Entidad de Certificación

THOMAS SIGNE

Soluciones Tecnológicas Globales

Política de Seguridad

Información del documento

Nombre	Política de Seguridad
Realizado por	Thomas Signe Perú
País	Perú
Versión	1.3
Fecha	Septiembre 2021
Tipo de documento	Público
Código	THS-PE-AC-POL-00

Historial de versiones

Versión	Fecha	Descripción
1.0	02/10/2017	Elaboración de documento inicial.
1.1	01/04/2019	Integración con el sistema de gestión del Grupo. Cambio de código del documento de THS-PE-POL-SI-01 a THS-PE-POL-EC-AC-00 Se modifica la estructura del documento
1.2	30/12/2020	Ajuste de la codificación según el GSIGNE-GRAL-PR-01 Control de la Informacion Documentada Ed 2.5
1.3	16/09/2021	Cambio de imagen THS

ÍNDICE

1 INTRODUCCIÓN

Signe S.A. (en adelante 'Signe') es una empresa con domicilio en España que brinda principalmente servicios consistentes en la edición e impresión de documentos de seguridad para empresas públicas y privadas. A partir del año 2010, Signe inicia su actividad como Prestador de Servicios de Certificación (PSC) que emite certificados reconocidos según la Ley 59/2003, de 19 de diciembre, de firma electrónica en España.

Desde hace más de 30 años, Signe se ha especializado en el diseño y desarrollo de soluciones de seguridad documental, produciendo y editando documentos -tanto en soporte papel como digital- protegidos contra posibles falsificaciones y modificaciones fraudulentas.

Hoy en día, gracias a una constante inversión en tecnología punta y la aplicación de estrictos controles de calidad, Signe se posiciona como un referente dentro del sector a nivel europeo y, cada vez más, también a nivel mundial.

En el año 2018, en una alianza comercial entre Signe y Thomas Greg & Sons de Perú, se ha creado la empresa Thomas Signe de Perú S.A. (en adelante Thomas Signe), para actuar como Entidad de Certificación, Entidad de Registro, Software de Firma Digital y Servicios de Valor Añadido como Sistema de Intermediación Digital y Autoridad de Sellado de Tiempo (Timestamp); y así brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

Como Entidad de Certificación Digital - EC, Thomas Signe provee servicios de emisión, re-emisión, distribución y revocación de certificados digitales.

La infraestructura tecnológica y operativa de la EC de Thomas Signe es provista por SIgne. Dicha infraestructura ha obtenido la cualificación Eidas y se verifica anualmente por auditores autorizados.

Junto a los servicios de certificación digital, Thomas Signe brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales. Además de servicios de valor añadido de intermediación digital y sellado de tiempo.

2 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas de seguridad del proveedor de infraestructura de Thomas Signe para la administración de los servicios de la Entidad de Certificación Digital – EC de Thomas Signe, conforme al marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura de servicios de certificación digital brindados por Thomas Signe a través de Signe, la cual cuenta con la cualificación eIDAS.

Signe, como proveedor de infraestructura y responsable de la gestión de operaciones de los servicios de la Entidad de Certificación de Thomas Signe, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC de Thomas Signe.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación - EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital.

Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Titular	Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital
Suscriptor	Persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.
ACC	Autoridad Administrativa Competente -
IOFE	Infraestructura Oficial de Firma Electrónica
PSC	Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica
PKI	Infraestructura de Clave Pública (Public Key Infraestructure)
CPS	Declaración de Prácticas de Certificación (Certificate Practice Statement)
HSM	Módulo de Seguridad Criptográfico (Hardware Security Module)
CRL	Lista de Certificados Revocados (Certificate Revocation List)
OCSP	Online Certificate Status Protocol
ETSI	European Telecommunications Standard Institute

5 PKI PARTICIPANTES

5.1 ENTIDAD DE CERTIFICACIÓN THOMAS SIGNE (EC THOMAS SIGNE)

Thomas Signe, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

A Thomas Signe, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la ACC a fin de poder ingresar a la IOFE.

