a nivel físico como lógico, impidiendo que una única persona tenga acceso a las mismas.

6.2.3. Repositorio de la clave privada de las CAs

Las claves privadas de la ACGISS se generan en módulos criptográficos con medidas de seguridad estrictas, y se almacenan en espacios ignífugos y protegidos por controles de acceso físico que garantizan que el acceso lo realiza sólo personal autorizado.

Los HSM se someten a controles de seguridad adecuados durante su transporte y almacenamiento, y se operan en un entorno seguro y siguiendo procedimientos de operación y mantenimiento que garantizan su correcto funcionamiento a lo largo del tiempo.

6.2.4. Backup de la clave privada de las CAs

Por razones de continuidad de negocio, existe backup de las claves privadas de las CAs de ACGISS en tokens seguros almacenados en dependencia independiente de aquella donde se almacenan habitualmente y bajo estrictos controles de acceso y de procedimiento. Adicionalmente las claves generadas se replican en varios HSM conectados en cluster y sincronizados de forma segura, minimizando así la posibilidad de pérdida de las claves privadas.

6.2.5. Archivo de las claves privadas

No estipulado.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la ACGISS se generan directamente en el módulo criptográfico, no siendo necesaria su introducción en él. Cualquier transferencia posterior se realizará entre módulos criptográficos o desde los tokens de backup, asegurando en todo caso la seguridad del proceso.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos, en particiones específicas creadas para ello, que cuentan con las medidas de seguridad necesarias para garantizar su protección.

6.2.8. Método de activación de la clave privada

Las claves privadas de las CAs se activan mediante operaciones de SW realizadas por los roles autorizados.

6.2.9. Método de desactivación de la clave privada

La clave privada podrá ser desactivada a través del SW de la AC, por los roles especificados en los correspondientes procedimientos de operación.

6.2.10. Método de destrucción de la clave privada

Las claves privadas son destruidas siguiendo un procedimiento que impide su robo, modificación, divulgación no autorizada o uso no autorizado.

Todas las copias de las claves de la CA serán destruidas al finalizar su ciclo de vida.

6.2.11. Evaluación de los módulos criptográficos

Los módulos criptográficos de la ACGISS cumplen los requisitos de seguridad necesarios para garantizar la protección de las claves de la PKI de acuerdo con las normas y estándares internacionales, según lo establecido anteriormente en este documento.

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 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 este periodo 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 de las claves privadas de AC, se realiza según lo indicado anteriormente en este documento, siguiendo el procedimiento establecido para la ceremonia de generación de claves de las CAs. Las contraseñas o códigos de acceso se generan según unos requisitos mínimos establecidos de cara a asegurar un adecuado nivel de protección.

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

6.4.2. Protección de los datos de activación

Los datos de activación de las claves privadas de ACGISS sólo son conocidos por el personal autorizado. Los códigos de acceso se cambian periódicamente con el fin de aumentar su protección.

Para certificados finales, esta protección de datos de activación se especifica en la correspondiente Política.

6.4.3. Otros aspectos de los datos de activación

Sin estipulación adicional.

6.5. Controles de seguridad informática

ACGISS garantiza la aplicación de controles de seguridad adecuados para la protección de los sistemas y los datos de la PKI.

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 GISS mantiene una política de seguridad y diversa normativa técnica asociada, para la gestión adecuada de sus sistemas de información.
- La GISS utiliza redes y componentes seguros, adecuadamente gestionados y monitorizados.
- La ACGISS garantiza una administración efectiva del nivel de acceso de los usuarios para mantener la seguridad del sistema, incluyendo la gestión de cuentas de usuario, la realización de auditorías y el inicio de las 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 establecida. Para ello dispone de sistemas propios de gestión de identidades y de autorización de acceso a los sistemas.

  En concreto, se dispone de controles de acceso para detectar los intentos de añadir o borrar certificados o modificar cualquier otra información relacionada.
- El personal de la organización está identificado y autorizado antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal es responsable de las acciones realizadas en el ejercicio de sus funciones y puede 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.
- El acceso a los repositorios públicos de la información de la ACGISS cuenta con un control de accesos para modificaciones o borrado de datos.
- La GISS garantiza que dispone de medios suficientes para garantizar la integridad y continuidad de los procesos y datos en caso de contingencias.

- La ACGISS utiliza productos HW y SW certificados y con garantías suficientes para el desarrollo de sus funciones.
- En concreto, se definen controles de seguridad relacionados con la protección contra software malicioso, la gestión de soportes, el deterioro y las actualizaciones y parches de seguridad de aplicaciones.

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 GISS de cara a detectar posibles debilidades, mediante la realización de auditorías internas y externas y el establecimiento de los controles de seguridad necesarios.

