LICENCIAMIENTO DE LA AUTORIDAD CERTIFICANTE DE LA OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI).

INFORME DE AUDITORÍA.

22 SEP 2010

1- MARCO INTRODUCTORIO.

La OFICINA NACIONAL DE TECNOLOGÍAS DE INORMACIÓN dependiente de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE LA GESTIÓN PÚBLICA dependiente de la JEFATURA DE GABINETE DE MINISTROS a efecto de iniciar su Licenciamiento solicitó a la máxima autoridad de su jurisdicción la correspondiente autorización para llevar a cabo el procedimiento de rigor.

El proceso enmarcado en la Infraestructura de Firma Digital de la República Argentina se encuentra legalmente regulado por la Ley N° 25.506 de Firma Digital, su Decreto reglamentario N° 2628 del 19 de diciembre de 2002 y la Decisión Administrativa N° 6 del 7 de diciembre de 2007.

La Autoridad Certificante de la ONTI (AC ONTI) tiene por objeto la emisión de certificados de firma digital a favor de personas físicas de Entes Públicos y de personas físicas que realicen trámites con éste, conforme a los términos y condiciones de la política de certificación que es objeto de licenciamiento.

El artículo 20 de la Ley N° 25.506 dispone que para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la referida norma y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones.

El artículo 30 inc. h) de la norma mencionada otorga a la Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina la función de otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación. Dichas exigencias surgen de lo establecido en el Decreto N° 2628/02, reglamentario de la Ley N° 25.506 de Firma Digital y de la Decisión

Administrativa N° 6/07, que establecen y reglamentan el marco normativo aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

La mencionada DA N° 6/07 establece en su Capítulo X –"Normas de Procedimiento", las distintas etapas que conforman el procedimiento de licenciamiento, a saber: Admisibilidad de la solicitud (art. 42), Adecuación de condiciones (art. 43), Dictamen de aptitud (art.44) y Finalización del trámite (art.45).

II- OBJETIVO:

La presente Auditoría se enmarca en lo establecido en la Ley N° 25.506 y sus normas reglamentarias particularmente en la ya mencionada Decisión Administrativa N° 6/7.

Tiene como objetivo principal verificar el cumplimiento de las observaciones informadas el 7 de Septiembre del 2010 para cumplir con los requisitos exigidos para el Licenciamiento lo que implica controlar su infraestructura tecnológica y la legalidad de los documentos que la sustentan.

III.-ALCANCE.

El presente trabajo de Auditoría realizado durante los días 15 de Septiembre al 22 de Septiembre del 2010 abarcó la revisión de los ajustes efectuados a la aplicación, infraestructura y documentación efectuados por la ONTI en virtud de las observaciones del informe presentado el 7 de Septiembre del 2010.

IV.- ACTIVIDADES REALIZADAS

a) Se analizaron los documentos presentados por el auditado.

b) Se auditó el Data Center ubicado en la Secretaría de la Gestión Pública

c) Se efectuaron tareas de relevamiento que incluyeron entrevistas con personal de la ONTI afectado al área de Firma Digital

V. OBSERVACIONES DETECTADAS Y RECOMENDACIONES

Con relación a las observaciones y recomendaciones presentadas oportunamente, se detalla a continuación el estado de cumplimiento de las mismas

a.1) POLÍTICA DE CERTIFICACIÓN:

Observación 1: En el Punto 1.2 se detectó que la dirección del sitio web de publicación de la Política de Certificación no es la correcta.
Recomendación: Proceder a su corrección
Estado de Situación: Cumplido

Observación 2: Se deben actualizar los datos de contacto ya que los mismos son inexactos
Recomendación: Proceder a su actualización.
Estado de Situación: Cumplido

Observación 3: El sitio web de publicación de la Lista de certificados Revocados no es el correcto.
Recomendación: Proceder a su actualización.
Estado de Situación: Cumplido

