Jefatura de Gabinete de Ministros
Secretaria de Gabinete
Subsecretaria de Tecnologias de Gestión
Oficina Nacional de Tecnologías de Información

Ref.: CUDAP EXP – JGM: N° 0029090/2014

BUENOS AIRES, 27 OCTUBRE 2014

ASUNTO: Licenciamiento DIGILOGIX S.A. Informe de Auditoría.

I. INTRODUCCIÓN.

A partir del proceso de licenciamiento iniciado por la empresa DIGILOGIX S.A. mediante la Solicitud de Licencia de Certificador ingresada a la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN dependiente de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, el día 17 de octubre de 2014, se dio inicio a la auditoría de la Autoridad Certificante AC - DIGILOGIX, en el marco de la Infraestructura de Firma Digital de la República Argentina, creada por la Ley de Firma Digital N° 25.506.

La revisión de la documentación presentada por la empresa solicitante tuvo por objetivo determinar el efectivo cumplimiento de las normas vigentes y lo establecido en los documentos elaborados por DIGILOGIX S.A., y que fueran utilizados como base de la presente evaluación.

Como modalidad de trabajo se presenta en primer lugar, el objetivo y alcance de la auditoría realizada a DIGILOGIX S.A., luego se continúa con una breve reseña sobre los aspectos técnicos de la aplicación y de la infraestructura tecnológica sobre la que se prestarán los servicios de certificación y finalmente una sección que resume las actividades de revisión efectuadas y los hallazgos encontrados.

Sin perjuicio de ello corresponde adelantar que no se encontraron observaciones clasificadas como "relevantes" que implicarían un alto grado de exposición para la empresa y un condicionante para la continuidad del proceso de licenciamiento.

No obstante ello resulta procedente formular algunas observaciones "Adicionales" que la Auditoría designada al efecto, consideró de menor criticidad, pero que sí requieren de acciones correctivas, sin que ello obstaculice la continuación del trámite de Licenciamiento de la AC - DIGILOGIX de DIGILOGIX S.A. aludido precedentemente.

El informe incorpora además una serie de sugerencias con el propósito de contribuir a una mejora de los servicios a brindar por la AC - DIGILOGIX en trámite.

En último término, se presenta la conclusión del informe de Auditoría.

II. OBJETIVO.

La presente revisión se enmarca en lo establecido en la Ley de Firma Digital N° 25.506 y sus normas reglamentarias y en particular, en lo establecido en la Decisión Administrativa N° 06/07. Tiene por fin verificar el cumplimiento de los requisitos de licenciamiento previstos en la normativa antes citada, así como la efectiva aplicación de lo indicado en los documentos elaborados y presentados por DIGILOGIX S.A., en el marco de la Infraestructura de Firma Digital de la República Argentina.

III. ALCANCE.

La Auditoría realizada abarcó la revisión de la funcionalidad y de los controles implementados en el sitio principal de la AC - DIGILOGIX, en su servicio de publicación, en el sitio de contingencia y en la Autoridad de Registro Central.

La revisión de la aplicación tuvo un enfoque funcional, no abarcándose la revisión de su código.

IV. DESCRIPCIÓN TÉCNICA.

La infraestructura correspondiente a la AC - DIGILOGIX se basa en la arquitectura Microsoft para PKIs, Windows Certificate Service, con SQL Server, con algunos desarrollos propios que corren como servicios y una aplicación web para la gestión de solicitudes de certificados, renovación y revocación. Se encuentra compuesta por tres capas: capa de presentación, capa de negocios y capa de datos.

El equipamiento la Autoridad Certificante se aloja en un recinto exclusivo dentro del área de máxima seguridad.

La autorización de las funciones críticas del HSM está basada en roles, y cuenta con doble factor de autenticación realizado mediante tokens criptográficos USB y PIN.

El esquema de seguridad se basa en la utilización de firewalls y conexiones de VPN.

V. ACTIVIDADES REALIZADAS.

El equipo de auditores de la Oficina Nacional de Tecnologías de Información de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN dependiente de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS integrado por la Dra. Iris CIDALE y el Lic. Guillermo KOZYRA concurrió a la empresa DIGILOGIX S.A., a fin de proceder a auditar a la AC - DIGILOGIX de DIGILOGIX S.A., ubicada en la calle Defensa Nº 570 Piso 1º de la Ciudad Autónoma de Buenos Aires, donde se llevaron a cabo diversas pruebas y entrevistas con el personal designado por la empresa solicitante, según el documento roles y funciones oportunamente acompañado.