Adicionalmente, la GISS dispone de diversas certificaciones de productos y procesos utilizados en la prestación de sus servicios, que garantizan su adecuado nivel de seguridad informática.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Se realiza un análisis de requerimientos de seguridad por un centro especializado de la GISS durante las fases de diseño y especificación de requisitos de los componentes utilizados en la ACGISS. Los desarrollos se llevan a cabo siguiendo la normativa interna existente que garantiza su calidad y su adecuación a las prácticas aprobadas.

Se establecen procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

Se dispone de diversos entornos independientes para desarrollo, preexplotación y producción de sistemas, con procedimientos y requisitos específicos para la promoción entre ellos.

6.6.2. Controles de gestión de seguridad

La ACGISS mantiene un inventario actualizado de sus activos informáticos y realiza controles de seguridad de los mismos de acuerdo con sus necesidades de protección, establecidas en la normativa interna aplicable.

Con el fin de protegerlos para que no sean retirados sin autorización, existe un exhaustivo control de entrada y salida de material e información.

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 lógica y de almacenamiento para los activos de información.

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 está 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.
- Se emplean mecanismos y procedimientos de gestión de red que garantizan la seguridad de las operaciones de la GISS.
- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras.
- Se garantiza que los componentes locales de red se encuentran ubicados en entornos seguros, así como el control periódico de sus configuraciones.
- En concreto, los sistemas de las CAs se mantienen en una zona segura con controles de seguridad específicos que protegen los sistemas y las comunicaciones entre los componentes.
- Se aplican controles de seguridad relacionados con segregación de red y comunicaciones seguras, existiendo zonas con distintos niveles de seguridad.
- Existe control de acceso a las redes específicas de la PKI mediante VLANs dedicadas.
- Se dispone de una conexión de red externa redundante para garantizar la disponibilidad de los servicios.
- Se realizan tests de intrusión con carácter periódico, registrando las evidencias.

6.8. Sellado de tiempo

La fuente de tiempo utilizada para el sellado de tiempo de las operaciones de ACGISS se encuentra sincronizada con el Real Instituto y Observatorio de la Armada utilizando el protocolo NTP.

7. PERFILES DE CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS REVOCADOS

7.1. Perfil de certificado

Los certificados serán conformes con lo establecido en los estándares aplicables a cada tipo de certificado y seguirán el formato X.509 v3.

Este punto se desarrollará en la correspondiente Política de Certificación.

7.2. Perfil de la lista de certificados revocados (CRLs)

Las listas de certificados revocados son conformes con los estándares aplicables y en concreto con el perfil X.509 v2.

Los principales campos de las CRLs son:

- Versión de la CRL.
- Identificación del emisor.
- Fecha de emisión de la CRL y de próxima actualización.
- Número de la CRL.
- Número de serie del certificado revocado.
- Fecha de revocación.
- Razón de revocación del certificado.

7.3. Perfil OCSP

Los servicios ofrecidos por ACGISS son conformes con la RFC 6960 (*Internet X.509 Public Key Infraestructure Online Certificate Status Protocol – OCSP*). Los certificados OCSP utilizarán el estándar X.509 versión 3.

7.4. Otros

La información específica sobre las prácticas y los perfiles de certificados utilizados para el sellado de tiempo se establecen en la política de certificación específica de la TSA (Autoridad de Sellado de Tiempo).

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.

8.1. Frecuencia de la auditoría de conformidad

Se deberá realizar una auditoría bienal de conformidad de los servicios cualificados de la PKI de acuerdo con lo establecido en el Reglamento UE nº 910/2014.

No obstante, se realizarán cuantas auditorías internas y externas intermedias se estimen convenientes para comprobar el funcionamiento de la PKI.

8.2. Identificación y calificación del auditor

La ACGISS dispone de un departamento de auditoría que será el encargado de realizar las auditorías internas que estime convenientes.

Para la realización de las auditorías externas la ACGISS acudirá a un auditor independiente externo, el cual deberá demostrar experiencia suficiente en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Prestadores y sus elementos relacionados, además de estar acreditado para ello.

8.3. Relación del auditor con la entidad auditada

Las auditorías externas serán realizadas por auditores independientes a la GISS.

Las auditorías internas serán llevadas a cabo por un departamento independiente a aquéllos que realizan la administración y operación de la ACGISS.

8.4. Relación de elementos objeto de auditoría

Los elementos mínimos objeto de auditoría serán los siguientes:

- Procesos de Autoridades de Certificación y elementos relacionados.
- Sistemas de información involucrados en las actividades de la ACGISS.
- Protección física adecuada de los elementos afectados.
- Documentación relacionada con la prestación de servicios de confianza.

