Auditoría General de la Nación

Oficina Nacional de Tecnologías de Información

-ONTI-

Firma Digital en el Estado Argentino

Auditoría General de la Nación
Gerencia de Planificación y Proyectos Especiales
Departamento de Auditoría Informática

Índice

1. OBJETO DE AUDITORÍA 1
2. ALCANCE 1
2.1. Ejecución del Trabajo de Auditoría 1
2.2. Enfoque del Trabajo de Auditoría 2
2.3. Procedimientos de Auditoría 2
3. ACLARACIONES PREVIAS 3
3.1. Principios de la Firma Digital 3
3.2. La Oficina Nacional de Tecnologías de Información 9
3.3. Infraestructura de TI para la Firma Digital 15
4. COMENTARIOS Y OBSERVACIONES 19
5. RECOMENDACIONES 33
6. CONCLUSIONES 36
7. COMUNICACIÓN AL ENTE 38
8. LUGAR Y FECHA 40
9. FIRMA 40
10. ANEXOS 41
ANEXO I – Comentarios del auditado 41
ANEXO II – Análisis de los comentarios del auditado 58

Glosario

AC: Autoridades Certificantes.

AC-Raíz: Autoridad Certificante Raíz.

AR: Autoridad de Registro.

COBIT: *Control Objectives for Information and Related Technology* u Objetivos de Control para Información y Tecnologías Relacionadas. Se utiliza como marco de referencia de buenas prácticas en TI.

Código *Hash*: Los *hash* o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena de caracteres que *solo* puede volverse a crear con esos mismos datos).

CRL: *Certificate Revocation List* o Lista de Certificados Revocados.

CRM: *Customer Relationship Management* o Administrador de Relaciones Comerciales.

DAT: Dirección de Administración Tecnológica, dependiente de la Jefatura de Gabinete de Ministros.

DIT: Dirección de Innovación Tecnológica, dependiente de la ONTI.

DC: *Data Center*, Centro de Procesamiento de Datos o Centro de Cómputos.

DER: Diagrama de Entidad-Relación, modelo de red que describe la distribución de los datos almacenados en una base de datos.

DMZ: *Demilitarized Zone* o Zona Desmilitarizada. Nivel de seguridad que se utiliza habitualmente para ubicar servidores que pueden ser accedidos por usuarios externos (correo electrónico, web, entre otros).

Hash: ver Código *hash*.

Housing: Servicio que consiste en brindar espacio físico en un DC para alojar equipamiento informático de terceros.

HSM: *Hardware Security Module* o Módulo de Seguridad de Hardware. Dispositivo en el que se resguarda la clave privada de AC-ONTI.

ITIL: *Information Technology Infrastructure Library* o Biblioteca de Infraestructura de Tecnologías de Información. Se utiliza como marco de referencia de buenas prácticas en TI.

ONTI: Oficina Nacional de Tecnologías de Información. A la fecha de cierre del período auditado, la ONTI dependía de la Subsecretaría de Tecnologías de Gestión, de la Secretaría de Gabinete, de la Jefatura de Gabinete de Ministros. A la fecha de elaboración de este informe, depende de la Subsecretaría de Tecnología y Ciberseguridad del Ministerio de Modernización (Dto. 13/16, acciones de la Subsecretaría de Tecnología y Ciberseguridad).

OR: Oficial de Registro.

PKI: *Public Key Infrastructure* o Infraestructura de clave pública. Sistema de certificados digitales, entidades de certificación (AC y AC-Raíz) y autoridades de registro (AR) que comprueban y autentican la validez de cada entidad implicada en una transacción electrónica, mediante el uso de la criptografía de clave pública.

TI: Tecnologías de la Información.

Token: Dispositivo criptográfico de conexión USB, similar a las memorias Flash o Pen Drive.

Auditoría General de la Nación

INFORME DE AUDITORIA

Al Señor Ministro de Modernización
Lic. Andrés Horacio Ibarra

En uso de las facultades conferidas por el artículo 118 de la Ley 24.156, la AUDITORÍA GENERAL DE LA NACIÓN procedió a efectuar un examen en la Oficina Nacional de Tecnologías de Información, con el objeto que se detalla en el apartado 1.

1. OBJETO DE AUDITORÍA

Evaluación del estado de las tecnologías de información en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI), referida a Firma Digital en el Estado Argentino.

2. ALCANCE

2.1. Ejecución del Trabajo de Auditoría

El examen fue realizado de conformidad con las Normas de Auditoría Externa (NAE) aprobadas por la AUDITORÍA GENERAL DE LA NACIÓN mediante la Resolución N° 145/93, dictada en virtud de las facultades conferidas por el artículo 119 inciso "d" de la Ley N° 24.156, aplicándose los procedimientos detallados en el punto 2.3.

El inicio de las tareas de auditoría se notifican al organismo el 15/09/14 mediante Nota N° 60/14-AG4. Posteriormente, por su similar N° 106/14-AG4 con fecha de recepción 19 de diciembre de 2014, por cuestiones operativas se informa al auditado de la suspensión provisoria de la auditoría hasta nuevo aviso, cuya reanudación se notifica oportunamente por medio de la nota 96/15-A06, recibida el 27/08/15.

INFORME DE AUDITORIA

En función de estos antecedentes resulta:

Período auditado: 31/07/2014 al 31/07/2015

Las tareas de campo se desarrollaron de septiembre a diciembre de 2015.

2.2. Enfoque del Trabajo de Auditoría

La tarea abarcó la verificación de la gestión de la administración de firma digital por parte de la Dirección de Innovación Tecnológica de la Oficina Nacional de Tecnología de la Información, en lo referente a Firma Digital en el Estado Nacional. Para ello, y a partir de la información obtenida, se identificaron los temas de mayor exposición al riesgo, realizándose pruebas sustantivas y de cumplimiento para el control de los mismos.

La auditoría tuvo en cuenta estándares internacionales establecidos como marco de referencia para buenas prácticas de TI, tales como, COBIT (*Control Objectives for Information Technologies and Related*) versión 4.1, normas ISO 27000 y 27001 e ITIL, entre otras. Estas describen los procedimientos que una organización debe implementar para obtener resultados óptimos en la gestión de la información.

2.3. Procedimientos de Auditoría

En la etapa de análisis se realizaron los siguientes procedimientos:

- Inspección y control del cumplimiento de lo establecido por la Ley 25.506, Decreto 2628/2002, 624/2003 y Resolución 435/2004 de la Jefatura de Gabinete de Ministros.
- Verificación del cumplimiento de las Disposiciones N° 12/2014 y 918/2014 de la Jefatura de Gabinete de Ministros.
- Observación de los procedimientos relativos a la operación y mantenimiento de la infraestructura de PKI.

- Inspección ocular a los Data Centers de la Dirección de Administración Tecnológica de la Jefatura de Gabinete de Ministros y de la AFIP, donde se evaluaron los procedimientos relativos al control de la seguridad física y lógica.
- Verificación de la existencia del procedimiento para la firma del certificado raíz.
- Observación de los procedimientos vinculados al mantenimiento del plan de continuidad de servicios.
- Inspección y observación de los procedimientos de auditoria vinculados a la operación de Firma Digital de las autoridades de certificación.
- Observación del curso de capacitación y actualización para oficiales de registro.
- Recopilación de datos mediante entrevistas mantenidas con los responsables y personal de la Dirección de Innovación Tecnológica y de la Dirección de Administración Tecnológica.
- Entrevistas con los auditores internos responsables de auditar los procedimientos operativos de ONTI.
- Exportación y verificado de estructura de Base de Datos del Sistema de firma digital

3. ACLARACIONES PREVIAS

3.1. Principios de la Firma Digital

La Real Academia Española define como firma al *"Nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido."*[1] Hasta la última década del Siglo XX, el método comúnmente utilizado para asegurar la autoría de un mensaje fue la firma hológrafa.

Mientras la documentación tuvo como soporte excluyente al papel, este paradigma se mantuvo inalterado, pero a partir del surgimiento de las nuevas tecnologías –que

[1] www.rae.es. Vigesimotercera edición. Extraído de http://dle.rae.es/?id=Hyte6ty, el 4/03/2016.

permitieron el uso masivo del correo electrónico y la transferencia de grandes volúmenes de información en soporte digital–, la firma hológrafa resultó inadecuada para asegurar la validez de la información y su autoría. Surgió entonces la necesidad de proporcionar a esta nueva forma de comunicarse con herramientas que brinden seguridad y robustez. Ello derivó en el desarrollo de métodos de validación actualmente conocidos como Firma Digital.

La Ley N° 25.506 define a la Firma Digital como el *"resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La Firma Digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".*

Cualquier otro método que no permita cumplir simultáneamente con los principios de autenticidad (de origen) e integridad (de contenido), no puede ser considerado Firma Digital. Entre ellos se encuentran los siguientes:

- Firma Digitalizada (por ej., una firma escaneada),
- firma electrónica (por ej., contraseñas o *password*, firmas biométricas, etc.),[2]
- documentado encriptado.

Entre otros objetos que se pueden firmar digitalmente se encuentran los siguientes:

- datos enviados a través de un formulario web,
- imágenes, audio o video,
- bases de datos,

[2] De acuerdo al art 5° de la Ley 25.206, *"se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada Firma Digital"*.

