



Valencia, 17 de Marzo de 2011

Informe de Auditoría Independiente

A la Dirección de la Autoridad de Certificación de EDICOM (ACEDICOM):

Hemos auditado las [Manifestaciones](#) realizadas por los Administradores de la Autoridad de Certificación de EDICOM (en adelante ACEDICOM) en lo relativo a sus servicios como emisora de certificados digitales para la Autoridad de Certificación raíz RootCA y las Autoridades de Certificación Delegadas ACEDICOM01 y ACEDICOM02, durante el periodo comprendido entre el 1 de Marzo de 2010 al 28 de febrero de 2011.

En este periodo, ACEDICOM:

- Divulgó sus prácticas sobre la privacidad de la información y sus prácticas de negocio sobre la gestión del ciclo de vida de los certificados y claves (CPS de ACEDICOM publicadas en su página web corporativa <http://acedicom.edicomgroup.com/es/contenidos/practicasyPolíticas/punto1.htm>)
- Proporcionó tales servicios de acuerdo con sus prácticas manifestadas.
- Mantuvo controles efectivos para suministrar una seguridad razonable de forma que:
 - La información del suscriptor fue autenticada adecuadamente por la actividad de registro, realizada por la propia ACEDICOM;
 - La integridad de las claves y de los certificados gestionados por ACEDICOM fue establecida y protegida a través de sus ciclos de vida;
 - La información del suscriptor y de las partes relacionadas, estuvo restringida a las personas y recursos autorizados y, protegida frente a usos no especificados en las Manifestaciones de prácticas de negocio de ACEDICOM;
 - La continuidad de las operaciones de gestión del ciclo de vida de las claves y de los certificados fue mantenida; y
 - El desarrollo, mantenimiento y operaciones de los sistemas de CA fueron autorizados y realizados adecuadamente para mantener la integridad de los sistemas de CA.

de acuerdo con los requisitos Webtrust que para las Autoridades de Certificación, imponen los Criterios WebTrust de AICPA/CICA y el IACJCE ([Programa Webtrust para Autoridades de Certificación](#)).



La Dirección de ACEDICOM es la responsable de sus Manifestaciones. Nuestra responsabilidad es expresar una opinión sobre de dichas Manifestaciones, basada en nuestra auditoria.

La auditoría se llevó a cabo de acuerdo con los estándares establecidos para la revisión de los Criterios WebTrust para Autoridades de Certificación, fijados por los organismos competentes en esta materia, que son el AICPA/CICA/IACJCE. Dichos estándares nos han requerido planear y realizar la revisión de manera que obtengamos una certeza razonable sobre las manifestaciones de la Dirección y su adecuación. Nuestra auditoría incluyó:

- Obtener una adecuada comprensión de las prácticas sobre la gestión del ciclo de vida de las claves y de los certificados, sobre las medidas de privacidad de la información y de negocio y de los controles sobre la integridad ambos, sobre la autenticidad y privacidad de la información del suscriptor y de las partes relacionadas, sobre la continuidad de las operaciones de gestión del ciclo de vida del certificado y de las claves y, finalmente, sobre el desarrollo, mantenimiento y aseguramiento de la integridad de los sistemas;
- Pruebas selectivas de transacciones ejecutadas de acuerdo con las prácticas divulgadas sobre la gestión del ciclo de vida de los certificados y clave y de privacidad de la información;
- Probar y evaluar de la eficacia operativa de los controles; y
- Realizar otros procedimientos que consideramos necesarios según las circunstancias.

Creemos que nuestra evaluación proporciona una base razonable para soportar nuestra opinión.

En nuestra opinión, las Manifestaciones de los Administradores de ACEDICOM para el periodo del 1 de Marzo de 2010 al 28 de febrero de 2011, en relación con sus Prácticas como Autoridad de Certificación, están adecuadamente formuladas, en todos sus aspectos significativos basándonos en los criterios del programa AICPA/CICA Webtrust para Autoridades de Certificación.

Debido a limitaciones inherentes en los controles del sistema, pueden ocurrir errores o fraude que no hayan podido ser detectados. Adicionalmente, la proyección de cualquier conclusión, basada en nuestros resultados, en periodos futuros al de la fecha de nuestro informe, está sujeta a los siguientes riesgos:

- (1) cambios realizados al sistema o a los controles;
- (2) cambios en los requisitos de proceso;
- (3) cambios requeridos a causa del paso del tiempo; o
- (4) el grado de conformidad con las políticas o los procedimientos pueda alterar la validez de estas conclusiones.

El Sello de WebTrust de Confianza para Autoridades de Certificación que aparece en el Website de ACEDICOM (<http://acedicom.edicomgroup.com>), constituye una representación simbólica del contenido de este informe, y no se pretende, ni debe ser interpretado, para actualizar este informe, ni ser utilizado para otras finalidades.



La eficacia e importancia relativa de controles específicos en ACEDICOM y su efecto sobre las evaluaciones del riesgo de controles para los suscriptores y usuarios, son dependientes de su interacción con los controles y otros factores presentes en las ubicaciones de los suscriptores y de las partes confiantes. No hemos realizado procedimientos para evaluar la efectividad de los controles en las ubicaciones de los suscriptores individuales ni de las partes confiantes.