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 resultados de las auditorías

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

El informe de auditoría acreditando el cumplimiento de los requisitos técnicos y de seguridad establecidos por la normativa para los certificados cualificados, será remitido al organismo supervisor.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. Tarifas

No se establecen tarifas para los servicios del prestador.

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 o restringidas 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 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.
- Planes de seguridad de los sistemas afectados.
- Documentación de operaciones y restantes planes de operación.

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” o publicada en el Repositorio del Prestador.

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 involucrados.

9.4. Protección de datos personales

9.4.1. Plan de Protección de Datos Personales

Los datos personales se recaban y tratan atendiendo a los planes de protección aprobados en la Seguridad Social de acuerdo con lo establecido en el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (RGPD).

El Prestador no divulga ni cede estos datos personales, excepto en los casos previstos o cuando sea exigible legalmente.

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 normativa de protección de datos está protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

9.4.3. Información no considerada privada

No se considera privada la información que se incluye en los certificados y en el referido mecanismo de comprobación del estado de los certificados, de acuerdo con lo previsto en el artículo 17.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

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

- Los certificados conteniendo la clave pública.
- 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 la política correspondiente.
- Los usos 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.

9.4.4. Responsabilidad correspondiente a la protección de los datos personales

La Seguridad Social garantiza como mínimo el cumplimento de sus obligaciones legales 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 la normativa aplicable de protección de datos personales.

La Seguridad Social establece un procedimiento de notificación, gestión y respuesta ante las incidencias relacionadas con los datos personales.

La Seguridad Social 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 prestación de consentimiento para el tratamiento de datos personales se realiza de acuerdo con lo dispuesto en la normativa aplicable de protección de datos personales.

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

La ACGISS sólo divulga la información confidencial en los casos legalmente previstos.

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 la normativa de protección de datos donde así se requiera.

9.4.7. Otros supuestos de divulgación de la información

La ACGISS incluye, en la política de confidencialidad prevista en este documento, cualesquiera otras 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 de la Seguridad Social son las únicas entidades que disfrutan de los derechos de propiedad intelectual sobre los certificados que emita.

9.5.2. Propiedad de políticas de certificación y DPC

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, sus correspondientes Políticas de Certificación y cualquier otro documento relacionado con los servicios ofrecidos.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor o titular 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 responsables de los certificados. Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave son propiedad del responsable 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.

En concreto, será responsable de:

- Emitir certificados conformes con las Políticas aprobadas y de acuerdo a los estándares aplicables.
- Revocar los certificados en los términos recogidos en la DPC.
- Mantener disponible gratuitamente los sistemas de comprobación del estado de los certificados.
- Utilizar sistemas y productos fiables y certificados, con las adecuadas medidas de protección, que garanticen la seguridad de los procesos de certificación.
- Mantener actualizada la información presente en el repositorio público del prestador.
- Comunicar los cambios de la DPC y las Políticas de Certificación según los procedimientos y las condiciones establecidas.
- Proteger las claves privadas de ACGISS según lo indicado en este documento.
- Conservar y archivar correctamente la información generada durante el tiempo legalmente exigible.
- Responder por los daños y perjuicios causados en el ejercicio de su actividad de acuerdo con lo estipulado en la Ley 59/2003, de 19 de diciembre.
- Colaborar en los procesos de auditoría que se realicen interna y externamente.
- Respetar los procedimientos establecidos para el cese de su actividad.

9.6.2. Autoridades de Registro

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

Son obligaciones de las Autoridades de Registro:

- Respetar las condiciones establecidas en la DPC y en las Políticas de Certificación específicas.

- Comprobar la identidad de los suscriptores de los certificados.
- Verificar la información suministrada por los suscriptores antes de la emisión de certificados.
- Informar al suscriptor y a los usuarios de las obligaciones que asumen y de la información mínima relativa al prestador.
- Tramitar y entregar los certificados de acuerdo a lo indicado en las políticas correspondientes.
- Archivar la documentación generada en el ejercicio de sus funciones.

9.6.3. Suscriptores/titulares

Son obligaciones de los suscriptores/titulares de los certificados:

- Suministrar a las Autoridades de Registro información exacta, completa y veraz en relación con los datos solicitados en los procesos del ciclo de vida de los certificados.
- Notificar cualquier modificación posterior de los datos suministrados.
- Conocer y aceptar las condiciones de emisión y de utilización de los certificados.
- Utilizar los certificados y sus claves de acuerdo a las condiciones y los usos permitidos establecidas en la DPC y en las políticas respectivas.
- No utilizar los certificados cuando haya expirado su período de validez o cuando éste haya sido revocado.
- Proteger sus claves privadas tomando las precauciones oportunas para evitar la pérdida, revelación o uso no autorizado.
- Comunicar a la GISS cualquier mal funcionamiento de los certificados.
- Observar los procedimientos establecidos en las políticas aplicables en caso de modificación de las circunstancias que dieron derecho a la emisión de los certificados, como el cese de prestación de servicios en la organización.

