Assurance & Advisory Business Services (AABS)
Torre Picasso
Plaza Pablo Ruiz Picasso
28020 Madrid

Tel: 91 572 72 00
Tel: 91 572 72 70
www.ey.com/es

Informe de Auditoria Independiente

A los Administradores de:

La Autoridad de Certificación EDICOM (ACEDICOM)

Alcance

Hemos examinado las Manifestaciones (http://acedicom.edicomgroup.com/es/contenidos/practicasyPoliticas/punto1.htm) realizadas por los Administradores de la ACEDICOM en su labor como emisora de certificados digitales para la Autoridad de Certificación raíz RootCA y las Autoridades de Certificación Delegadas ACEDICOM01 y ACEDICOM02, durante el período que va desde el 1 de Enero de 2009 al 31 de Diciembre de 2009. En el citado periodo, la ACEDICOM:

- Manifestó 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 (ver CPS de ACEDICOM en http://acedicom.edicomgroup.com/es/contenidos/practicasyPoliticas/punto1.htm) y suministró tales servicios de acuerdo con dichas prácticas manifestadas.
- Mantuvo controles efectivos para suministrar una seguridad razonable de que:
  - La información del suscriptor fue autenticada adecuadamente por la actividad de registro, realizada por la propia ACEDICOM y
  - La integridad de las claves y de los certificados gestionados por la 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 la ACEDICOM.
  - Se mantuvo la continuidad de las operaciones de gestión del ciclo de vida de las claves y de los certificados; y
  - El desarrollo, mantenimiento y operaciones de los sistemas de la ACEDICOM fueron autorizados y realizados adecuadamente para mantener la integridad de los sistemas de la ACEDICOM.

todo ello de acuerdo con los requisitos Webtrust que para las Autoridades de Certificación, imponen los Criterios WebTrust para Autoridades de Certificación de AICPA, la CICA y el IACJCE (Programa Webtrust para Autoridades de Certificación).

Los Administradores de la ACEDICOM son responsables de sus Manifestaciones. Nuestra responsabilidad es expresar una opinión acerca de dichas Manifestaciones, basada en el trabajo que hemos realizado.

Nuestro examen ha sido realizado de acuerdo con las normas específicas de revisión de los Criterios WebTrust para Autoridades de Certificación, establecidas por los organismos competentes en esta materia, que son el AICPA, el CICA y el Instituto de Censores de Jurados de Cuentas de España, e incluye

(1) Obtención y adecuada comprensión sobre:

- Las prácticas de privacidad de la información y de negocio de la gestión del ciclo de vida de las claves, de los certificados, y de los controles sobre la integridad ambos.
- La autenticidad y privacidad de la información del suscriptor y de las partes relacionadas
- La continuidad de las operaciones de gestión del ciclo de vida del certificado y de las claves y,
- El desarrollo, mantenimiento y aseguramiento de la integridad de los sistemas;

(2) Realización de pruebas selectivas sobre transacciones ejecutadas de acuerdo con sus prácticas manifestadas de privacidad de la información y, con sus prácticas de negocio sobre la gestión del ciclo de vida de los certificados y claves

(3) Prueba y evaluación de la eficacia operativa de los controles; y

(4) Realización de otros procedimientos de revisión y evaluación, que hemos considerado necesarios sobre la base de las circunstancias de cada momento.

Entendemos que nuestra evaluación suministra una base suficientemente para soportar razonablemente nuestra opinión.

Opinión del Auditor

En nuestra opinión, para el periodo comprendido entre el 1 de Enero de 2009 al 31 de Diciembre de 2009, las Manifestaciones de los Administradores de ACEDICOM, en relación con sus Prácticas como Autoridad de Certificación, basada en los criterios del programa AICPA/CICA Webtrust para Autoridades de Certificación referidos arriba, están adecuadamente formuladas, en todos sus aspectos significativos.

Limitaciones inherentes

A causa de las limitaciones inherentes en los propios controles del sistema, puede que existan errores o fraudes que no hayan sido detectados. Además, la toma de alguna conclusión en periodos posteriores al de la fecha de nuestro informe, basada en nuestras afirmaciones, están sujetas al riesgo de que se produzcan:

(1) cambios en los controles o en el sistema establecido,

(2) cambios en los requisitos de procesamiento,

(3) cambios requeridos a causa del propio paso del tiempo, o

(4) que el grado de cumplimiento de las políticas o procedimientos puedan alterar la validez de nuestras conclusiones.

Exclusiones

El Sello de Confianza WebTrust para Autoridades de Certificación que aparece en el sitio web de ACEDICOM (http://acedicom.edicomgroup.com/), constituye una representación simbólica de los

contenidos de este informe, y no va dirigido a actualizar este informe, ni debe ser interpretado como tal, ni ser utilizado para otros fines.

La eficacia e importancia relativa de determinados controles de ACEDICOM y su efecto en las evaluaciones del riesgo de control para los suscriptores y usuarios depende de su interacción con los controles y otros factores presentes en las ubicaciones de los subscriptores y de las partes confiantes. No hemos realizado procedimientos para evaluar la efectividad de los controles en las ubicaciones de los subscriptores y de las partes confiantes.

Este informe no incluye ninguna opinión profesional acerca de la calidad de los servicios prestados por la ACEDICOM, ni de su idoneidad para los objetivos concretos de cualquier suscriptor, más allá de los criterios de WebTrust para Autoridades de Certificación cubiertos.

ERNST & YOUNG, S.L.
Auditores de Cuentas

Madrid, España
10 de Enero de 2010

Manuel Giralt Herrero
Socio-Auditor

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 Enero de 2009 al 31 de Diciembre de 2009.

10 de Enero de 2010

La 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 la 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 la 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 la 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 de el 1 de Enero de 2009 al 31 de Diciembre de 2009:

- 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 su 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/practicasyPoliticas/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