5.2 ENTIDAD DE REGISTRO THOMAS SIGNE (ER THOMAS SIGNE)

Thomas Signe, brinda también los servicios de Entidad de Registro, la cual es la encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

5.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL E INFRAESTRUCTURA

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación Thomas Signe, entre sus principales funciones se encuentran las siguientes:

a) Garantizar la seguridad, disponibilidad y calidad de las operaciones de gestión de los certificados digitales de los usuarios finales.

b) Garantizar la seguridad de las claves de la EC Raíz y las EC Subordinadas durante todo su ciclo de vida.

c) Garantizar la disponibilidad y accesibilidad de los servicios de consulta de estado de revocación de los certificados digitales

d) Garantizar la protección de los datos personales de los usuarios finales.

e) Garantizar la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece Thomas Signe son provistos, en un contrato de tercerización.

El Proveedor de Servicios de Certificación (PSC) emite certificados reconocidos según la Ley de Firma Electrónica. Asimismo, es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida de los certificados.

5.4 TITULAR

Titular es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Dentro de la Infraestructura Oficial de Firma Electrónica, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado.

Tratándose de personas naturales, éstas son titulares y suscriptores del certificado digital.

5.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad.

Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

5.6 SOLICITANTE

En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular y suscriptor del certificado digital.

En el caso de personas jurídicas, la solicitud del certificado digital y el registro o verificación de su identidad deberán realizarse a través de un representante debidamente acreditado.

5.7 TERCERO QUE CONFÍA

Personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

5.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el certificado.

6 RESPONSABILIDADES

Signe, como proveedor de infraestructura y responsable de la gestión de operaciones de los servicios de la EC de Thomas Signe, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC de Thomas Signe.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por Thomas Signe.

Thomas Signe es responsable de exigir y supervisar las operaciones de los servicios de la EC que son administrados por el proveedor de infraestructura y responsable de la gestión de operaciones.

Como Entidad de Registro, Thomas Signe es responsable de la correcta identificación de las personas naturales o jurídicas y de la seguridad en la entrega de certificados digitales, siempre que esta sea realizada por los Operadores de Registro autorizados.

Las peticiones, quejas o reclamos sobre los servicios prestados por Thomas Signe o de su proveedor de infraestructura son recibidas directamente por la EC o ER de Thomas Signe. La línea telefónica es permanente para la atención a suscriptores y terceros debido a consultas relacionadas con el servicio que dispone Thomas Signe. Asimismo, pueden acercase hacia la oficina de ER de Thomas Signe indicando que presenta una queja, reclamo o petición. El suscriptor recibirá un mensaje de correo electrónico, cuando el reclamo o apelación sea resuelto.

7 ALCANCE

La presente política es de cumplimiento obligatorio por los proveedores de servicios de certificación digital e infraestructura contratados por Thomas Signe.

8 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

SIGNE subcontrata a Firmaprofesional el hosting, la gestión y operación de sus servicios de certificación. Con ello, SIGNE se adhiere a la Declaración de Prácticas de Certificación de Firmaprofesional, concretamente a su apartado 5º: CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES, del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN de Firmaprofesional, S.A., en la versión vigente en el momento de la publicación del presente documento.

8.1 CONTROLES FÍSICOS

La EC tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación de certificados ofrece protección frente:

a) Accesos físicos no autorizados.

b) Desastres naturales.

c) Incendios.

d) Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)

e) Derrumbamiento de la estructura.

f) Inundaciones.

g) Robo.

h) Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones garantiza la presencia de fuerzas de seguridad en un plazo no superior a 30 minutos, al encontrarse en el centro urbano de una capital de provincia.

8.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

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

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

8.1.2 ACCESO FÍSICO

El acceso físico a las dependencias del Prestador de Servicios de Certificación donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

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

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

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

8.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

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

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

8.1.4 EXPOSICIÓN AL AGUA

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

8.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

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

8.1.6 SISTEMA DE ALMACENAMIENTO

Cada medio de almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información que contenga y permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento, se guarda en armarios ignífugos o bajo llave permanentemente, requiriéndose autorización expresa para su retirada.

8.1.7 ELIMINACIÓN DE LOS SOPORTES DE INFORMACIÓN

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

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.
- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

8.1.8 COPIAS DE SEGURIDAD FUERA DE LAS INSTALACIONES

La EC mantiene un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos independiente del centro operacional.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

8.2 CONTROLES DE PROCEDIMIENTO

8.2.1 ROLES DE LOS RESPONSABLES

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de la jerarquía de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación.

Según lo especificado en las normas ETSI EN 319 401 y ETSI EN 319 411, los roles mínimos establecidos son:

- Responsable de seguridad (Security Officer): Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Operador de RA (Registration Officer): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final, así como las oportunas verificaciones en certificados de autenticación web.