9.6.4. Verificadores y terceros aceptantes de los certificados

Los terceros que acepten y confíen en los certificados emitidos por ACGISS, deberán:

- Asumir la responsabilidad en la correcta comprobación de la validez y del estado de revocación de los certificados.
- Asumir la responsabilidad en la correcta validación de las firmas electrónicas realizadas con los certificados de ACGISS.
- Conocer las responsabilidades derivadas de la aceptación de los certificados.
- Limitar la aceptación de los certificados a los usos permitidos establecidos en los mismos y en las políticas de certificación aplicables.

9.7. Renuncias de garantías

No estipulado.

9.8. Limitaciones de responsabilidad

9.8.1. Limitaciones de responsabilidad del Prestador

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

En particular, no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, ante incumplimiento de las obligaciones establecidas en este documento a los suscriptores, titulares y terceros que aceptan sus certificados.

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 del Prestador, 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 para los certificados emitidos a partir de ese momento.

9.10.3. Efectos de la finalización

Las obligaciones y restricciones que establecen esta DPC y las correspondientes Políticas de Certificado, subsistirán tras su sustitución por una nueva versión para todos aquellos certificados emitidos con anterioridad.

9.11. Notificaciones

La ACGISS establece mecanismos de notificación entre las partes en las correspondientes políticas y en los procedimientos internos aplicables.

Adicionalmente publicará las principales notificaciones que afecten a los servicios prestados en su página web.

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 normativa tiene que ser aprobada por ACGISS según el procedimiento establecido para ello.

9.12.2. Periodo y mecanismos para notificaciones

En caso de que las modificaciones realizadas puedan afectar a la aceptabilidad de los certificados, la ACGISS las notificará a los usuarios a través de su página web y hará pública la nueva versión de la DPC.

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

Los OIDs establecidos en ACGISS se modificarán por exigencia normativa o en caso de emisión de nuevas versiones de certificados, que supongan la aplicación de nuevas prácticas de certificación diferentes a las anteriores. Se requerirá aprobación interna de los nuevos OIDs.

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.

Por otra parte, para la resolución de quejas y sugerencias se podrá utilizar el correspondiente buzón disponible en la Sede de la Seguridad Social, así como los procedimientos internos publicados en la Intranet corporativa.

9.13.2. Jurisdicción competente

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

9.14. Legislación que rige

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

- Reglamento UE nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
- 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.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (RGPD).
- 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.

Adicionalmente será de aplicación toda la normativa relacionada con los procedimientos administrativos referidos en este documento, así como la relativa a los derechos y obligaciones del personal que presta sus servicios en la Administración.

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

- ETSI EN 319 401: General policy requirements for TSPs supporting electronic signatures.
- ETSI EN 319 411: Policy and security requirements for TSPs issuing certificates.
- ETSI EN 319 412: Profiles for TSPs issuing certificates.
- ETSI EN 319 421: Policy and Security Requirements for TSPs issuing Time-Stamps.
- ISO/IEC 9595: Information technology -- Open Systems Interconnection -- Common management information service (X.500).
- RCF 3647 - Internet X. 509 Public Key Infrastructure Certificate Policy.
- RFC 3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- RFC 5280 - Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL).
- RFC 6960 - Online Certificate Status Protocol – OCSP.

9.15. Conformidad con la legislación aplicable

La ACGISS manifiesta su conformidad con la normativa vigente.

9.16. Cláusulas diversas

No aplica.

9.17. Otras cláusulas

9.17.1. Aspectos organizativos

Las unidades de GISS encargadas de la generación y revocación de certificados son responsables de la prestación de los servicios sin presiones de ningún tipo que puedan poner en duda la confianza en los servicios prestados.

Estas unidades están correctamente identificadas dentro de la estructura organizativa.

Asimismo, se garantiza que no existe discriminación de ningún tipo en la prestación de los servicios de certificación de ACGISS.

Los servicios son prestados por la GISS sin subcontratación u outsourcing de ninguno de ellos.

9.17.2. Pruebas

El prestador proporcionará capacidad de prueba de certificados cualificados a terceras partes de confianza.

Todos los certificados de prueba estarán correctamente identificados como tales en su nombre distintivo y se utilizarán exclusivamente para este fin.

9.17.3. Acceso a discapacitados

La Seguridad Social dispone de mecanismos y procedimientos adecuados para facilitar el acceso a los servicios a personas con discapacidad.

9.17.4. Términos y condiciones

Los términos y condiciones relativos a los certificados emitidos por ACGISS serán publicados en la Intranet de la Seguridad Social y adicionalmente en la página web del prestador cuando se trate de certificados cualificados.