- páginas web,
- correos electrónicos,
- código fuente de un programa,
- archivos almacenados en discos rígidos, CDs, o DVDs,
- otros archivos en general.

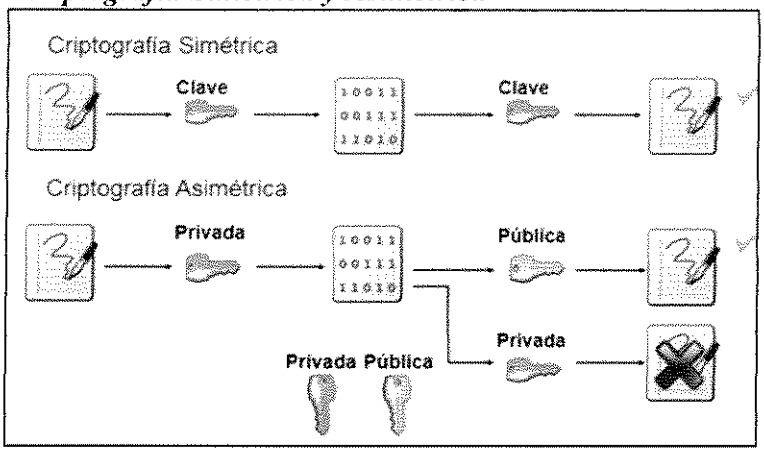
A nivel informático, la Firma Digital es un pequeño archivo denominado "código *hash*", que se genera al aplicar una función *hash* al contenido del documento a ser firmado.[3] El código *hash* es posteriormente encriptado y adjuntado al documento (al igual que lo que sucede con la firma hológrafa, la Firma Digital es un elemento que se *suma* al documento).

Por otra parte, la validez del código *hash* depende de su autenticidad, que reposa en el proceso de encriptación y desencriptación. Este se realiza mediante un proceso conocido como "encriptación pública asimétrica". La asimetría se asocia al hecho de que no se utiliza una sola clave para encriptar y desencriptar, sino una clave para encriptar y una distinta para desencriptar.[4] El proceso requiere que, en su oportunidad, el firmante defina tanto la privada (que permanece exclusivamente en posesión del firmante) como la pública (que se publica en diversos canales de distribución).

[3] Una función *hash* aplicada a un documento genera una cadena de caracteres (o código *hash*) a partir del propio contenido del documento. Las funciones *hash* tienen algunas propiedades importantes que la hacen adecuada para su uso en firmas digitales, a saber: i) no son reversibles, lo que significa que el contenido del documento puede generar un código *hash*, pero a partir de éste no se puede recuperar el contenido del documento, y ii) pequeños cambios en el documento de origen generan grandes cambios en el código *hash*. Así, una misma función hash aplicada dos veces sobre un mismo documento ofrecerá el mismo código *hash* sólo si no hubo modificaciones en el contenido.

[4] La encriptación pública asimétrica se apoya en esquemas de encriptación avanzados y en la capacidad de los sistemas actuales para procesar rápidamente algoritmos matemáticos complejos. La metodología resulta posible gracias a las propiedades de los números primos y la utilización de matemática modular.

Ilustración N° 1
"Criptografía Simétrica y Asimétrica"



Fuente: información provista por el auditado

Para firmar un documento digital, el emisor utiliza su clave privada. Recibido el mensaje, el receptor utiliza la clave pública del emisor para desencriptar el código *hash*. Conforme a los principios de los métodos asimétricos de encriptación, si el código *hash* puede ser desencriptado, entonces se cumplirá la condición de autenticidad (dado que sólo el emisor conoce la clave privada con la cual fue encriptado). Por otra parte, si el código *hash* recibido (que fue generado con el documento de origen) coincide con el código *hash* que se obtiene de aplicar el mismo algoritmo, pero esta vez al documento recibido, entonces también se cumplirá la condición de "integridad".[5]

Ahora bien, para que en este esquema se asegure que el emisor o firmante es quien dice ser –en otras palabras, para asegurar que no hubo sustitución de identidades–, se recurre a un marco institucional que, por medio de certificaciones, valida la identidad de los firmantes.

[5] La Firma Digital no implica garantía de confidencialidad del documento. Para que ello suceda habría que encriptar el documento (en vez de la firma), cuestión que no está contemplada en el proceso de firma.

En efecto, los "Certificados Digitales" son expedidos por entidades que verifican la identidad del firmante mediante la confirmación de datos como DNI, CUIL, CUIT, etc. Sin embargo, para garantizar la autenticidad e integridad del propio Certificado Digital expedido, éste también debe estar firmado digitalmente por la entidad emisora, lo que conduce a la necesidad de que una nueva entidad (jerárquicamente superior), certifique la identidad de aquella. Se genera así una cadena denominada "de confianza".[6]

Tal como sucede en otras partes del mundo, la ley Argentina contempla una serie de instituciones y organismos que procuran afianzar la confiabilidad de los certificados expedidos. Se trata de las denominadas "Autoridades Certificantes" (AC) o Certificadores Licenciados, que emiten los "Certificados de Clave Pública",[7] cuya función principal es vincular la clave pública con un titular determinado. El certificado es emitido por un período determinado. No obstante ello, puede ser revocado antes de su vencimiento en caso que la confidencialidad de la clave privada del titular esté comprometida, se haya detectado falsificación de los datos del titular, o cualquier otra situación que determine un riesgo a la seguridad que debe brindar el sistema.[8]

La entidad de nivel superior encargada de certificar la identidad de las AC, es la Autoridad Certificante Raíz (AC Raíz) o Ente Licenciante, que expide los certificados de clave

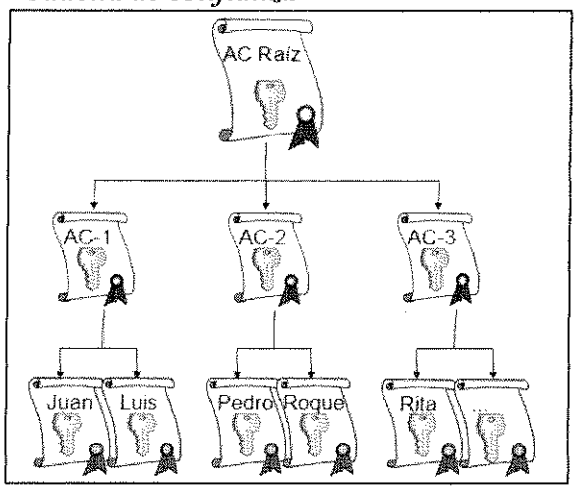
[6] Claramente puede haber una firma de este tipo mediante un acuerdo celebrado entre dos partes, las cuales se obligan a reconocerla según los criterios que los contratantes fijen. Sin embargo, el costo de negociar estos acuerdos es alto entre las partes que no se conocen o que están situados en lugares lejanos y no tienen referencias. La figura del tercero certificante otorga confianza y disminuye los costos de la transacción.

[7] Su nombre obedece al hecho de que el certificado digital contiene la clave pública que el receptor utilizará para validar la firma recibida.

[8] Según la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) los principales factores a tener en cuenta para determinar el grado de Fiabilidad de una Autoridad Certificante deben ser: i) Independencia, es decir, ausencia de interés financiero o de otro tipo de en las transacciones subyacentes; ii) Recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdidas; iii) Aprobación del equipo y programa informático; iv) Mantenimiento de un registro de auditorías realizadas por una entidad independiente; v) Existencia de plan de contingencias para casos de emergencia; vi) Disposiciones para proteger su propia clave privada; vii) Seguridad interna; viii) Capacidad para intercambiar datos con otras AC nacionales e internacionales; ix) Capacidad de revocación de claves en caso de riesgos de seguridad; entre otras.

pública de las AC. Como último paso, la AC Raíz emite su clave pública en un Certificado Digital autofirmado, culminando de esta forma con la verificación de la denominada "Cadena de Confianza".[9]

Ilustración N° 2
"Cadena de confianza"



Fuente: información provista por el auditado

El proceso resulta complejo desde el punto de vista tecnológico y matemático, no así respecto a la interacción con el usuario, que en la práctica es muy baja. La clave privada puede almacenarse utilizando un software especial, o en un dispositivo criptográfico denominado "*Token*" (un pequeño periférico USB similar a las memorias *Flash*). Cuando un emisor desea firmar digitalmente un documento, simplemente selecciona la opción "firmar" en la aplicación utilizada para generar el documento, sea éste un archivo de texto, una presentación de diapositivas, un correo electrónico u otros. Asumiendo que la aplicación sea compatible con el proceso de Firma Digital, ésta ejecuta el procedimiento antes descripto y adjunta la firma al documento. Del lado del receptor, en el caso general

[9] Además de las AC y la AC-R, hay dos figuras que desempeñan tareas operativas. Una de ellas es la Autoridad de Registro (AR), encargada de efectuar la validación de identidad y demás datos de los solicitantes y suscriptores de certificados, y registrar las presentaciones y trámites que les sean formulados. La otra lo constituye el Oficial de Registro (OR), que se encarga de generar y almacenar las claves de registro utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2.

puede observar un ícono que muestra que el documento está firmado y verificado. Si el usuario acciona el ícono, se despliegan los detalles de la firma y sus verificaciones, siempre que el dispositivo cuente con el Certificado de Clave Pública pre-cargado, o este haya sido enviado junto al archivo firmado.

