

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

1 de Julio de 2008:

FIRMAPROFESIONAL, S.A., (en adelante Firmaprofesional) opera como un prestador de servicios de certificación (PSC), según la definición de la ley 59/2003, de 19 de diciembre, de firma electrónica, (ley 59/2003) a través de su jerarquía de certificación compuesta por una Autoridad de Certificación (AC) Raíz y una Autoridad de Certificación Delegada o Subordinada (AC Firmaprofesional-CA1), proporcionando los siguientes servicios:

- Registro del suscriptor
- Gestión del ciclo de vida de los certificados electrónicos (emisión, renovación, suspensión, rehabilitación y distribución – utilizando repositorio on-line - )
- Publicación del estado de los certificados mediante lista de certificados revocados (CRL) y On-line Certificate Status Protocol (OCSP)
- Gestión del ciclo de vida de dispositivos seguros de creación de firma (DSCF) como tarjetas de circuito integrado criptográficas o tokens USB criptográficos

Para llevar a cabo la prestación de los servicios de certificación, Firmaprofesional subcontrata tareas como la identificación de los Solicitantes de Certificados a Autoridades de Registro (AR), según permite la ley 59/2003. Estas tareas se desarrollan según lo establecido en las Políticas y Prácticas de Certificación de Firmaprofesional (<http://www.firmaprofesional.com/cps>) y en los acuerdos suscritos entre Firmaprofesional y las AR's.

La Dirección de Firmaprofesional es responsable de establecer y mantener los controles efectivos sobre las operaciones y procedimientos de las AC de Firmaprofesional, 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, en este último caso, si procede) y los controles del Entorno de las AC. Estos controles contienen mecanismos de monitorización, y se toman acciones para corregir las deficiencias encontradas.

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. Aún así, incluso los controles efectivos pueden proporcionar solamente una seguridad razonable en relación con las operaciones, procedimientos y entorno de Firmaprofesional como PSC. Adicionalmente, debido a cambios en las condiciones, la efectividad de los controles puede variar cada cierto tiempo.

Por todo ello, Firmaprofesional, 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 Firmaprofesional)
  - 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 restringida a personal autorizado y la información está protegida de usos no especificados en las prácticas de negocio publicadas de Firmaprofesional
- 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:

- CEN Workshop Agreement 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- ETSI TS 101 456; Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
- ISO 27001 Information technology - Security techniques - Information security management systems – Requirements
- AICPA/CICA WebTrust para Autoridades de Certificación

### **Principio 1: Declaración de Prácticas de Negocio**

Declaración de Prácticas y Políticas de Certificación para AC Raíz y AC Firmaprofesional-CA1 (<http://www.firmaprofesional.com/cps>), incluyendo:

- CPS - Declaración de Prácticas de Certificación
- Política de CERTIFICADO DE COLEGIADO (con o sin DSCF)
- Política de CERTIFICADO DE PERSONA VINCULADA (con o sin DSCF)
- Política de CERTIFICADO DE PERSONA JURÍDICA (con o sin DSCF)
- Política de CERTIFICADO DE FACTURA ELECTRÓNICA (con o sin DSCF)
- Política de CERTIFICADO DE SERVIDOR SEGURO
- Política de CERTIFICADO DE SERVICIO SEGURO
- Política de CERTIFICADO DE FIRMA DE CÓDIGO PERSONAL
- Política de CERTIFICADO DE FIRMA DE CÓDIGO CORPORATIVO
- Política de CERTIFICADO DE FIRMA MOVIL
- Política de SELLADO DE TIEMPO

### **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
  - Suspensión / rehabilitación de certificados
  - Distribución de certificados
  - Información sobre el estado de los certificados
  - Gestión del ciclo de vida del DSCF

### **Principio 3: Controles Generales de la AC**

- Gestión de las Prácticas de Certificación y las Políticas de Certificados
- Gestión de la seguridad
- Clasificación y gestión de activos
- Seguridad del personal
- Seguridad física y del entorno, en concreto del Centro de Proceso de Datos
- Gestión de Operaciones
- Gestión de acceso al sistema
- Desarrollo y mantenimiento de sistemas
- Gestión de la continuidad de negocio
- Seguimiento y cumplimiento de normas, leyes y políticas
- Registro de incidencias

Fdo.: **Alfredo Gosálvez de la Macorra**  
**Director General**  
**FIRMAPROFESIONAL, S.A.**