- Responsable de revocación (Revocation Officers): Responsable de realizar los cambios en el estado de un certificado.
- Administradores del sistema de certificación (System Administrators): Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- Operadores de sistemas (System Operator): Responsables de la gestión del día a día del sistema (Monitorización, backup, recovery,…).
- Auditor interno (System Auditor): Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
- Operador de CA - Operador de Certificación: Responsables de activar las claves de la CA en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.

8.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

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

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

8.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

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

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

8.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Las tareas de Auditor son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

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

8.3 CONTROLES DE PERSONAL

8.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTOS PROFESIONALES

Todo el personal que realiza tareas calificadas como confiables sin supervisión, lleva al menos seis meses trabajando en el centro de producción y tiene contrato laboral fijo.

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

La EC se asegura que el personal de registro es personal confiable de una Corporación para realizar las tareas de registro. A tal efecto se exige una declaración en tal sentido por parte de la Entidad que asume funciones de ER.

El empleado del registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las peticiones. Al final de dicho curso, un auditor externo procederá a evaluar sus conocimientos del proceso.

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

8.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

Las ERs pueden establecer criterios diferentes, siendo responsables por la actuación de las personas que autoricen a acceder a los sistemas de la ER.

8.3.3 REQUERIMIENTOS DE FORMACIÓN

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, realiza los cursos necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

8.3.4 REQUERIMIENTOS Y FRECUENCIA DE ACTUALIZACIÓN DE LA FORMACIÓN

Se realizarán actualizaciones con una frecuencia anual, salvo por modificaciones a la DPC, que serán notificadas a medida que sean aprobadas.

8.3.5 SANCIONES POR ACTUACIONES NO AUTORIZADAS

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe dispone de un régimen sancionador interno por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

8.3.6 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados contratados para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y la requerimientos operacionales empleados por la EC. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

8.3.7 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

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

8.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

8.4.1 TIPOS DE EVENTOS REGISTRADOS

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la EC. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la EC a través de la red.
- Intentos de accesos no autorizados a la red interna de la CA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la Entidad de Certificación.
- Encendido y apagado de la aplicación de la EC.
- Cambios en los detalles de la EC y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico de la EC.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Las ceremonias de creación de claves de las EC y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza en la EC.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de las EC.

8.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

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

8.4.3 PERIODO DE CONSERVACIÓN DE LOS REGISTROS DE AUDITORÍA

Se almacenará la información de los logs de auditoría durante 15 años para garantizar la seguridad del sistema en función de la importancia de cada log en concreto.

8.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

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

Son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la Entidad de Certificación.

Los dispositivos son manejados en todo momento por personal autorizado.

8.4.5 PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

La EC tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena en armario ignífugo bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado. Se realizan copias diarias incrementales y completas semanales.

Adicionalmente se mantiene copia de los logs de auditoría en centro de custodia externo.

8.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

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

8.4.7 ANÁLISIS DE VULNERABILIDADES

La EC realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

8.5 ARCHIVO DE REGISTROS

8.5.1 TIPOS DE EVENTOS ARCHIVADOS

Se conservarán los eventos que tengan lugar durante el ciclo de vida del certificado, incluyendo la renovación del mismo. Se almacenará por la EC o, por delegación de ésta en la ER:

- Todos los datos de la auditoría.
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores y los datos relativos a su identificación.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos o publicados.
- CRL's emitidas o registros del estado de los certificados generados.
- La documentación requerida por los auditores.
- Las comunicaciones entre los elementos de la PKI.
- La EC es responsable del correcto archivo de todo este material y documentación.

8.5.2 PERIODO DE CONSERVACIÓN DE REGISTROS

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. En particular:

- Los certificados se conservarán publicados en el repositorio durante al menos un año desde su expiración.
- Los contratos con los Suscriptores y cualquier información relativa a la identificación y autenticación del Suscriptor serán conservados durante al menos 15 años (desde el momento de la caducidad del certificado) o el periodo que establezca la legislación vigente.

8.5.3 PROTECCIÓN DE ARCHIVOS

La EC asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

La EC dispone de documentos técnica y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

8.5.4 PROCEDIMIENTOS DE COPIA DE SEGURIDAD DEL ARCHIVO

La EC dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

8.5.5 REQUERIMIENTOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los registros están fechados con una fuente fiable.

Existe dentro de la documentación técnica y de configuración de la EC un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

8.5.6 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Durante la auditoría requerida por el documento CPS, el auditor verificará la integridad de la información archivada.