A propósito de la disponibilidad de Certificados de Clave Pública en los dispositivos, de esta parte del proceso participan otras entidades que brindan servicios conexos. Uno de ellos consiste en administrar y distribuir los certificados de clave pública de forma tal que los sistemas operativos cuenten con los certificados de las AC Raíz y las AC intermedias pre-cargados. El servicio permite que el proceso de autenticación sea transparente para el usuario. En caso que la AC-Raíz no recurra a este servicio, el usuario se ve obligado a buscar y descargar el certificado de clave pública desde Internet e instalarlo en su dispositivo, acción que no está libre de riesgos.

El marco institucional que regula, promueve y verifica el proceso de Firma Digital está hoy en poder de la Oficina Nacional de Tecnologías de Información (ONTI), cuyo marco normativo e institucional se desarrolla a continuación.

3.2. La Oficina Nacional de Tecnologías de Información.

En 1998 la Administración Pública Nacional consideró oportuno proceder a la eliminación del uso de papel, debiéndose automatizar los circuitos administrativos e introducir nueva tecnología.[10] A tal fin y por Dto. 427/98 se estableció a nivel nacional el reconocimiento de la Firma Digital con validez jurídica susceptible de la misma garantía de confianza que una firma hológrafa.

[10] Considerandos - Dto. 427/1998.-

INFORME DE AUDITORIA

En 2001 y por Ley 25.506 de alcance federal, se legisló sobre el empleo de la Firma Digital y la Firma Electrónica procediéndose a derogar el Dto. 427/98 por encontrarse subsumido en el objetivo de la ley. A partir de la invitación de adhesión contenida en el artículo 50 de la ley, numerosas provincias llevan a cabo el proceso de implementación de Firma Digital bajo la supervisión de la ONTI.[11]

La propia ley de Firma Digital recomienda al Estado Nacional la utilización de esta tecnología en su ámbito interno y en sus relaciones con los administrados, estableciendo un plazo máximo de cinco años para que la misma sea aplicada a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas del Administración Pública Nacional:

> *"El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156, promoverá el uso masivo de la Firma Digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.*
>
> *En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de Firma Digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156."*

También establece la creación de una Comisión Asesora para la Infraestructura de Firma Digital integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, por un período de cinco años renovables por única vez. La función de la citada Comisión, es evaluar los

[11] Han adherido a la mencionada ley nacional las provincias de La Pampa (Ley Nro. 2.073), Tucumán (Ley Nro. 7.291), Jujuy (Ley Nro. 5.425), Tierra del Fuego (Ley Nro. 633), Formosa (Ley Nro. 1.454), Río Negro (Ley Nro. 12.491), Neuquén (Ley Nro. 2.578), Santa Fe (Ley Nro. 12.491), Buenos Aires (Ley Nro. 13.666), la Ciudad Autónoma de Buenos Aires (Ley Nro. 2.751), Mendoza (Ley Nro. 7.234) y San Luis, que ha aprobado una Ley de Procedimientos Administrativos que admite el uso de medios electrónicos para su tramitación.

estándares tecnológicos, los requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales respecto de los términos de las políticas de certificación, los requerimientos y metodología para el resguardo físico de la información, y cualquier otro tema que le sea requerido por la autoridad de aplicación. Se estipula una frecuencia mínima de reuniones trimestrales.

Como consideraciones fundamentales de la Firma Digital se establece en el art.7° la presunción de autoría: "Se *presume, salvo prueba en contrario, que toda Firma Digital pertenece al titular del certificado digital que permite la verificación de dicha firma*", y por el art. 8° la presunción de integridad: "*Si el resultado de un procedimiento de verificación de una Firma Digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma*".

Legislativamente, la diferencia entre Firma Digital y Firma Electrónica radica en el valor probatorio que tiene cada una. Concordantemente, para la primera se aplica el principio que establece el art. 7° mencionado. Por el contrario, en el supuesto de la firma electrónica, se invierte la carga de la prueba; es decir, en caso de ser desconocida la firma, corresponde a quién invoca su autenticidad acreditar su validez.

El Dto. 2628/02 reglamenta la Ley de Firma Digital, estableciendo una infraestructura regulatoria y creando un Ente Administrador de Firma Digital.[12] Posteriormente, el Dto. 283/03 autoriza a la Oficina Nacional de Tecnologías de Información[13] a emitir certificados digitales, "*con carácter transitorio, y hasta tanto se encuentre la Administración Pública Nacional en condiciones de emitir certificados digitales en los términos previstos por la*

[12] Conforme al Dto. 2628/02, el Ente estaba encargado, entre otros, de: i) otorgar las licencias a los certificadores y supervisar su actividad, ii) dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores, iii) proteger a los usuarios de Firma Digital.

[13] Entonces dependiente de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros.

ley 25.506" y su Dto. Reglamentario. Sin embargo, posteriormente se resuelve disolver al Ente Administrador de Firma Digital creado en la reglamentación, asignándosele competencias de AC-Raíz a la ONTI (Dto. 1028/03).[14]

Más allá de ejercer funciones de AC desde 2003, la Res. 227/10 de la Secretaría de la Gestión Pública otorga a la ONTI la licencia para operar como Certificador Licenciado, es decir, como Autoridad Certificante o AC (art. 2°). Cabe destacar también, que las Autoridades Certificantes cumplen funciones de Autoridad de Registro, que son los organismos encargados de otorgar firmas digitales a los usuarios finales.

La Oficina Nacional de Tecnologías de Información, conforme su estructura organizativa aprobada por Dto. 624/03 y modificada por su similar 1028/03, entiende en: i) la supervisión y ayuda sobre aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica del Sector Público Nacional; ii) mantener actualizados los estándares sobre tecnologías en materia informática y conexos –ETAPS–; iii) brindar asistencia técnica a los organismos nacionales, provinciales o municipales que así lo requieran; iv) mantener el Portal General de Gobierno de la República Argentina y v) definir las normas y procedimientos reglamentarios del régimen de Firma Digital definido

[14] De acuerdo al Dto.1028/2003, y destacándose las funciones inherentes a una AC-Raíz, la ONTI debe: (18) "*Intervenir en el otorgamiento de licencias habilitantes para acreditar a los certificadores de Firma Digital y fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados*"; (19) "*Proponer el rechazo de las solicitudes y la revocación de las licencias de Firma Digital otorgadas a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos en la normativa*"; (21) "*Solicitar los informes de auditoría y realizar inspecciones a los certificadores licenciados de Firma Digital...*". Otras funciones importantes son: (1) "*Entender en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y Firma Digital...*"; y (23) "*Llevar un registro que contenga los domicilios, números telefónicos, direcciones de internet y certificados digitales de los certificadores de Firma Digital licenciados y de aquellos cuyas licencias hayan sido revocadas, y difundir los mencionados datos en forma permanente e ininterrumpida, a través de Internet*". Así mismo, la Dec. Adm. 6/07 (Cap.VIII art. 32°) estipula que el Ente Licenciante deberá realizar "*... auditorías ordinarias a los certificadores y a sus autoridades de registro a fin de verificar el cumplimiento de los requisitos de licenciamiento. Dichas auditorías se realizarán previamente al otorgamiento de la licencia y posteriormente en forma anual*".

en la Ley 25.506, brindar asistencia e impulsar programas a fin de dar cumplimiento a lo establecido en sus art. 47° y 48° (objeto del presente informe), entre otras.

De esta manera, y en el marco de las acciones que normativamente le corresponden, la ONTI ejerce las funciones de Autoridad Certificante (en virtud de las facultades conferidas por la Res. SGP 227/10, simultáneamente con las de AC Raíz de Firma Digital para el Sector Público Nacional (a partir de lo dispuesto por Dto. 1028/03). La misma norma estipula que la ONTI debe actuar como Autoridad Certificante para los organismos del Sector Público Nacional.

En la tabla que se expone a continuación se presentan las distintas denominaciones y organismos que conforman la cadena de confianza.

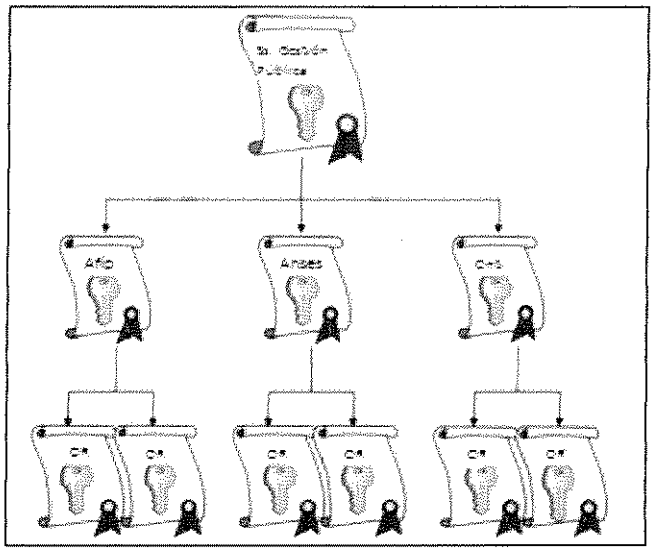
Tabla Nº 1
"Nomenclatura y actores de la cadena de confianza"

Autoridad de Aplicación	**Jefatura de Gabinete de Ministros** *A la fecha de elaboración de este informe, la autoridad de aplicación es el Ministerio de Modernización.*	Ley 25.506, art. 29°
Ente Licenciante *También denominado "Autoridad Certificante Raíz" (AC-Raíz) y, en el marco de la Ley 25.506, "Órgano Técnico de la Autoridad de Aplicación".*	**Ente Administrador** *El Ente fue disuelto y reemplazado su accionar por la* ***ONTI*** *(Dto. 1028/03).*	Dto. 2628/02, art. 11°
Certificador Licenciado *También denominado "Autoridad Certificante" (AC).*	**ONTI** (AC-ONTI) *La AFIP y la ANSES también operan como Certificadores Licenciados.*	Res. SGP 227/10

Fuente: elaboración propia en base a normativa relacionada y página de PKI argentina.