Estuvieron presentes y participaron en el proceso de la auditoría:

Definidores

- Karen Berniger (T)
- Patricio Lopez Seco (T)
- Nicolas Berniger (S)
- Javier Gonzalez (S)

Desarrolladores de software

- Nicolas Berniger (T)
- Ivan Casbarro (S)

Homologadores

- Javier Gonzalez (T)
- Daniel Otero (S)

Administrador de Servidores

- Patricio Lopez Seco (T)
- Javier Gonzalez (S)

Administrador de HSM

- Patricio Lopez Seco (T)
- Javier Gonzalez (S)

Responsable de AR

- Alberto Sperber (T)
- Daniel Trachter (S)
- Mendel Berniger

Oficial de Registro

- Karen Berniger (T)
- Patricio Lopez Seco (S)

Responsable de Comunicaciones

- Patricio Lopez Seco (T)
- Daniel Otero (S)

Responsable de Seguridad

- Daniel Otero (T)
- Patricio Lopez Seco (S)

Administrador de Partición

- Patricio Lopez Seco (T)
- Javier Gonzalez (S)

Mesa de Ayuda

- Nicolas Berniger (T)
- Ivan Casbarro (S)

Las entrevistas realizadas versaron sobre los siguientes temas:

- Apertura de la auditoría y presentación del programa de trabajo.
- Funcionalidad de la aplicación de la AC.
- Plan de Seguridad.
- Configuración de los Firewall.
- Análisis de vulnerabilidades.
- Seguridad Física de la AC.
- Configuración de la AC.
- Protección de recursos sensibles.
- Prueba de los diferentes roles.
- Revisión de los registros de auditoría.
- Plan de contingencia.
- Seguridad Física del sitio de contingencia.
- Responsabilidades de la Autoridad de Registro.
- Funcionamiento y controles de la Autoridad de Registro.
- Seguridad del Personal.

VI. OBSERVACIONES RELEVANTES

No surgen observaciones de carácter relevante que formular.

VII. OBSERVACIONES ADICIONALES.

Observación 1: Del relevamiento efectuado surge que no existe un procedimiento formal de verificación de cumplimiento de certificación de los dispositivos criptográficos a utilizar de acuerdo a lo establecido en la Política de Certificación y Manual de Procedimientos.

Riesgo: Los solicitantes de certificados podrían utilizar dispositivos criptográficos por hardware que no cumplan con la certificación correspondiente.

Recomendación: generar un procedimiento de verificación de certificación de los dispositivos criptográficos y dar a conocer el mismo a través de tutoriales publicados en el sitio web del Certificador.

Observación 2: Del relevamiento efectuado surge que las tareas llevadas a cabo por el operador de Backup son realizados en el nivel 4 de operaciones críticas de la AC.

Riesgo: El operador podría afectar el servicio de la AC o del HSM.

Recomendación: que la mencionada tarea sea realizada en el Nivel 3 correspondiente a las operaciones de la AC y que solo las operaciones críticas de la AC se realicen en el Nivel 4

Observación 3: Del relevamiento surge que la actividad del Oficial de Registro en la aplicación que administra el ciclo de vida de los certificados de firma digital solo es autenticada mediante usuario y clave.

Riesgo: que otro usuario pueda ingresar en la aplicación en nombre del Oficial de Registro.

Recomendación: se sugiere utilizar procesos de ingreso a la aplicación mediante mecanismos más robustos. Por ejemplo utilizando el propio certificado del Oficial de Registro para validar su ingreso.

Observación 4: Del relevamiento surge que durante el proceso de renovación de los certificados de personas jurídicas no se ha tenido en cuenta si los datos validados en primera instancia son los mismos al momento de renovar el certificado.

Riesgo: que pueda emitirse un certificado con datos inválidos o erróneos.

Recomendación: Implementar un procedimientos para mitigar el riesgo, posiblemente con una declaración jurada presentada por la persona que representa a la persona jurídica.

Observación 5: se observa que en las rutinas de Backup a fin de cumplir con la guarda de los datos, no se ha tenido en cuenta los registros de los accesos biométricos.

Riesgo: No se cumple con la normativa vigente.

Recomendación: implementar rutinas de backup teniendo en cuenta los mencionados registros, haciendo guarda de los mismos por 10 años más el período de vigencia de los certificados.

VIII. SUGERENCIAS.

Permitir revocar el certificado de suscriptor con su certificado vigente o mediante un PIN otorgado durante el proceso de emisión del certificado.

Incluir en el Plan de Contingencia solo aquellos riesgos que implican la declaración de la contingencia y adjuntar como Anexo del Manual de Procedimientos de Certificación (Reservado) toda la evaluación de riesgos realizada.

IX. CONCLUSIÓN

De la auditoría llevada a cabo por equipo de auditoría ya mencionado, surgen algunas observaciones adicionales de menor criticidad y algunas sugerencias formuladas con el propósito de contribuir con la mejora de los servicios a brindar por la Autoridad Certificante DIGILOGIX de DIGILOGIX S.A.

Sin perjuicio de ello se considera procedente seguir adelante con el proceso de licenciamiento en trámite.

Abog. Iris D. Cidale
A/C Dirección de Innovación Tecnológica
Oficina Nacional de Tecnologías de Información
Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros