Declaración de los Administradores sobre sus prácticas de negocio y controles como Prestador de Servicios de Certificación

2 de abril de 2019.

SIGNE, S.A. (en adelante, "SIGNE"), opera como un prestador de servicios de certificación/confianza (PSC) y la Autoridad de Certificación Subordinada “SIGNE Autoridad de Certificación” emite certificados digitales a personas físicas, a corporaciones privadas y a corporaciones públicas, conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, (en adelante, “Ley 59/2003”) y al 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 y por la que se deroga la Directiva 1999/93/CE (en adelante, “Reglamento eIDAS”). SIGNE forma parte de la Jerarquía de Certificación de Firmaprofesional, que está compuesta por una Autoridad de Certificación (AC, en inglés, CA o Certification Authority) Raíz y varias Autoridades de Certificación Delegadas o Subordinadas entre las que se encuentra “SIGNE Autoridad de Certificación”, proporcionando los siguientes servicios:

- Registro del suscriptor.
- Gestión del ciclo de vida de los certificados electrónicos (emisión, renovación y revocación).
- Publicación del estado de los certificados mediante lista de certificados revocados (CRL) y Online Certificate Status Protocol (OCSP).
- Cuando proceda, gestión del ciclo de vida de dispositivos (seguros/cualificados) de creación de firma electrónica o sello electrónico (DSCF/DCCF/DCCS), como tarjetas de circuito integrado criptográficas o tokens USB criptográficos.

Para llevar a cabo la prestación de los servicios de certificación, SIGNE subcontrata tareas como la identificación de los solicitantes de certificados a Autoridades de Registro (AR), según permiten la Ley 59/2003 y el Reglamento eIDAS. Estas tareas se desarrollan según lo establecido en las Políticas y Prácticas de Certificación de SIGNE (consultables en http://www.signe.es/signe-ac/dpc/) y en los acuerdos suscritos entre SIGNE y las AR.

La Dirección de SIGNE es responsable de establecer y mantener los controles efectivos sobre las operaciones y procedimientos de su AC, incluyendo las Manifestaciones de sus Prácticas de Negocio como AC, la integridad del servicio (incluyendo controles para gestionar el ciclo de vida de las claves, los certificados y los DSCF/DCCF u otros dispositivos de creación de firma electrónica o sello electrónico, en este último caso, si procede) y los controles del Entorno. Estos controles contienen mecanismos de monitorización, y se toman acciones para corregir las deficiencias encontradas. Para estos controles cuenta con la colaboración de su proveedor de servicios de certificación Firmaprofesional.

Existen limitaciones inherentes en algunos controles, incluyendo la posibilidad de errores humanos y la evasión o anulación de los controles. En las ocasiones en que un análisis de riesgos recomienda la inclusión de controles compensatorios para cubrir las mencionadas limitaciones inherentes, éstos se incluyen. Aun así, incluso los controles efectivos pueden proporcionar solamente una seguridad razonable en relación con las operaciones, procedimientos y entorno de SIGNE como PSC. Adicionalmente, debido a cambios en las condiciones, la efectividad de los controles puede variar cada cierto tiempo.

Por todo ello, SIGNE en colaboración con Firmaprofesional y con el pleno apoyo de la dirección:

- Hace públicas sus Prácticas de Negocio sobre la gestión del ciclo de vida de las claves y los certificados, así como su política de privacidad de la información y proporciona sus servicios conforme a dichas afirmaciones.

- Mantiene controles efectivos para proporcionar una seguridad razonable de que:
  - La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por SIGNE).
  - La integridad de las claves y certificados gestionados se mantiene a lo largo de todo su ciclo de vida.
  - La privacidad de las claves privadas se mantiene a lo largo de todo su ciclo de vida.
  - El acceso a la información de suscriptores y usuarios está restringido a personal autorizado y la información está protegida de usos no especificados en las prácticas de negocio publicadas de SIGNE.
  - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.
  - Las tareas de explotación, desarrollo y mantenimiento de los sistemas de la AC son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos.

Todo ello alineado con los estándares internacionalmente aceptados:

- ISO 27001

Principio 1: Declaración de Prácticas de Negocio

Declaración de Prácticas y Políticas de Certificación para “SIGNE Autoridad de Certificación” (http://www.signe.es/signe-ac/dpc/), incluyendo:

- DPC - Declaración de Prácticas de Certificación

- Política de certificación de Certificados Corporativos de Persona Física
- Política de certificación de Certificados Corporativos de Sello Electrónico
- Política de certificación de Certificados Corporativos de Firma Empresarial
- Política de certificación de Certificados de Sello de Órgano
- Política de certificación de Certificados de Titulado

Principio 2: Integridad del Servicio

- Controles de la Gestión del Ciclo de Vida de las Claves
  - Generación de las claves de la AC
  - Almacenamiento, copias de seguridad y recuperación de las claves de la AC
  - Distribución de la clave pública de la AC
  - Uso de las claves de la AC y de los certificados de entidad final
  - Destrucción de las claves de la AC
  - Archivo de claves de AC
  - Gestión del ciclo de vida de hardware criptográfico
  - Servicios de gestión de la provisión de la clave del suscriptor

- Controles de la Gestión del Ciclo de Vida de los Certificados
  - Registro de suscriptores
  - Emisión de certificados
  - Renovación de certificados y claves
  - Revocación de certificados
  - Información sobre el estado de los certificados
  - Gestión del ciclo de vida de los DSCF/DCCF/DCCS u otros dispositivos de creación de firma electrónica o sello electrónico

Principio 3: Controles ambientales de la Autoridad de Certificación

- Restringir el acceso lógico y físico a los sistemas de la Autoridad de Certificación y los datos dando sólo acceso a las personas autorizadas
- Mantener la continuidad de las operaciones de gestión de claves y certificados
- Autorizar y ejecutar adecuadamente la operación, el mantenimiento y el desarrollo de los sistemas de la Autoridad de Certificación, con el fin mantener su integridad.

EDUARDO QUINTERO BARONA

Firmado digitalmente por EDUARDO QUINTERO BARONA
Nombre de reconocimiento (DN): c=ES, st=Tres Cantos, Madrid, o=SIGNE S.A., ou=Presidencia, title=Apoderado, sn=QUINTERO BARONA, givenName=EDUARDO, serialNumber=05264367N, cn=EDUARDO QUINTERO BARONA, email=eduardo.quintero@signe.es, 1.3.6.1.4.1.4710.1.3.2=A11029279
Fecha: 2019.04.02 11:21:08 +02'00'

Fdo.: **D. Eduardo Quintero Barona**
Presidente
SIGNE, S.A.