Actualmente existen 3 AC públicas autorizadas a emitir certificados digitales (AFIP, ANSES y ONTI), 84 Autoridades de Registros y 263 Oficiales de Registro. Por su parte, en el sector privado existen cinco AC autorizados por la ONTI para emitir certificados digitales, más uno en proceso de autorización para comenzar a operar a partir de 2016. Todos ellos operan bajo la supervisión de la ONTI, en su carácter de Ente Licenciante.

Ilustración Nº 3
"Cadena de confianza en el Estado Nacional"



Fuente: elaboración propia en base a normativa vigente a la fecha de corte.

3.3. Infraestructura de TI para la Firma Digital

3.3.1. La infraestructura de clave pública o PKI (por las siglas en inglés de *Public Key Infraestructure*) es un sistema de certificados digitales, entidades de certificación y autoridades de registro que comprueban y autentican la validez de cada entidad implicada en una transacción electrónica, mediante el uso de la criptografía de clave pública.[15] Para poder brindar los servicios asociados al PKI, la ONTI cuenta con infraestructura física propia alojada en centros de cómputos de la AFIP (sitio principal de AC Raíz), en la Dirección de Administración Tecnológica –DAT[16]- (sitio principal de AC ONTI) y ANSES (sitio alternativo de AC ONTI) La ONTI recurre a esta facilidad –denominada *housing*- en virtud de la criticidad de algunos de los servicios que brinda, que requieren de centros de cómputos con un alto nivel de seguridad física.

[15] Recuérdese el concepto de "encriptación pública asimétrica", en 3.1. "*Principios de la Firma Digital*"
[16] Otros servicios periféricos (como telefonía IP, Internet, correo electrónico, etc.) son brindados a la ONTI por la DAT, con su propia infraestructura.

INFORME DE AUDITORIA

De acuerdo al Anexo VIII de la Resolución 918/14 de la Jefatura de Gabinete de Ministros la gestión de TI es delegada a la Dirección de Innovación Tecnológica de la ONTI, encargada de implementar, distribuir, mantener y dar soporte a la infraestructura que hace posible la utilización de la Firma Digital en la República Argentina.

Algunas de sus acciones son las siguientes:

- Investigar nuevas tecnologías para la optimización de la gestión de la Administración Pública Nacional y proponer su implementación.
- Intervenir en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento firmado digitalmente y firma digital.
- Intervenir en aquellos aspectos vinculados con la incorporación de la firma digital a los circuitos de información del sector público y con su archivo en medios alternativos al papel.
- Administrar la Autoridad Certificante de Firma Digital para el Sector Público Nacional.

3.3.2. RESERVADO – COLEGIO DE AUDITORES GENERALES – SESIÓN DEL 16/11/16

3.3.3. La gestión de TI que lleva adelante la ONTI y sus dependencias le permiten ofrecer los servicios de PKI que a continuación se detallan, cada uno de los cuales requiere de distintos niveles de redundancia y disponibilidad, según su criticidad:

a) Publicación de Certificado Raíz y Certificado AC-ONTI: Estos certificados deben estar disponibles a fin que las personas interesadas en verificar una firma digital, puedan acceder a la clave pública del firmante. Tal como se expusiera en el apartado 3.1. "Principios de la Firma Digital", uno de los servicios complementarios para la infraestructura de clave pública consiste en administrar y distribuir los certificados de clave pública de forma tal que los sistemas operativos cuenten con los certificados de

las AC Raíz y las AC intermedias pre-cargados.[17] Prescindir de este servicio implicaría que, ante determinadas circunstancias, el usuario deba descargar el certificado requerido desde alguno de los sitios oficiales en los que se encuentra disponible.

- Nivel de disponibilidad necesario: Medio.
- Disponibilidad Recomendable: 95% en horario de oficina[18].

b) Publicación de CRL (Lista de Certificados Revocados): La lista CRL es una base de datos alojada en los servidores de la ONTI, en la que se publica la lista de certificados digitales revocados tanto por AC-ONTI como por AC-Raíz.[19] En oportunidad de proceder a validar una firma digital, esta lista es consultada por las aplicaciones compatibles con el proceso, sin intervención del usuario. La lista debe ser firmada por AC-ONTI cada doce horas, a menos que haya una revocación, lo que obliga al sistema a emitir una CRL de emergencia. La validez de la CRL emitida por AC-Raíz es de seis meses.

- Nivel de disponibilidad necesario para AC-ONTI: Medio.
- Tiempo de indisponibilidad máximo diario para AC-ONTI: 24 horas.
- Nivel de disponibilidad necesario para el sitio de publicación de CRL: Alto.
- Disponibilidad recomendable para el sitio de publicación de CRL: 99% en horario de oficina.

c) Sistema de Registro de Firma Digital: Se trata de otra base de datos de la ONTI en la que se almacena información de las personas que poseen Firma Digital provista por AC-ONTI. La base refleja la validez y estado del certificado ("emitido", "revocado", "en trámite", etc.), que alimenta a la lista CRL mencionada precedentemente. Su

[17] Denominados "*trust services*", son brindados por *Web Trust, American Institute of Certified Public Accountants, Inc. (AICPA)*, entre otras compañías que realizan auditorías y respaldan la distribución de certificados de clave pública.

[18] Estos parámetros de acuerdos de niveles de servicio para data centers y los siguientes se basan en ANSI/BICSI - 002

[19] A la fecha de corte, no había antecedentes de certificados revocados por la AC-Raíz.

criticidad se encuentra ligada fundamentalmente a la baja de certificados digitales, los que deben procesarse con celeridad de manera de impedir que se validen documentos firmados con posterioridad a la baja de la firma, así como permitir que el usuario pueda gestionar dicha baja con rapidez.

- Nivel de disponibilidad necesario: Alto.
- Disponibilidad recomendable: 99% en horario de oficina.

4. COMENTARIOS Y OBSERVACIONES

4.1. *La ONTI opera como Ente Licenciante y como Certificador Licenciado simultáneamente, resultando dicha situación incompatible en virtud de vulnerar el principio de control por oposición de intereses.*

La infraestructura de la Firma Digital de la República Argentina, conforme la normativa en la materia, prevé que el Ente Licenciante (AC-Raíz) realice auditorías operativas a los Certificadores Licenciados (AC) con el objeto de verificar que su funcionamiento se corresponda con las disposiciones vigentes (Dec. Adm. 6/07, Cap. VIII, art 32°).

A la fecha de cierre de los trabajos de campo, y en base a entrevistas y análisis de documentación recabada, se pudo determinar que la Dirección de Innovación Tecnológica dependiente de la ONTI es la encargada de llevar adelante la función citada en el párrafo precedente.

Cabe señalar que por Dto. 1028/03 se disolvió el Ente Administrador de Firma Digital, decretándose que su accionar sería llevado por la Oficina Nacional de Tecnologías de Información. Por otra parte, y mediante Res. N° 227/10 se resuelve en su art. 2°: "*Otorgar la Licencia para operar como Certificador Licenciado a la Oficina Nacional de Tecnologías de Información..., ordenándose su inscripción en el Registro de Certificadores Licenciados*".

De acuerdo a lo expuesto, la Dirección de Innovación desempeña una doble función. Por un lado como personal que cumple tareas delegadas por el Ente Licenciante y por el otro como prestador de servicios y soporte en su rol de Autoridad Certificante. Aun obedeciendo a un mandato legal, esta doble intervención vulnera la independencia que requiere todo control.

4.2. RESERVADO – COLEGIO DE AUDITORES GENERALES – SESIÓN DEL 16/11/16

4.3. *El nivel de seguridad física de la oficina donde opera AR ONTI es inferior al que indica la norma, lo que pone en riesgo la seguridad y confidencialidad de la infraestructura de Firma Digital.*

La Disposición SSTG 01/2015 determina que las Autoridades de Registro deben operar en una oficina que cumpla con una serie requisitos de seguridad, denominados de "Nivel 1". Entre otros requisitos, uno de ellos estipula que se deberá establecer un control y el registro de los ingresos y egresos, e impedir el acceso físico de toda persona ajena a la AR que no se haya registrado previamente".

Durante las tareas de campo se verificó que el ingreso a las oficinas no era controlado ni registrado, ni se encontró evidencias de la existencia de un Libro de Visitas. Esto impide que quede registrado quien visita un área donde se trabaja con información sensible y confidencial.