Este informe no incluye ninguna representación en cuanto a la calidad de los servicios prestados por ACEDICOM, más allá de los criterios de WebTrust para Autoridades de Certificación cubiertos, ni de la idoneidad de los servicios de ACEDICOM para los objetivos concretos del cliente.

A handwritten signature in blue ink, appearing to read 'Juan Jordá Samper', enclosed within a blue oval shape.

Juan Jordá Samper
Auditor de Cuentas
DNB



Manifestaciones de los Administradores sobre sus Prácticas de Negocio y sus Controles en relación con sus operaciones como Autoridad de Certificación durante el periodo que va desde el 1 de Marzo de 2010 al 28 de febrero de 2011.

17 de Marzo de 2011

ACEDICOM opera como una Autoridad de Certificación (AC) raíz mediante ACEDICOM RootCA, y una Autoridad de Certificación Delegada vinculada a la anterior Autoridad de Certificación Raíz mediante ACEDICOM01 y ACEDICOM02, y proporciona los siguientes servicios de Autoridades de Certificación:

- Registro del Subscriptor.
- Emisión de certificados.
- Renovación de certificados.
- Distribución de Certificados.
- Suspensión de Certificados.
- Revocación de Certificados.
- Procesamiento de la información del estado de los Certificados (utilizando un repositorio online).
- Gestión del ciclo de vida de una tarjeta de circuito integrada.

Para llevar a cabo la prestación del servicio de certificación la ACEDICOM hace uso de Autoridades de Registro para la identificación de los solicitantes de certificados, conforme a las normas de la Declaración de Prácticas de Certificación (CPS).

La Dirección de ACEDICOM es responsable de establecer y mantener los controles efectivos sobre las operaciones de las AC de ACEDICOM, incluyendo las Manifestaciones de sus Prácticas de negocio como AC, la Integridad de Servicio (incluidos los controles de la gestión del ciclo de vida de los certificados y de sus claves) y los Controles del Entorno de la AC. Esos 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. Como consecuencia, incluso los controles efectivos pueden proporcionar solamente una seguridad razonable respecto a las operaciones de ACEDICOM como Autoridad de Certificación. Adicionalmente, debido a cambios en las condiciones, la efectividad de los controles puede variar cada cierto tiempo.

La Dirección de ACEDICOM ha evaluado los controles sobre sus operaciones como AC mediante la autoridad de certificación raíz ACEDICOM RootCA y las autoridades de certificación delegadas ACEDICOM01 y ACEDICOM02. En base a dicha evaluación, en opinión de la Dirección de la ACEDICOM, durante el periodo del 1 de Marzo de 2010 al 28 de febrero de 2011:

- Hizo públicas sus Prácticas de Negocio sobre la Gestión del Ciclo de Vida de los certificados y de sus claves, y sus prácticas sobre la privacidad de la información, y suministró tales servicios de acuerdo con las prácticas manifestadas.

- Mantuvo controles efectivos para proporcionar una seguridad razonable de que:
 - La información del suscriptor es autenticada adecuadamente (por la actividad de registro llevada a cabo por ACEDICOM).
 - La integridad de los certificados y de sus claves se estableció y protegió a lo largo de todo sus ciclos de vida.
 - La información de los suscriptores y partes de confianza está restringida a personal autorizado y, protegida de usos no especificados en las manifestaciones de prácticas de negocio de la ACEDICOM.
 - Se mantiene la continuidad de las operaciones a la gestión del ciclo de vida de las claves y certificados; y
 - Las tareas de explotación, mantenimiento y desarrollo de los sistemas de la AC son autorizadas convenientemente y realizadas para mantener la integridad de los mismos.

todo ello de acuerdo con los Criterios AICPA/CICA WebTrust para Autoridades de Certificación, incluyendo los siguientes:

- Declaración de Prácticas de Certificación.
- Políticas de Certificados personales y entidades sobre soporte software, dispositivo seguro centralizado y SmartCard.
- Políticas de Certificados no personales.

<http://acedicom.edicomgroup.com/es/contenidos/practicasyPolíticas/punto1.htm>

Integridad en el Servicio

Controles en 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 la Clave de la AC Destrucción de la clave de la AC Archivo de claves de la AC

Gestión del ciclo de vida de la tarjeta de circuito integrado

Controles en la Gestión del Ciclo de Vida del Certificado

Registro de suscriptores

Renovación de certificados

Emisión de certificados

Distribución de certificados

Revocación de certificados

Procesamiento de la información del estado de los Certificados

Controles de Entorno de la AC

Gestión de las CPS Y CP

Gestión de la seguridad

Clasificación y gestión de Activos

Seguridad del personal

Seguridad física y medioambiental Gestión de operaciones
Gestión de acceso al sistema Sistemas desarrollados y mantenidos Gestión de la continuidad de
negocio Seguimiento y conformidad
Registro de incidencias

Jose Vilata Tamarit
Responsable de Seguridad de la ACEDICOM



EDICOM
Ronda Agustín y Lluís Lantier, 12
46100-Pq. Tec. Pardo VALENCIA
N.I.F. B - 89.490.867