El acceso a la información archivada se realiza solo por personal autorizado.

La EC proporcionará la información y los medios al auditor para poder verificar la información archivada.

8.6 CAMBIO DE CLAVES DE LA EC

8.6.1 EC RAÍZ

Antes de que el certificado de la EC Raíz expire se realizará un cambio de claves (rekeying) y, en su caso, se introducirán cambios en el contenido del certificado que se ajusten mejor a la legislación vigente y la realidad de Firmaprofesional y del mercado. La EC antigua y su clave privada sólo se usarán para la firma de

CRL's mientras existan certificados activos emitidos por la EC antigua. Se generará una nueva CA con una clave privada nueva.

La documentación técnica y de seguridad de la EC detalla el proceso de cambio de claves de la EC.

8.6.2 EC SUBORDINADA

En el caso de las EC subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves. Sólo cuando se realice el cambio se aplicará lo descrito en el punto anterior.

8.7 PLAN DE RECUPERACIÓN DE DESASTRES

8.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

La EC ha desarrollado un plan de contingencias, detallado en el documento "Política de Seguridad", para recuperar todos los sistemas en menos de 48 horas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la EC para implementar dichos procesos.

8.7.2 ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

En el caso de que tuviera lugar un incidente que alterara o corrompiera tanto recursos hardware, software como datos, el Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, procederá según lo estipulado en el documento "Política de seguridad".

8.7.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA ENTIDAD DE CERTIFICACIÓN

El plan de contingencias de la jerarquía del Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe, trata el compromiso de la clave privada de la EC como un desastre.

En caso de compromiso de la clave privada de la EC:

- Informará a todos los suscriptores, usuarios y otras ECs con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de la EC.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

8.7.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

La EC restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con el documento CPS dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

La EC dispone de un centro alternativo, en caso de ser necesario, para la puesta en funcionamiento de los sistemas de certificación.

8.8 CESE DE UNA EC O ER

8.8.1 ENTIDAD DE CERTIFICACIÓN

Thomas Signe informará a todos los titulares, con una anticipación de treinta (30) días, sobre la terminación de su actividad o actividades, la fecha precisa de cesación y las consecuencias jurídicas de esta respecto de los certificados expedidos. Si por causas de fuerza mayor el servicio es suspendido temporalmente, Thomas Signe informará al titular dentro de las veinticuatro (24) horas siguientes de ocurrido el incidente.

Los registros competentes de los certificados emitidos a los ciudadanos y empresas privadas serán mantenidos hasta ser cumplido el plazo de diez (10) años.

8.8.2 ENTIDAD DE REGISTRO O VERIFICACIÓN

En el caso de cese de actividades de la Entidad de Registro o Verificación, se debe informar con un (1) mes de anticipación tanto al INDECOPI como a los titulares, suscriptores y terceros que confían.

9 CONTROLES TÉCNICOS DE SEGURIDAD

SIGNE subcontrata a Firmaprofesional el hosting, la gestión y operación de sus servicios de certificación. Con ello, SIGNE se adhiere a la Declaración de Prácticas de Certificación de Firmaprofesional, concretamente a su apartado 6º: CONTROLES DE SEGURIDAD TÉCNICA, del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN de Firmaprofesional, S.A., en la versión vigente en el momento de la entrada en vigor del presente documento.

9.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

9.1.1 GENERACIÓN DEL PAR DE CLAVES

La generación de la clave de las ECs se realiza, de acuerdo con el proceso documentado de ceremonia de claves, dentro de la sala de seguridad del PSC, en dispositivos criptográficos hardware (HSM), por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de Firmaprofesional, de la organización titular de la EC y del auditor externo.

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe garantiza que las claves de firma de la EC no son empleadas para otro supuesto que los indicados en este documento.

Para los certificados de entidad final:

a) El Custodio de claves recibirá por correo electrónico la confirmación de la solicitud, juntamente con un código de autenticación a la aplicación online de emisión de certificados.
b) Para poder acceder a la aplicación online de emisión de certificados será necesario que el Custodio de claves proporcione el código de autenticación recibido. Una vez autenticado, el Custodio de claves procederá a la descarga del certificado electrónico (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá).