La falta de registros de ingreso y egreso y controles de Nivel 1 vulnera las normas de seguridad establecidas, lo que pone en riesgo la seguridad y confidencialidad de la infraestructura de Firma Digital.

4.4. *La Dirección de Administración Tecnológica-DAT, no cuenta con soporte energético alternativo que garantice la continuidad del servicio, lo que temporariamente podría afectar la validez de la lista de certificados revocados.*

La Dirección de Administración Tecnológica de la Jefatura de Gabinete de Ministros provee el Data Center para los Equipos de Procesamiento de Datos, Telecomunicaciones, Seguridad Informática y otros Sistemas de Soporte. Este servicio brindado a todas las áreas de la Jefatura de Gabinete de Ministros, tiene por propósito mantener un ambiente de operación apropiado. Así mismo, brinda el servicio de *housing* para los servidores de procesamiento de datos de Firma Digital.

Actualmente, el respaldo energético del Data Center está compuesto por dos equipos de UPSs con una autonomía conjunta de aproximadamente dos horas. Este tiempo resulta suficiente como para realizar un apagado normal de todos los equipos en caso de cortes de energía superiores a las dos horas. Sin embargo, la DAT no cuenta con un soporte energético de instancia superior (grupo electrógeno); debido a restricciones edilicias que dificultan su emplazamiento, según lo manifestado por el auditado.

El riesgo de no contar con el respaldo de un grupo electrógeno es que, ante cortes prolongados de energía, resulta imposible asegurar la continuidad del servicio en los aplicativos de Firma Digital, debiendo recurrirse entonces al sitio alternativo.

El proceso más crítico que se podría afectar tras una interrupción del servicio es el de actualización y publicación de la lista de revocación. En efecto, tras la denuncia de baja de un certificado, la indisponibilidad del servicio antes descripto podría impedir el bloqueo de la firma (lo que puede conducir a tomar por válidas firmas que en ese momento deberían encontrarse bloqueadas).

4.5. *La política de back-up de PKI cuenta con debilidades en sus procedimientos de ejecución, lo que podría afectar la disponibilidad de la información y sus respectivos servicios.*

La Dirección de Innovación Tecnológica cuenta con un documento que detalla los alcances de las políticas y procedimientos para la ejecución de back-ups de resguardo de la base de datos y aplicativos de PKI.

De las tareas de auditoría surge que aquél documento detalla qué bases de datos y aplicativos deben ser resguardados, pero no especifica cuál es el procedimiento para hacerlo.

Además, se ha detectado que no se llevan a cabo procedimientos de pruebas de restauración de back-ups para comprobar la efectividad de los respaldos obtenidos, en caso de tener que responder con ellos ante una contingencia.

Por último se ha podido verificar que los back-up se realizan en discos externos que se guardan en una caja ignifuga ubicada dentro de la propia Dirección de Innovación Tecnológica, no contemplando la guarda de una copia de los back-ups fuera del edificio, de

acuerdo a lo que indican las buenas prácticas de seguridad de la información.

De las observaciones levantadas en los procedimientos de back-ups se desprenden los siguientes riesgos:

- Ante un posible incidente edilicio en las oficinas de ONTI (ejemplo: incendio), no se cuenta con copias alternativas de los resguardos de información para reestablecer el servicio.
- Si no se realizan pruebas de restauración de los back-ups no se puede garantizar un adecuado restablecimiento de la disponibilidad de la información y sus respectivos servicios.
- Si en la documentación de políticas y procedimientos de back-ups no se detallan los instructivos de cómo se deben realizar las tareas de resguardo de información, se depende de personal crítico para la realización de esta tarea.

4.6. *La Dirección de Innovación Tecnológica no cuenta con un plan de contingencia que determine los pasos a seguir ante eventualidades que interrumpan el servicio, lo que podría generar inconvenientes para recuperar el servicio ante incidentes.*

Tanto AC-ONTI como AC-Raíz brindan servicios desde una infraestructura que cuenta con mecanismos de restablecimiento factibles. Sin embargo, los mismos no se encuentran debidamente documentados y formalizados.

Toda organización debe contar con un plan unificado, con instrucciones claras y precisas de cómo proceder ante eventualidades que interrumpan parcial o totalmente el servicio brindado.

La falta de formalización de estos planes puede provocar inconvenientes para recuperar el servicio, y genera dependencia sobre el personal especializado en realizar la tarea.

INFORME DE AUDITORIA

4.7. *La Dirección de Innovación Tecnológica dependiente de la ONTI no cuenta con un sistema de seguimiento de pedidos de soporte, lo que limita la calidad del mantenimiento de los sistemas.*

La Dirección de Innovación Tecnológica de ONTI realiza tareas de soporte al usuario para una serie de sistemas. Entre estos se destacan por un lado el sistema que administra a los usuarios poseedores de una Firma Digital brindada por ONTI, ya sea directamente o a través de sus Autoridades de Registro; y por otro el sistema que utilizan otras Autoridades Certificantes para interactuar con la Autoridad Certificante Raíz.

Cuando los usuarios se encuentran con un inconveniente o deben realizar alguna consulta al soporte técnico, se contactan telefónicamente o vía correo electrónico con la Dirección de Innovación Tecnológica. El número de contacto está asociado a todos los teléfonos del personal asignado a esta tarea, por lo que las llamadas recibidas se derivan a todos ellos en forma simultánea. Los pedidos de asistencia no se registran en ningún medio o sistema, ya sea por parte del agente que recibió el pedido inicialmente o por quien lo reemplace, lo que dificulta su seguimiento, imposibilita la realización de análisis históricos sobre problemas frecuentes y reduce la eficiencia de la tarea de mantenimiento.

Tal y como indican las buenas prácticas, cada pedido de soporte debería registrarse en un sistema que permita identificar en forma unívoca cada solicitud, tanto para hacer un seguimiento del estado de los pendientes, como para servir de base de conocimiento y acelerar así la tarea de los agentes. Podría también ser abierta al usuario con el fin de disminuir la cantidad de contactos entrantes (llamadas y correos electrónicos), para medir el nivel de servicio o conocer los pedidos activos.

El no contar con un sistema de estas características conlleva el riesgo de no resolver el inconveniente de algunos usuarios, o no darle la prioridad adecuada. Asimismo, la falta del

sistema imposibilita o dificulta la distribución correcta de las tareas entre los agentes que corresponda, e impide la identificación de problemas recurrentes a los fines de brindar soluciones más eficientes.

4.8. *La estructura operativa de la Dirección de Innovación Tecnológica, dependiente de la ONTI, no se encuentra formalizada en el organigrama oficial del organismo, y los recursos humanos asignados en esa dirección resultan insuficientes para el cumplimiento de los objetivos del área.*

El organigrama oficial de la Jefatura de Gabinete de Ministros expone su estructura hasta el nivel de Dirección. En consecuencia, la Dirección de Innovación Tecnológica que depende de la ONTI no cuenta con un organigrama formalmente definido, ni se encuentran formalizados los perfiles, las funciones y las responsabilidades del equipo de trabajo que integra dicha dirección.

A partir de entrevistas realizadas durante las tareas de campo se detectó que, si bien se cubren las demandas operativas del área, se produce un solapamiento de roles, funciones y responsabilidades, de lo que se desprende que los recursos humanos que componen el equipo de trabajo son insuficientes para cubrir los roles que demandan las actividades y servicios que brinda la dirección. Cabe destacar que la Ley 25.506, en el artículo 21, inciso v, determina como obligaciones del certificador licenciado, "*Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación*".

La falta de formalización de roles, funciones y responsabilidades por perfil y la insuficiencia de recursos conduce al solapamiento de responsabilidades y de actividades. Esta situación dificulta el cumplimiento de las tareas propias de la oficina, como las relativas al control (al respecto, véase observación siguiente).

INFORME DE AUDITORIA

4.9. *El Ente Licenciante no lleva a cabo con la periodicidad estipulada las auditorías de seguimiento sobre las Autoridades Certificantes y de Registro.*

De acuerdo a lo normado en el artículo 33 de la Ley 25.506, y según lo establecido en la Decisión Administrativa Nro. 927/2014, el Ente Licenciante (AC-Raíz) debe realizar en períodos anuales las auditorías de seguimiento y control sobre las Autoridades Certificantes y sobre las Autoridades de Registro habilitadas y en activa operación.

De las tareas realizadas surge que el Ente Licenciante no cumple con este aspecto de la normativa vigente. Los únicos organismos auditados fueron las Autoridades Certificantes de AFIP y ANSES, auditándolas sólo una vez desde que están operativas (hace 8 años), quedando pendientes las auditorías de todas las Autoridades Certificantes privadas, siendo la más antigua Encode S.A., que opera desde 2012.

La Subsecretaría de Tecnologías de Gestión no cuenta con una estructura operativa técnica propia que le permita cumplir con los procesos de auditoría requeridos en la norma y, a su vez, con las actividades diarias. Por otro lado, de acuerdo a lo manifestado por el auditado, la estructura operativa que tiene a cargo el trabajo de campo en estas auditorías no cuenta con el debido presupuesto a los efectos de cubrir los gastos requeridos para el traslado de los recursos asignados a estas auditorías.

