Servicios de Valor Añadido

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

Política de Seguridad del Servicio de Valor Añadido

Autoridad de Sellado de Tiempo

Información del documento

THS-PE-POL-SI-TSA-01

Nombre	Política de Seguridad del Servicio de Valor Añadido – Autoridad de Sellado de Tiempo
Realizado por	Thomas Signe Perú
País	Perú
Versión	1.1
Fecha	Abril del 2019
Tipo de documento	Confidencial
Código	THS-PE-POL-TSA-AC-00

Historial de versiones

Versión	Fecha	Descripción
1.0	02/10/2017	Elaboración de documento inicial.
1.1	01/04/2019	Integración en el Sistema de gestión del Grupo Cambio de código del documento de THS-PE-POL-SI-TSA-01 a THS-PE-POL-TSA-AC-00 Se modifica la estructura del documento

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 con la empresa Thomas&Greg Perú, se ha creado la empresa Thomas Signe Soluciones Tecnológicas Globales (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 Sellado de Tiempo – TSA, Thomas Signe asume las responsabilidades de representación de los servicios de sello de tiempo brindados por Signe mediante su proveedor Firmaprofesional, la cual es una infraestructura tercerizada y certificada.

2 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y procedimientos que utiliza Thomas Signe para la garantizar la seguridad de la información de sus servicios como SVA de Sellado de Tiempo, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de emisión de sellos de tiempo brindados por Thomas Signe a través de Signe y Firmaprofesional. Ambos proveedores cuentan con la certificación eIDAS para los procesos de gestión y operación de los servicios de emisión de sellos de tiempo y certificados digitales.

Thomas Signe representa a Signe y Firmaprofesional para todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Autoridad de Sellado de Tiempo.

4 DEFINICIONES Y ABREVIACIONES

4.1 DEFINICIONES

Autoridad de Sellado de Tiempo (TSA)	Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
Declaración de Prácticas de la TSA	Conjunto de declaraciones acerca de políticas y prácticas que dirigen las actividades y procesos de la TSA y que son publicadas para conocimiento de suscriptores y terceros que confían.

Política de Sellado de Tiempo	Conjunto de directivas que dirigen la aplicabilidad y requisitos en la administración de un servicio de sello de tiempo para una determinada comunidad de usuarios y un determinado alcance.
Sello de Tiempo	Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. El sello de tiempo incluye: - La firma digital de la entidad de sellado de tiempo - Identificador electrónico único del documento (HASH o resumen) - Fecha y hora recogida de una fuente fiable de tiempo
Unidad de Sellado de Tiempo	Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo. Todas las TSU mencionadas en el presente documento pertenecen a Firmaprofesional.
Sistemas de la TSA	Sistemas de tecnologías de la información que soportan la provisión de servicios de sellado de tiempo.
Suscriptor	Persona natural o jurídica que requiere los servicios provistos por una Autoridad emisora de sellos de tiempo – TSA y que está conforme con los acuerdos y obligaciones descritos en la Declaración de Prácticas y la Política de Sellado de Tiempo.
Tercero que confía	Persona natural o jurídica que recibe un documento con un sello de tiempo y confía en la validez de dicho sello provisto por la TSA de Thomas Signe y Firmaprofesional.

4.2 ABREVIACIONES

BIPM International Bureau of Weights and Measures (Bureau International Des Poids et Mesures)

GMT Greenwich Mean Time

IERS International Earth Rotation Service

TAI International Atomic Time (Temps atomique international)

TSA Time-Stamping Authority

TSU Time-Stamping Unit

UTC Coordinated Universal Time

5 ALCANCE

La presente política es de cumplimiento obligatorio para el personal y terceros subcontratados por Thomas Signe, quienes participan de las operaciones críticas de los Servicios de Valor Añadido conforme a las responsabilidades específicas en las siguientes secciones.

6 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe ,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.

6.1 CONTROLES FÍSICOS

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

- Accesos físicos no autorizados.

- Desastres naturales.

- Incendios.

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

- Derrumbamiento de la estructura.

- Inundaciones.

- Robo.

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

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

6.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Las instalaciones de Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

6.1.2 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.

6.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones de Firmaprofesional 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.

6.1.4 EXPOSICIÓN AL AGUA

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

6.1.5 PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

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

6.1.6 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.

6.1.7 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.

6.1.8 COPIAS DE SEGURIDAD FUERA DE LAS INSTALACIONES

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

6.2 CONTROLES DE PROCEDIMIENTO

6.2.1 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 la norma CEN CWA 14167-1, 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

- 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 Firmaprofesional en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.

- Operador de RA (Registration Officer): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final.

6.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

- La generación de la clave

- La recuperación y back-up de la clave privada

- La emisión de certificados

- Activación de la clave privada

- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la root

6.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN POR ROL

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara 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.

6.2.4 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.

6.3 CONTROLES DE PERSONAL

6.3.1 REQUISITOS RELATIVOS A LA CALIFICACIÓN, CONOCIMIENTO Y EXPERIENCIA 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.

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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 RA.

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.

Firmaprofesional 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.