Observación 4: Punto 6.2.6: se establece que en el caso de los suscriptores, éstos podrán utilizar dispositivos criptográficos para generar sus claves o bien, incorporarlas con posterioridad a su generación.
Recomendación: Este concepto debe ser modificado toda vez que en la Política se definió que el certificado es NO EXPORTABLE.
Estado de Situación: Cumplido

Observación 5: Punto 6.5.2. Calificaciones de Seguridad Computacional. No se expresan cuáles son las calificaciones de seguridad computacional

Recomendación: Expresar las calificaciones de seguridad computacional y se deberá agregar en la nueva Política, de existir, las Certificaciones del hardware empleado.
Estado de Situación: Cumplido

Observación 6: Punto 6.6.3: Calificaciones de seguridad del ciclo de vida. No se encuentra definido el ciclo de vida.
Recomendación: Definir el ciclo de vida.
Estado de Situación: Cumplido

Observación 7: Punto 7.1: Los perfiles de los certificados descritos no se corresponden con los perfiles de los certificados emitidos.
Recomendación: Adecuar la documentación a los perfiles emitidos.
Estado de Situación: Cumplido

Observación 8: No se encuentra detallado el perfil de la AC ONTI
Recomendación: Detallar el perfil de la AC ONTI.
Estado de Situación: Cumplido

a.2) MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN.

Observación 1:.El sitio web de publicación del Manual de Procedimientos no es el correcto.
Recomendación: Actualizar el Sitio de Publicación del Manual de Procedimientos y demás sitios web de acceso a la aplicación.
Estado de Situación: Cumplido

Observación 2:.Punto 1.3 Participantes y aplicabilidad. Este punto no se encuentra totalmente actualizado conforme lo prescripto en la Política de Certificación de Personas Físicas del Sector Público y de particulares que realicen trámites con el Estado.
Recomendación: Actualizar este punto en el mismo sentido que la Política de Certificación.
Estado de Situación: Cumplido

Observación 3:.Con relación al alcance del Manual de Procedimientos se señala que el mismo no resulta en muchos de sus puntos ajustado a lo dispuesto en la Política de Certificación.

Recomendación: Efectuar una revisión general del Manual de Procedimientos a fin de su actualización.

Estado de Situación: Cumplido

Observación 4 :.Con relación a las designaciones de las Autoridades de Registro, Oficiales de Registro, Instructores de Firma Digital y Soportes de Firma Digital se señala que no resulta claro el mecanismo para proceder a sus designación.

Recomendación: Rever los procedimientos para la designación de las personas que van a cumplir las pre citadas funciones minimizando la posibilidad de conflictos.

Estado de Situación: Cumplido

Observación 5: Del análisis del Manual de Procedimientos surge que no se contempló un Plan de Transición hasta hacer efectivamente operativa la AC ONTI. La dependencia auditada informó que se estaba llevando a cabo la última revisión de tal documento.

Recomendación: Finalizar con la revisión del mencionado documento toda vez que resulta necesario contar con el citado Plan antes de proceder al licenciamiento.

Estado de Situación: Cumplido

Observación 6: Del análisis de la Nota de Certificación de Servicios que debe emitir el titular de las áreas de Recursos Humanos o equivalentes no se desprende el tiempo de validez de la misma.

Recomendación: Se sugiere contemplar un plazo máximo de validez que no exceda de 20 días hábiles administrativos a fin de asegurar la actualidad de los datos en ella incluidos.

Estado de Situación: Cumplido

Observación 7: La conservación de la documentación vinculada al proceso de validación de identidad, efectuada por el Oficial de Registro, es responsabilidad de la Autoridad de Registro y no siendo el Oficial de Registro quien debe conservarla durante el período establecido en la Política de Certificación

Recomendación: Debe especificarse claramente el procedimiento de resguardo, lugar y plazo de conservación de la documentación en el Manual de Procedimientos.

Estado de Situación: Cumplido

Observación 8: Con relación a la renovación de los Certificados Digitales se observa que no resulta claro cuando proceder ni el procedimiento para renovarlos.

Recomendación: Debe aclararse y ampliarse el procedimiento de renovación de los Certificados Digitales.