La falta de auditorías de seguimiento sobre las Autoridades Certificantes y de Registro operativas debilita el control que la ONTI, en su carácter de Ente Licenciante, debe ejercer sobre las entidades que certifica.

4.10. *No se encuentran formalizados los acuerdos de niveles de servicio entre los organismos que brindan soporte a la plataforma tecnológica de Firma Digital y a la ONTI.*

La infraestructura tecnológica que brinda servicios al entorno operativo de Firma Digital, tanto a nivel del Ente Licenciante (AC-Raíz) como a nivel de la Certificador Licenciado (AC-ONTI) se encuentra implementada en modalidad *housing* en los siguientes organismos:

- ANSES para la contingencia de AC-ONTI
- AFIP para el sitio principal de AC-Raíz
- DAT - Dirección de Administración Tecnológica – para el soporte de telecomunicaciones, energía y refrigeración para el HSM principal AC-ONTI.

El servicio de *housing* que estos organismos brindan a la plataforma de Firma Digital, tiene por objetivo principal disponer dentro de sus propios Data Center de un espacio en el cual se alojan los servidores, los equipos de comunicaciones y redes, y equipos de seguridad informática propiedad de ONTI. Este cofre o espacio se ofrece garantizando el cumplimiento de las normas de seguridad física que debe tener un Data Center de alta disponibilidad de servicio.

A partir de entrevistas realizadas y de las inspecciones realizadas a los Data Center pertinentes, se pudo constatar que, si bien las condiciones generales del servicio de *housing* se cumplen razonablemente, los servicios no se encuentran formalizados en documentos y/o actas donde queden asentados los acuerdos de niveles de servicios ofrecidos por los organismos prestadores del servicio, y los requeridos por la ONTI, para garantizar la demanda de disponibilidad tecnológica que necesitan los procesos operativos de Firma Digital.

De este modo no se cuenta con una herramienta que permita a ambas partes medir el nivel de calidad del servicio en aspectos tales como tiempo de respuesta, disponibilidad horaria,

documentación disponible, personal asignado al servicio, etc., como indican las mejores prácticas al respecto, y lo que deriva en una administración informal del servicio de locación de los activos tecnológicos de la ONTI.

4.11. *No se cuenta con una planificación y programación formalizando las reuniones periódicas para el seguimiento y control de los productos y servicios provistos por el proveedor de desarrollo de software, lo que no permite cumplir adecuadamente con el proceso de Gestión de Proveedores de TI, según lo establecen las buenas prácticas relativas a gestión de rendimiento de servicios.*

En el marco del servicio provisto por DATCO S.A., orientado a brindar soporte tecnológico a los procesos de Firma Digital (Pliego de Bases y Condiciones Particulares, Expediente Nro. CUDAP: EXP-JGM 12169/2014 del 14-7-2014), es responsabilidad de la Dirección de Innovación Tecnológica de ONTI realizar el seguimiento y control de los servicios y productos provistos.

A partir de las entrevistas realizadas y en función del análisis y revisión de la documentación provista por el auditado, se ha detectado que a nivel operativo, el seguimiento sobre los niveles y performance de los servicios se realiza en forma continua. No obstante, dentro del esquema de trabajo no se encuentran previstas reuniones periódicas de seguimiento a nivel coordinación general, cuyo objetivo sea evaluar la performance y la calidad del servicio y el estado actual de las carteras de trabajo, para medir los grados de avances de los requerimientos de ONTI sobre el aplicativo, tomar acciones correctivas ante los desvíos detectados y obtener nuevos compromisos formales de parte del proveedor.

La falta de reuniones periódicas de seguimiento con el proveedor a nivel de coordinación general, no permiten cumplir adecuadamente con el proceso de Gestión de Proveedores de TI, según lo establecen las buenas prácticas relativas a gestión de rendimiento de servicios.

4.12. *No se realizan las reuniones trimestrales de Comisión Asesora para la Infraestructura de Firma Digital, orientadas a generar recomendaciones de mejoras en base a estándares tecnológicos.*

Según lo establecido en la Ley 25.506, en el Decreto 2628/2002 y en la Resolución 435/2004, regularmente debe reunirse una "Comisión Asesora para la Infraestructura de Firma Digital", conformada por especialistas en la materia.

El objetivo principal de dichas reuniones es generar y emitir recomendaciones por iniciativa propia o a solicitud de la Autoridad de Aplicación de la Ley 25.506 (Ley de Firma Digital), en materia de estándares tecnológicos, sistema de auditoría, requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados y otros aspectos que le sean requeridos.

Del relevamiento realizado surge que la Comisión Asesora para la Infraestructura ha sido designada por el Poder Ejecutivo. No obstante ello, se incumple con lo establecido normativamente respecto de la periodicidad de las reuniones. Según la ley de Firma Digital, la comisión debe reunirse al menos una vez cada 3 meses. Sin embargo, el trabajo de campo realizado señala que sólo se reunieron una vez.

Al no realizarse las reuniones de Comisión Asesora para la Infraestructura, se carece de los productos y herramientas que dicha Comisión debe generar en términos de soporte y asesoramiento a los titulares o potenciales titulares de certificados.

4.13. *Se encuentran desactualizados los procedimientos y guías técnicas sobre la plataforma e infraestructura tecnológica de Firma Digital utilizadas por el personal de soporte de la ONTI, lo que genera dependencia de personal clave.*

Los documentos que describen los procedimientos técnicos de la ONTI sobre la plataforma e infraestructura tecnológica de Firma Digital fueron generados en septiembre de 2010, y

no se cuenta con versiones actualizadas a la fecha de cierre de esta auditoría. Dichos documentos abarcan los siguientes temas:

- Plataforma Tecnológica: Requerimientos a nivel de negocio, de usuario, de seguridad y de operación. Infraestructura de la solución PKI 2.0, Inventario de equipos, Arquitectura de procesadores, Configuración del Software, Arquitectura de Red, Bases de Datos (Diccionario de datos, DER, etc.)
- Plan de Contingencia y Procedimiento de la Declaración de Contingencia
- Documentación para la instalación de servidores y aplicativos
- Documentación sobre los aplicativos provistos por la empresa DATCO para el soporte de los procesos y procedimientos de Firma Digital.

A partir de entrevistas realizadas y del análisis y revisión de la documentación provista por el auditado, se concluye que los documentos son suficientes y cuentan con un alcance adecuado en relación a los aspectos que conforman la plataforma e infraestructura tecnológica de Firma Digital. No obstante, la brecha existente entre la documentación vigente y la infraestructura actualmente instalada no permite dar un adecuado soporte al personal técnico a cargo de la administración de la plataforma tecnológica de Firma Digital. Esto genera una dependencia de personal clave para la realización de ciertas tareas, dificultando que las mismas sean llevadas a cabo en su ausencia, o ante la incorporación de personal.

4.14. *Los legajos de las Autoridades Certificantes no cuentan con un soporte digital adecuado para realizar consultas, revisiones y actualizaciones.*

En el marco de los procedimientos administrativos de la Subsecretaría de Tecnologías de Gestión, los legajos de las Autoridades Certificantes que administra la Dirección de Innovación Tecnológica se gestionan en formato impreso.

INFORME DE AUDITORIA

Durante las tareas de campo se relevaron legajos correspondientes a habilitación y seguimiento de Autoridades Certificantes. Como parte del circuito administrativo los legajos pasan por diferentes sectores, tanto dentro de la Subsecretaria de Tecnologías de Gestión como de la Autoridad Certificante pertinente. Ante cada corrección requerida en la cadena de verificación documental, el procedimiento contempla la reimpresión completa del documento antecedente, lo que deriva en una multiplicación exponencial de documentos, hecho que se pudo constatar mediante inspección ocular

Cabe señalar que la Ley de Firma Digital establece en su Artículo 48 que:
"El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156, promoverá el uso masivo de la Firma Digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.".

Y luego agrega que: *"En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de Firma Digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156."*

La gestión de documentos actual deriva en legajos voluminosos, lo que además de dificultar su acceso, eleva los costos de archivo y gestión documental. Si bien se cuenta con los documentos escaneados, su accesibilidad es poco eficiente y redunda en una contradicción entre la realidad de los procedimientos administrativos de la oficina y el principio de despapelización que da impulso al desarrollo de la Firma Digital.

4.15. *El Sistema de Registro de Firma Digital en el que se registra la información personal de los subscriptores de Firma Digital de AC-ONTI, admite que puedan no cargarse datos que son considerados imprescindibles, lo que atenta contra la completitud de la información allí almacenada.*

En la base de datos de AC-ONTI se almacenan los datos personales de todos los subscriptores a su servicio de Firma Digital. Muchos de estos datos deben estar almacenados de forma obligatoria. Sin embargo, estos campos están configurados de forma tal que pueden quedar vacíos. Durante las tareas de campo, en una inspección a una copia de respaldo de la base de datos activa, se pudo comprobar que utilizando esta debilidad de diseño, una serie de subscriptores no contaban con uno o más de estos datos obligatorios (por ejemplo CUIT), a pesar de que estos datos son confirmados personalmente ante la dirección de innovación tecnológica previo a la emisión del certificado.

Por otra parte, hay campos que utilizan formatos de datos ineficientes o no recomendados por las buenas prácticas de diseño de bases de datos.