9.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

La ER será responsable de garantizar la entrega del certificado al firmante, habilitándole los mecanismos para su descarga y posterior uso, asegurándose así que éste último está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

a) La descarga del certificado electrónico por el Custodio de claves incluye la descarga de la clave privada, protegidos con una contraseña que él mismo establecerá.
b) El Custodio de claves podrá instalar las claves y el certificado en su ordenador o sistema informático introduciendo la contraseña que él mismo estableció en el momento de la descarga.

9.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El envío de la clave pública a la EC para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X.509 autofirmado, utilizando un canal seguro para la transmisión.

9.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS ACEPTANTES

El certificado de las ECs de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en la página web de Firmaprofesional, como prestador de servicios de Thomas Signe.

9.1.5 TAMAÑO DE LAS CLAVES

Certificado	Tamaño claves RSA (bits)	Periodo validez (años)
CA Raíz	4096	21
CA Subordinadas	2048	15 (máximo)
Entidad final	1024 / 2048	3 (máximo)
Operador / Administrador	1024 / 2048	1 (máximo)

(*) Únicamente 2048 desde 1 de enero de 2017

9.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

Se utilizan los parámetros recomendados en el documento de especificaciones técnicas de la ETSI: TS 119 312.

Concretamente los parámetros utilizados son los siguientes:

Entry name of the signature suite	**Entry name for the hash function**	**Entry name for the padding method**	**Entry name for the signature algorithm**
sha256-with-rsa	sha256	No padding required	rsa

9.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509V3)

Todos los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de la claves.

Los usos admitidos de la clave para cada certificado están definidos en la Política de Certificación correspondiente.

9.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

9.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos empleados para generar y almacenar las claves de la Entidad de Certificación están certificados con la norma FIPS-140-2 nivel 3.

Las claves de los Operadores de Registro y administradores son generadas de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 3, ITSEC E4 High u otro de nivel equivalente.

9.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

El acceso a las claves privadas de la EC requiere el concurso simultáneo de dos dispositivos criptográficos diferentes de cinco posibles, protegidos por una clave de acceso.

9.2.3 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de la EC raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

Las claves privadas de las EC Subordinadas están custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3.

El Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe no custodia copias de respaldo de las claves privadas de los suscriptores de certificados (key escrow).

9.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

Existen unos dispositivos que permiten la restauración de la clave privada de la EC, que son almacenados de forma segura y sólo accesibles por personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro.

Este procedimiento se describe en detalle en las políticas de seguridad del Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe.

9.2.5 ARCHIVO DE LA CLAVE PRIVADA

La EC no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de la EC para comunicarse entre sí, firmar y cifrar la información serán archivadas por un periodo de al menos 10 años, después de la emisión del último certificado.

9.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA DESDE EL MÓDULO CRIPTOGRÁFICO

Esta actividad es realizadapor el Proveedor de Servicio de Certificación Digital e Infraestructura de Thomas Signe.

9.2.7 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves de la EC se activan por un proceso que requiere la utilización simultánea de 2 de 5 dispositivos criptográficos (tarjetas).

El acceso a la clave privada del Firmante o Creador del Sello en DCCF o DCCS portable se realiza habitualmente por medio de un código de activación (PIN). Generalmente, el dispositivo tiene un sistema de protección contra intentos de acceso que lo bloquean cuando se introduce más de un determinado número de veces un código de acceso erróneo. Para desbloquear el dispositivo, habitualmente, el dispositivo dispone de un código de desbloqueo (PUK). Generalmente, si se introduce un determinado número de veces erróneamente, el dispositivo se bloquea definitivamente, quedando inservible.

El PIN y el PUK son secretos y personales para el usuario y, en el caso de que el Custodio de claves no aporte su propio dispositivo DCCF/DCCS, le son entregados por la RA en el proceso de emisión del certificado. Tanto el PIN como el PUK pueden ser modificados posteriormente por el usuario utilizando las aplicaciones correspondientes.

El acceso a la clave privada del Firmante en DCCF centralizado se realiza mediante la utilización de dos factores de autenticación de categorías distintas (contraseña definida por el Firmante, como factor de autenticación basado en el conocimiento, y contraseña de un solo uso que el Firmante recibe en su teléfono móvil, como factor de autenticación basado en la posesión). Adicionalmente, no se podrá usar la clave privada del Firmante en DCCF centralizado para realizar la firma de copias electrónicas de títulos sin previa autorización del Firmante mediante firma con un certificado reconocido/cualificado.