Estado de Situación: Cumplido

Observación 9: No se expresa el procedimiento de revocación de un Certificado Digital en el caso que el suscriptor desee revocarlo, como tampoco que debe hacer si no puede acceder a su clave privada o a su código de revocación.

Recomendación: Debe aclararse y ampliarse el procedimiento de revocación de los Certificados Digitales.

Estado de Situación: Cumplido

Observación 10: No se expresa claramente el procedimiento de verificación del estado de los certificados.

Recomendación: Dada la importancia de poder verificar el estado de los certificados ya que lo contrario podría implicar graves consecuencias legales, debe aclararse y ampliarse este punto.

Estado de Situación: Cumplido

Observación 11: No se establece el procedimiento de uso del servicio OCSP.

Recomendación: como ya se mencionara en la Observación 2 del punto a.6) TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS debe describirse las características de este certificado y el procedimiento para su uso.

Estado de Situación: Cumplido parcialmente, se recomienda ampliar detalles de su utilización

Observación 12 Se solicitó el procedimiento de Control de seguridad del Personal observándose que no resulta completo.

Recomendación: Debe completarse el procedimiento de control de seguridad del personal.

Estado de Situación: Cumplido

Observación 13: Se solicitó el procedimiento de Disponibilidad de la clave pública del Certificador observándose que no resulta completo.

Recomendación: completar el procedimiento de Disponibilidad de la clave pública del Certificador más completo.

Estado de Situación: Cumplido

Observación 14: Se solicitó el procedimiento del Control M de N de Clave Privada observándose que no resulta completo.

Recomendación: completar el procedimiento del Control M de N de Clave Privada más completo.

Estado de Situación: Cumplido, se contempla en los Anexos confidenciales del Manual de Procedimientos

Observación 15: Se solicitó el procedimiento de Recuperación de clave privada observándose que no resulta completo.

Recomendación: completar el procedimiento de Recuperación de clave privada más completo.

Estado de Situación: Cumplido, se contempla en el anexo correspondiente

Observación 16: Se solicitó se completen los siguientes documentos:

- Copia de seguridad de clave privada
- Archivo de clave privada
- Método de activación de claves privadas
- Método de desactivación de claves privadas
- Método de destrucción de claves privadas
- Archivo permanente de clave pública
- Período de uso de clave pública y privada

Estado de Situación: Cumplidos

- Controles de desarrollo de sistemas
- Controles de administración de seguridad
- Controles de seguridad de red
- Procedimientos de cambio de especificaciones
- Procedimientos de publicación y notificación
- Calificaciones de seguridad computacional
- Requisitos Técnicos específicos
- Generación e instalación de datos de activación

Estado de Situación: pendiente de cumplimiento

a.3) PLAN DE CESE DE ACTIVIDADES:

Observación 1: El nombre de la política a la cual hace referencia este documento no es el mismo que el de la Política de Certificación que se propone licenciar.

Recomendación: Adaptar al nombre correcto y corroborar que se mantenga el mismo en todos los documentos.

Estado de Situación: Cumplido

Observación 2: El sitio web de publicación del Plan de Cese es incorrecta.

Recomendación: Proceder a la corrección del sitio web indicado en el Punto 4 del Plan de Cese.

Estado de Situación: Cumplido

a.4) PLAN DE SEGURIDAD.

Observación 1: Punto 4. Organización de Seguridad: En este punto se prevén distintas funciones a cumplir, sin embargo no surge del mismo la definición de roles necesarios para interactuar.

Recomendación: Definir claramente los Roles.

Estado de Situación: Cumplido parcialmente, se recomienda ampliar el detalle de los roles y funciones

Observación 2: Punto 5. Inventario de Activos. No existe un inventario de la información registrada.

Recomendación: Deberá confeccionarse un inventario y mantenerlo actualizado.

Estado de Situación: Cumplido

Observación 3: En el Punto 9. Se estableció como una de las responsabilidades del Responsable de Seguridad Informática la de definir pautas de utilización de Internet para todos los usuarios.