La base de datos debe contar con un diseño tal que impida la carga de datos de formato distinto al esperado, y que exija la carga de datos que son considerados imprescindibles.

Estas fallas de diseño acarrean el riesgo de no contar con información fidedigna en el momento de requerirse.

5. RECOMENDACIONES

La secuencia de las recomendaciones aquí expuestas sigue el mismo orden que las observaciones del capítulo precedente.

5.1. La Autoridad de Aplicación debe arbitrar los medios técnicos y presupuestarios para que el Ente Certificante cuente con su propio soporte técnico independiente de la AC-ONTI, a fin de llevar a cabo las auditorías de validación y habilitación de nuevas Autoridades Certificantes de acuerdo a lo establecido en la norma.

5.2. RESERVADO – COLEGIO DE AUDITORES GENERALES – SESIÓN DEL 16/11/16

5.3. La ONTI debe arbitrar los medios necesarios para acondicionar la oficina donde opera la Autoridad de Registro AR ONTI, de manera tal de alinearla a lo establecido por la Disposición SSTG 01/2015.

5.4. La ONTI debe gestionar la implementación de un sistema de suministro energético alternativo que permita garantizar la continuidad del servicio.

5.5. La ONTI debe: i) actualizar el documento de políticas y procedimientos de back-ups, incorporando un instructivo detallado de las tareas a realizar al respecto, ii) formalizar las tareas de pruebas de restauración de las copias de seguridad que se realizan (de acuerdo a lo especificado en las buenas prácticas se sugiere realizar como mínimo dos pruebas de restauración al año), iii) arbitrar los medios para guardar una copia de la información de PKI fuera del edificio de la ONTI.

5.6. La ONTI debe gestionar la redacción y aprobación de un procedimiento que describa detalladamente las acciones o pasos a seguir por cada uno de los integrantes, en caso de fallas que provoquen una indisponibilidad de servicio.

5.7. La ONTI debe gestionar la implementación de un sistema de tipo CRM con el fin de poder dar seguimiento, priorización y registro a los pedidos de asistencia técnica de los usuarios.

5.8. La ONTI debe formalizar la estructura operativa de la Dirección, las funciones y responsabilidades por roles. Dimensionar a la dirección para que pueda cumplir con sus objetivos y funciones de forma eficiente.

5.9. La Autoridad de Aplicación debe arbitrar los medios administrativos, técnicos y presupuestarios para cumplir adecuadamente con las auditorías anuales de seguimiento, según lo establecido en la norma.

5.10. En tanto responsable de la infraestructura tecnológica de Firma Digital, la ONTI debe formalizar acuerdos de niveles de servicio con los organismos prestadores del servicio de *housing*.

5.11. En el marco de la gestión de rendimiento del servicio provisto por DATCO, la ONTI debe formalizar una agenda de reuniones periódicas de seguimiento a nivel de gestión o coordinación general. Estas reuniones se deben llevar a cabo con una periodicidad suficiente para asegurar que se cumplen los niveles de servicio acordados.

5.12. La Comisión Asesora debe formalizar la programación anual de reuniones delineando los respectivos temarios y objetivos a cumplir en cada una de ellas.

5.13. La ONTI debe proceder a actualizar los documentos oficiales de guías y procedimientos técnicos de la plataforma tecnológica de Firma Digital

5.14. La ONTI debe tender a implementar un sistema dedicado a la gestión documental, que permita indexar y almacenar los documentos en una base de datos de legajos de ágil acceso. Haciendo uso de las herramientas propias de la dirección, debe impulsar medidas que optimicen los procesos administrativos inherentes a la Firma Digital, cuyo objetivo

principal es la despapelización, de forma tal que éste no genere el volumen actual de papel, sin dejar de cumplir con la legislación vigente.

5.15. La ONTI debe rediseñar la base de datos de la aplicación que registra y almacena los datos de los usuarios de AC-ONTI, a fin que se reflejen los datos considerados obligatorios., la optimización de tipos de datos, y las buenas prácticas de diseño y uso de tipos de datos definidas por el desarrollador del motor de base de datos.

6. CONCLUSIONES

La validez jurídica de la Firma Digital y su equivalencia con la firma hológrafa fue establecida por el Dto. 427/98. La ley N° 25.506 de "Firma Digital" (que deroga al Dto. 427/98 por subsumirlo en su objetivo), la define como el "*resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La Firma Digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma*".

Cabe destacar que la ley 25.506 de Firma Digital promueve su uso sin establecer la obligación de su cumplimiento.[20] Y si bien la Dirección de Innovación Tecnológica con frecuencia brinda cursos para promover la Firma Digital, no se ha logrado su uso masivo en el ámbito de la Administración Pública Nacional. En efecto, al cierre de tareas de campo subsisten expedientes en soporte papel, lo que trae aparejado un elevado costo económico en concepto de almacenamiento. En ese orden, la ley 19.549 de Procedimientos

[20] Excepto para las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156.

Administrativos todavía mantiene vigente en su art. 8° "el formalismo del acto administrativo": *"...El acto administrativo se manifestará expresamente y por escrito..."*,

Sin perjuicio de la cuestión normativa, y más allá de los fundamentos matemáticos que hacen posible la utilización de esta tecnología, el sistema requiere asegurar la identidad del firmante. Para ello se recurre a un marco institucional formal que emite "Certificados Digitales" con el fin de validar la identidad de una persona mediante la confirmación de sus datos. Sin embargo, para garantizar la autenticidad e integridad del propio Certificado Digital expedido, éste también debe estar firmado (digitalmente) por la entidad emisora. Ello conduce a la necesidad de que una segunda entidad jerárquicamente superior certifique la identidad de la primera.

En el marco de la "cadena de confianza" anteriormente descripta, se autoriza a la Oficina Nacional de Tecnologías de Información a ejercer funciones de Autoridad Certificante; esto es, con potestad para expedir Certificados Digitales (Dto. 283/03). Poco tiempo después se le asignan también competencias de AC-Raíz; es decir, como entidad de nivel superior encargada de certificar y auditar a las Autoridades Certificantes (Dto. 1028/03). De este modo, dos funciones contrapuestas son ejercidas por la propia ONTI, lo que deriva en una vulneración del principio de control por oposición de intereses, resultando ser éste aspecto el que da origen a una parte significativa de las observaciones expuestas en el presente informe de auditoría.

Relacionado con la calidad y continuidad del servicio brindado por la ONTI, no se tuvieron a la vista los acuerdos de niveles de servicios formalizados con los organismos que brindan soporte a la plataforma tecnológica de Firma Digital, ni se realizan tareas de seguimiento y control periódico a la empresa que provee soluciones informáticas para la Oficina. El riesgo consecuente no es adecuadamente administrado: la ONTI carece de un plan de contingencia que determine los pasos a seguir ante una eventual caída de servicio. Otra de

las falencias encontradas es la falta de un sistema de registro y seguimiento de pedidos de soporte, lo que al tiempo de poner en riesgo la resolución de las solicitudes realizadas por los usuarios, desaprovecha la posibilidad de realizar una adecuada gestión del conocimiento. Con el objeto de evaluar y perfeccionar el sistema en su conjunto, la ley N° 25.506 establece la creación de una "Comisión Asesora para la Infraestructura de Firma Digital", que debe reunirse como mínimo cada 3 meses. Del relevamiento realizado surge que el Poder Ejecutivo designó a sus integrantes, pero la Comisión solo se reunió una vez.

Por último, durante los trabajos de campo pudo relevarse que los recursos físicos y humanos asignados a las áreas vinculadas con Firma Digital resultan insuficientes para cumplir con lo que la normativa establece. A modo de ejemplo, las auditorías sobre las Autoridades Certificantes y de Registro no se realizan con la periodicidad estipulada; o también, que el personal de la Dirección de Innovación Tecnológica que opera para la Autoridad Certificante ONTI, es el mismo que controla su gestión, doble intervención que pone en riesgo la independencia del control realizado.

En el contexto actual, la Firma Digital constituye una herramienta de importancia para propender a una eficiente gestión documental en el ámbito de la Administración Pública Nacional. Si bien la ONTI cumple razonablemente con su tarea respecto a la gestión de firma digital, resulta necesario compatibilizar el marco normativo institucional y los recursos a ella asignados, con la importancia que la Oficina reviste en su carácter de entidad certificadora de mayor nivel de la Argentina; en rigor, como promotora del sistema y garante de la confianza en él depositado.

7. COMUNICACIÓN AL ENTE

Por nota N° 53/16-A06 la AGN remite el proyecto de informe al Ministerio de Modernización, quien lo recibe con fecha 30 de junio de 2016. El 28 de julio de 2016

dicho Ministerio hace llegar sus comentarios por medio de la nota N° IF-2016-00396107-APN-MM, que ingresa a la AGN el 3 de marzo del corriente.

En los ANEXOS I y II al presente informe, en orden simultaneo, se presentan tanto la respuesta del organismo auditado como los comentarios de la AGN.