6.3.2 PROCEDIMIENTOS DE COMPROBACIÓN DE ANTECEDENTES

Firmaprofesional realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

Asimimso, pueden establecer criterios diferentes, siendo responsables por la actuación de las personas que autoricen.

6.3.3 REQUERIMIENTOS DE FORMACIÓN

Firmaprofesional 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.

6.3.4 REQUERIMIENTOS Y FRECUENCIA DE ACTUALIZACIÓN DE LA FORMACIÓN

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

6.3.5 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Firmaprofesional dispone de un régimen sancionador interno por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

6.3.6 REQUISITOS DE CONTRATACIÓN DE TERCEROS

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

6.3.7 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Firmaprofesional 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.

6.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

6.4.1 TIPOS DE EVENTOS REGISTRADOS

Firmaprofesional registra y guarda los logs de todos los eventos relativos al sistema de seguridad. 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 Firmaprofesional a través de la red.

- Intentos de accesos no autorizados a la red interna.

- Intentos de accesos no autorizados al sistema de archivos.

- Acceso físico a los logs.

- Cambios en la configuración y mantenimiento del sistema.

- Registros de las aplicaciones de la Autoridad de Certificación.

- Encendido y apagado de la aplicación.

- Cambios en los detalles de Firmaprofesional 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.

- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, Firmaprofesional conserva, ya sea manual o electrónicamente, la siguiente información:

- Las ceremonias de creación de claves 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 CA.

- 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.

6.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA

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.

6.4.3 PERIODO DE CONSERVACIÓN DE LOS REGISTROS DE AUDITORÍA

Se almacenará la información de los logs de auditoría el tiempo que se considere necesario para garantizar la seguridad del sistema en función de la importancia de cada log en concreto.

6.4.4 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 Autoridad de Certificación.

Los dispositivos son manejados en todo momento por personal autorizado.

6.4.5 PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Firmaprofesional 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.

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, tiene implementado un procedimiento de backup seguro de los logs de auditoria, 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.

6.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA

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

6.4.7 ANÁLISIS DE VULNERABILIDADES

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

6.5 ARCHIVO DE REGISTROS

6.5.1 TIPO 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 Firmaprofesional o, por delegación de ésta:

- 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 y

- las comunicaciones entre los elementos de la PKI

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

6.5.2 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. 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 o el periodo que establezca la legislación vigente.

6.5.3 PROTECCIÓN DEL ARCHIVO

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

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

6.5.4 PROCEDIMIENTOS DE COPIA DE SEGURIDAD DEL ARCHIVO

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

6.5.5 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 Firmaprofesional un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

6.5.6 SISTEMA DE ARCHIVO DE INFORMACIÓN DE AUDITORÍA

No estipulado.

6.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

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

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

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

6.6 PLAN DE RECUPERACIÓN DE DESASTRES

6.6.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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 Firmaprofesional para implementar dichos procesos.

6.6.2 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, Firmaprofesional procederá según lo estipulado en el documento "Política de seguridad".

6.6.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD DE CERTIFICACIÓN

El plan de contingencias de la jerarquía de Firmaprofesional trata el compromiso de la clave privada de Firmaprofesional como un desastre.

En caso de compromiso de la clave privada, Firmaprofesional:

- Informará a todos los suscriptores, usuarios y otras CA's con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web.

- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

6.6.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con la CPS de Firmaprofesional dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

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

7 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

7.1 CONTROLES DE DESARROLLO DE SISTEMAS

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

7.2 CONTROLES DE GESTIÓN DE SEGURIDAD

7.2.1 GESTIÓN DE SEGURIDAD

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

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

7.2.2 CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN Y BIENES

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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 Firmaprofesional 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.

7.2.3 OPERACIONES DE GESTIÓN

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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 Firmaprofesional y de procedimientos del CPD se desarrolla en detalle el proceso de gestión de incidencias.

Firmaprofesional dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

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

7.2.4 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.

7.2.5 GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

- Firmaprofesional 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.

- Firmaprofesional registra toda la información pertinente del dispositivo para añadir al catalogo 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 Firmaprofesional almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.

- La configuración del sistema de Firmaprofesional así como sus modificaciones y actualizaciones son documentadas y controladas.

- Firmaprofesional 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.

7.3 CONTROLES DE SEGURIDAD DE LA RED

Firmaprofesional, como prestador de servicios de la TSA de Thomas Signe, 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.

7.4 FUENTE DE TIEMPO

El tiempo se obtiene mediante consulta al Real Observatorio de la Armada, siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en el RFC 1305 “Network Time Protocol”. Para más información, el sitio web es el siguiente:

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

8 RESPONSABLE DE SEGUIRDAD Y PRIVACIDAD

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 para su adecuado cumplimiento.

9 CONFORMIDAD

Este documento ha sido aprobado por el Responsable del Prestador de Servicios de Valor Añadido de Thomas Signe, y tiene carácter normativo sobre los servicios de Valor Añadido de la Autoridad de Sellado de Tiempo, por lo que cualquier incumplimiento por parte de lor roles responsables mencionados en el alcancee de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.