Recomendación: Debería eliminarse esta función ya que este equipo de Auditoría no considera que sea una solución de PKI.

Estado de Situación: Cumplido

Observación 4: el punto Política de Utilización de Controles Criptográficos no se considera claro.

Recomendación: Ampliar la descripción de Política de Utilización de Controles Criptográficos

Estado de Situación: Cumplido

Observación 5: se observo la escasez de detalle y comprensión de los siguientes puntos en el Plan de Seguridad:

- Inventario de Activos del Certificador

Estado de Situación: Cumplido

- Administración de Servidores

Estado de Situación: Pendiente

- Administración de Permisos en AD (ACTIVE DIRECTORY)

Estado de Situación: Cumplido

- Esquema de Red

Estado de Situación: Cumplido

- Administración de Firewall

Estado de Situación: Cumplido

- Monitoreo y Control

Estado de Situación: Cumplido

- Controles de Integridad

Estado de Situación: Pendiente

- Monitoreo de los Servicios de la Infraestructura de Firma Digital

Estado de Situación: Cumplido

- Análisis de Vulnerabilidades

Estado de Situación: Pendiente

- Administración de Logs de Servidores, HSM y Aplicaciones

Estado de Situación: Cumplido

- Administración de Recursos Sensibles

Estado de Situación: Cumplido

a.5) ACUERDO CON SUSCRIPTORES

Observación 1: Este documento reviste gran importancia ya que establece los derechos y garantías de las partes respecto a la solicitud, aceptación y uso de los certificados y a juicio de este equipo de Auditoría tales conceptos no se encuentran resguardados.

Recomendación: Deberá explicitarse con mayor precisión el procedimiento de solicitud de certificado del suscriptor.

Estado de Situación: Cumplido

a.6) TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS

Observación 1: El nombre de la política a la cual hace referencia este documento no es el mismo que el de la Política de Certificación que se propone licenciar.

Recomendación: Adaptar al nombre correcto y corroborar que se mantenga el mismo en todos los documentos.

Estado de Situación: Cumplido

Observación 2: Punto 4.1 Tipos de Certificados. En este punto queda establecido que la AC ONTI emite dos tipos de certificados: para persona física y para OCSPN sin mencionar sus características ni diferencias.

Recomendación: Ampliar la información vinculada a cada tipo de certificado.

Estado de Situación: Cumplido

Observación 3: Punto 4.2. En este punto se enumeran las aplicaciones en las podrán ser utilizados los certificados digitales emitidos en el marco de la Política de Certificación para Personas Físicas del Sector Público, indicando que para mayor detalle se podrá consultar el punto 1.3.4.-Aplicabilidad, de la citada Política.

Sin embargo los documentos deben autoabastecerse por sí mismos para evitar remisiones innecesarias.

Recomendación: Ampliar punto 4.2 Aplicabilidad

Estado de Situación: Cumplido

Observación 4: Punto 6 REVOCACIÓN DE LOS CERTIFICADOS DE NIVEL SUPERIOR. Conforme se desprende del análisis de los documentos que se viene practicando, este punto reviste particular importancia ya que implica evitar riesgos en el compromiso de las claves privadas de las ACs de nivel superior. No surgen claramente los aspectos importantes a tomar en cuenta.
Recomendación: Debería ampliarse este punto sobre todo en cuanto al procedimiento de verificación de la cadena de confianza del certificado.
Estado de Situación: Cumplido

Observación 5: Punto 7 LIMITACIONES DE RESPONSABILIDAD.
Este punto de suma implicancia legal se encuentra poco desarrollado.
Recomendación: Ampliar los conceptos especificando más precisamente los alcances de la Responsabilidad del Certificador y los eximentes de tal responsabilidad legal.
Estado de Situación: Cumplido

Observación 6: Los datos de Contacto no están actualizados.
Recomendación: Actualizar los datos de contacto
Estado de Situación: Cumplido

a.7) POLÍTICA DE PRIVACIDAD DE LA AUTORIDAD CERTIFICANTE ONTI.