El acceso a la clave privada del Creador del sello en DCCS centralizado se realiza únicamente para su utilización para la firma automatizada de documentos electrónicos expedidos por el Suscriptor, mediante la utilización de una contraseña definida por el Custodio de claves y configurada por éste en el sistema informático que realiza la firma automatizada.

9.2.8 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada del Firmante o Creador del Sello en DCCF o DCCS portable quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma o sello del dispositivo de lectura.

9.2.9 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de las ECs, o de los datos de activación de las mismas, incluyendo también los dispositivos que contengan cipias de dichas claves.

9.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

9.3.1 ARCHIVO DE LA CLAVE PÚBLICA

La EC conservará todas las claves públicas durante el periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación este activo y 6 meses más como mínimo, en otro caso.

9.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

Un certificado no debe ser usado después del periodo de validez del mismo aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación en línea válido para ese certificado.

9.4 DATOS DE ACTIVACIÓN

9.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación son generados en el momento de inicialización del dispositivo criptográfico.

Si la inicialización se produce en una entidad externa, los datos de activación le serán entregados al suscriptor mediante un proceso que asegure la confidencialidad de los mismos ante terceros.

9.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la EC raíz y ECs subordinadas.

Para los certificados de entidad final, una vez se ha hecho entrega del dispositivo y de los datos de activación, es responsabilidad del suscriptor de mantener la confidencialidad de estos datos.

9.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

9.5 CONTROLES DE SEGURIDAD INFORMÁTICA

La EC emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Firmaprofesional, como prestador de servicios de Thomas Signe, en los siguientes aspectos:

a) Configuración de seguridad del sistema operativo.

b) Configuración de seguridad de las aplicaciones.

c) Dimensionamiento correcto del sistema.

d) Configuración de Usuarios y permisos.

e) Configuración de eventos de log.

f) Plan de backup y recuperación.

g) Configuración antivirus.

h) Requerimientos de tráfico de red.

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

9.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de la EC incluye las siguientes funcionalidades:

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

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

9.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en el centro de datos de Firmaprofesional, como prestador de servicios de Thomas Signe.

9.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

9.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

La EC posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

9.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

9.6.2.1 GESTIÓN DE SEGURIDAD

La CA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un foro para la gestión de la seguridad.

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

9.6.2.2 CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN Y BIENES

La CA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la CA detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

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

9.6.2.3 OPERACIONES DE GESTIÓN

La CA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En la documentación técnica de la CA y de procedimientos del CPD se desarrolla en detalle el proceso de gestión de incidencias.

La CA dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

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

9.6.2.4 TRATAMIENTO DE LOS SOPORTES Y SEGURIDAD

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

9.6.2.5 PLANNING DEL SISTEMA

El departamento técnico de la CA mantiene un registro de las capacidades de los equipos.

Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

9.6.2.6 REPORTES DE INCIDENCIAS Y RESPUESTA

La CA dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

9.6.2.7 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

La CA define actividades asignadas a personas con un rol de confianza distinto a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

9.6.2.8 GESTIÓN DEL SISTEMA DE ACCESO

La CA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a) Gestión general de la CA:

- Se dispone de controles basados en firewalls de alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- La CA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- La CA dispone de un procedimiento para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.
- El personal de la CA será responsable de sus actos, por ejemplo, por retener logs de eventos.

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

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

d) Estado de la revocación:
- La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

9.6.2.9 GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

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

El Hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.

La CA registra toda la información pertinente del dispositivo para añadir al catálogo de activos de Firmaprofesional, S.A.

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

Firmaprofesional realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo criptográfico solo es manipulado por personal confiable.

La clave privada de firma de la CA almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.

La configuración del sistema de la CA así como sus modificaciones y actualizaciones son documentadas y controladas.

La CA posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

9.7 CONTROLES DE SEGURIDAD DE LA RED

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

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada.

9.8 SELLADO DE TIEMPO

El tiempo se obtiene mediante un hardware específico con reloj atómico de átomo de rubidio, sincronización GPS y consulta al Real Observatorio de la Armada1, siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en el RFC 5905 “Network Time Protocol”.

http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/06_Hora

10 RESPONSABLE DE PRIVACIDAD Y SEGURIDAD

El Responsable de Seguridad y Privacidad de datos personales de Thomas Signe se encarga de velar por el cumplimiento de la presente política, así como de su revisión periódica, difusión, concientización y capacitación al personal y terceros para su adecuado cumplimiento.

11 CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la EC de Thomas Signe, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

[1] Información del sitio web: http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/06_Hora