Observación 1: Los datos de Contacto no están actualizados.
Recomendación: Actualizar los datos de contacto
Estado de Situación: Cumplido

a.8) PLAN DE CONTINGENCIA.

Observación 1: El Plan de Contingencia analizado no resulta del todo explicativo en cuanto a los procedimientos y métodos de resguardo de la información, servicios que se brindan y servidores.
Recomendación: Analizar la posibilidad de actualizar en su totalidad este Plan para lograr un eficaz Backup de Certificate Services, servidores, máquinas virtuales, etc.

689

692

Estado de Situación: Cumplido parcialmente, se recomienda ampliar la descripción del plan de contingencia

a.9) PLATAFORMA TECNOLÓGICA. OBSERVACIONES RELEVANTES

Observación 1: Este documento no expresa la Infraestructura física y lógica actual de la solución.
Recomendación: Actualizar el documento atento a la criticidad de la Infraestructura que se está auditando.
Estado de Situación: Cumplido

a.10) OBSERVACIONES DE NIVEL GENERAL

Observación 1: A la fecha de la presente Auditoría no se encuentra implementado el sistema de renovación del Certificado Digital.
Recomendación: Si bien, este proceso no es requerido para el lanzamiento de la Autoridad Certificante Licenciada, deberá estar implementado antes de la próxima auditoría
Estado de Situación: Pendiente

Observación 2: A la fecha de la presente Auditoría se constató la falta de procedimientos para implementar el servicio que se pretende brindar.
Recomendación: Elaborar los siguientes procedimientos correspondientes a :

- Roles y Funciones

Estado de Situación: Cumplido parcialmente. Se recomienda ajustar la definición de roles

- Procedimiento de Instalación del HSM
- Procedimiento Retiro de Bienes y su Resguardo

Estado de Situación: Cumplidos

- Procedimientos Backup y Restore

Estado de Situación: Cumplido parcialmente, se recomienda ajustarlo en consecuencia con el plan de contingencia

- Implementación de Infraestructura
- Implementación de la Aplicación
- Control Acceso a Instalaciones Exclusivas
- Procedimiento Declaración de Contingencia
- Resguardo de Auditoría
- Procedimiento Solicitud y Control de Cambios

Estado de Situación: Cumplidos

Observación 3: Al momento de llevarse a cabo la presente Auditoría se constató que si bien la infraestructura tecnológica se encuentra operativa, la misma se encuentra instalada en el Data Center transitorio, incumpliendo con los niveles de seguridad requeridos.
Recomendación: Acelerar los tiempos para cumplir con la instalación de la referida Infraestructura en el Data Center.
Estado de Situación: Cumplido parcialmente, restan los pasos finales de adecuación de la infraestructura en el Data Center

Observación 4: Al requerir el equipo de Auditoría, las Actas de apertura de los dispositivos HSM no fueron presentados
Recomendación: La presentación de las referidas actas deberá efectivizarse a la brevedad.
Estado de Situación: Cumplido

Observación 5: Se ha podido detectar que no se han implementado suficientes herramientas que aseguren la integridad de los archivos instalados e involucrados en la solución de PKI.
Recomendación: Reforzar la seguridad de los archivos instalados.
Estado de Situación: Pendiente

VII.- CONCLUSIÓN

De la evaluación realizada y de los documentos presentados por el organismo, se concluye que la ONTI desarrolló e instaló la plataforma tecnológica necesaria y elaboró políticas, planes y procedimientos requeridos para la puesta en marcha de los servicios de certificación de la AC ONTI.

Si bien existen algunas observaciones pendientes de cumplimiento, fueron subsanadas las observaciones de mayor criticidad señaladas en el informe presentado el 7 de Septiembre del 2010 y por tanto, la ONTI estaría en condiciones de obtener una licencia como certificador licenciado en el marco de la Infraestructura de Firma Digital de la República Argentina creada por Ley N° 25.506, para la Política de Certificación presentada y objeto de la presente evaluación.