Como resultado del análisis realizado, a los fines de dar mayor precisión al informe, se aceptan las modificaciones propuestas al punto 3.3 de las Aclaraciones Previas, "*Infraestructura de TI para la Firma Digital*", mediante el reemplazo del texto:

" *Instalación, mantenimiento y actualización de los servidores involucrados en el proceso de Firma Digital, para AC-ONTI y AC-Raíz.*
- *Capacitación y soporte de primer nivel a los subscriptores directos de Firma Digital de AC-ONTI, a los Oficiales de Registro de AC-ONTI, y a los encargados de otras AC dependientes de AC-RAIZ.*
- *Escalamiento y seguimiento de errores de sistema a sus proveedores.*
- *Aseguramiento de la disponibilidad de los servicios de publicación de certificados.*
- *Administración de bajas de certificados.*
- *Aseguramiento de la seguridad y confidencialidad de los certificados.",*

por:

" *Investigar nuevas tecnologías para la optimización de la gestión de la Administración Pública Nacional y proponer su implementación.*
- *Intervenir en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento firmado digitalmente y firma digital.*
- *Intervenir en aquellos aspectos vinculados con la incorporación de la firma digital a los circuitos de información del sector público y con su archivo en medios alternativos al papel.*

- *Administrar la Autoridad Certificante de Firma Digital para el Sector Público Nacional."*

Asimismo, a fin de perfeccionar el texto de la observación N° 4.2, se acepta la sugerencia realizada por el auditado, sin que ello implique modificar la observación realizada.

8. LUGAR Y FECHA

BUENOS AIRES, Setiembre de 2016

9. FIRMA

Lic. Martín Rubione
Jefe de Departamento de Auditoria Informática
AUDITORÍA GENERAL DE LA NACIÓN

Dr. GERARDO G. PRATAVIERA
Gerente de Planificación
y Proyectos Especiales
AUDITORÍA GENERAL DE LA NACION

10. ANEXOS

ANEXO I – Comentarios del auditado

A continuación se exponen los comentarios del auditado sobre cada una de las observaciones señaladas.

Auditoría General de la Nación

INFORME DE AUDITORIA

"2016 - AÑO DEL BICENTENARIO DE LA DECLARACIÓN DE LA INDEPENDENCIA NACIONAL"

Ministerio de Modernización

Ref: CUDAP: EXP-S01: 0292293/2016

Asunto: CUDAP: EXP-S01: 0292293/2016 – ACLARACIONES AL INFORME DE LA AUDITORÍA GENERAL DE LA NACIÓN DE FECHA 28/06/2016.

SEÑORA AUDITORA:

Ingresan las actuaciones de referencia al MINISTERIO DE MODERNIZACIÓN, a mi cargo, por la que tramita la copia del "PROYECTO DE INFORME DE AUDITORÍA INFORMÁTICA" sobre la "EVALUACIÓN DE LA TECNOLOGÍA INFORMÁTICA EN LA ORCINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI), REFERIDA A FIRMA DIGITAL EN EL ESTADO ARGENTINO".

Asimismo, mediante Nota Nº 53/16-A06 – Ref.: ACT. Nº 383/14-AGN, de fecha 28 de junio de 2016, ingresada a la mesa de entradas del MINISTERIO DE MODERNIZACIÓN con fecha 30 de junio de 2016, la Auditora General de la Nación, Cdora. Vilma N. CASTILLO, remite las actuaciones de la referencia, acompañando el "Proyecto de Informe de Auditoría", que consta de CUARENTA Y UN (41) fojas. Al respecto, se informa que se ha incurrido en un error material toda vez que a fs. 1 se consignó "se adjunta informe en 45 fojas".

Dicho informe, a fs. 6/7 del punto 2.1 *"Ejecución del Trabajo de Auditoría"* indica que: *"El inicio de las tareas de auditoría se notificaron al organismo el 15/09/14 mediante Nota Nº 60/14-AG4. Posteriormente, por su similar Nº 106/14-AG4 de fecha 16 de diciembre de 2014, por cuestiones operativas se informa al auditado de la suspensión provisoria de la auditoría hasta nuevo aviso, cuya reanudación se notifica oportunamente por medio de la nota 95/15-A06, recibida el 27/08/15"*. Por último detalla que la auditoría alcanzó el período comprendido entre el 31/07/2014 y el 31/02/2015, teniendo en cuenta que *"...las tareas de campo se desarrollaron de septiembre a diciembre de 2015"*.

En dicho marco, durante los meses de septiembre a diciembre de 2015, funcionarios de la AGN concurrieron a las oficinas de la entonces DIRECCIÓN DE INNOVACIÓN TECNOLÓGICA perteneciente a la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS, y realizaron diversos procesos vinculados a las tareas propias de la revisión sobre la base de una serie de informes y documentos que fueron entregados oportunamente.

En este sentido, se deja sentado que esta instancia puso a disposición de los funcionarios de la AGN la totalidad de la documentación solicitada que obraba en su poder.

INFORME DE AUDITORIA

Con relación al Proyecto de Informe, y a mayor abundamiento, está compuesto de DIEZ (10) apartados, que a continuación se procederá a detallar. El primer apartado incluye el ***"Objeto de la Auditoría"***, mientras que su segundo apartado delimita su ***"Alcance"***. El tercer apartado denominado ***"Aclaraciones Previas"*** contiene un extenso análisis del marco legal e institucional aplicable a la firma digital, una revisión de los aspectos más relevantes, tales como la terminología, la organización de la infraestructura de firma digital, estructura del organismo y competencias, entre otros. El cuarto apartado describe los ***"Comentarios y Observaciones"*** vinculados a cada objetivo de control, mientras que el quinto apartado, detalla las ***"Recomendaciones"*** continuando el orden de las observaciones del apartado anterior. Por último, los apartados ocho y nueve corresponden a ***"Lugar y Fecha"*** y ***"Firma"*** respectivamente, y se deja constancia que los apartados seis ***"Conclusiones"***, siete ***"Comunicación al Ente"*** y diez ***"Anexos"***, se encuentran pendientes.

El Proyecto de Informe deja expresamente indicado que *"La tarea abocó la verificación de la gestión de la administración de firma digital por parte de la DIRECCIÓN DE INNOVACIÓN TECNOLÓGICA de la OFICINA NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN, en lo referente a Firma Digital en el Estado Nacional. Para ello, y a partir de la información obtenida, se identificaron los temas de mayor exposición al riesgo, realizándose pruebas sustantivas y de cumplimiento para el control de los mismos"* (apartado 2.2 "Enfoque del Trabajo de Auditoría").

Asimismo, en el apartado ***"3.3 INFRAESTRUCTURA DE TI PARA LA FIRMA DIGITAL"***, se hace mención al Resolución JGM Nº 918/14, que en su artículo 4º aprueba la estructura organizativa de segundo nivel operativo de la entonces SUBSECRETARIA DE TECNOLOGÍAS DE GESTIÓN de la ex SECRETARIA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, de conformidad con el Organigrama y Acciones que, como Anexos VII y VIII, forman parte integrante de la dicha resolución.

Al respecto, se aclara que las acciones consignadas no corresponden a la Resolución mencionada, teniendo en cuenta que según su Anexo VIII la DIRECCIÓN DE INNOVACIÓN TECNOLÓGICA tenía a cargo las siguientes acciones:

1. Investigar nuevas tecnologías para la optimización de la gestión de la Administración Pública Nacional y proponer su implementación.
2. Asistir al Director Nacional en el cumplimiento de las obligaciones y funciones establecidas en la Ley de Firma Digital y su decreto reglamentario.
3. Intervenir en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento firmado digitalmente y firma digital.

4. Intervenir en aquellos aspectos vinculados con la incorporación de la firma digital a los circuitos de información del sector público y con su archivo en medios alternativos al papel.
5. Administrar la Autoridad Certificante de Firma Digital para el Sector Público Nacional.
6. Intervenir en el proceso de otorgamiento de adicionales informáticos para el personal de la Administración Pública Nacional.

Finalmente, se deja constancia que desde la fecha de comienzo de la auditoría a la actualidad han surgido diversos cambios normativos y de estructura en materia de Firma Digital, por lo que se procede a aclarar que la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN en la actualidad carece de competencias en materia de firma digital, quedando vigente la denominación de la Autoridad Certificante (AC ONTI), con lo cual se informa que se está trabajando en la actualización normativa que refería a la estructura anterior.

Efectuadas las salvedades indicadas, se analizan a continuación los ***"Comentarios y Observaciones"*** y las ***"Recomendaciones"***, detalladas en los apartados cuarto y quinto respectivamente.

- ***"4.1. La ONTI opera como Ente Licenciante y como Certificador Licenciado simultáneamente, resultando dicha situación incompatible en virtud de vulnerar el principio de control por oposición de intereses".***

  Se recomienda que la Autoridad de Aplicación arbitre los medios técnicos y presupuestarios para que el Ente Certificante cuente con su propio soporte técnico independiente de la AC ONTI, a fin de llevar a cabo las auditorías de validación y habilitación de nuevas Autoridades Certificantes de acuerdo a lo establecido en la norma.

  Comentarios

  Con la creación del MINISTERIO DE MODERNIZACIÓN (**Decreto Nº 13/15**, modificatorio de la Ley de Ministerios Nº 22.520) y la nueva estructura conformada por: **Decreto Nº 151/15**, modificatorio del Decreto Nº 357/2002; **Decreto Nº 13/16**, modificatorio del Decreto Nº 357/2002; **Decisión Administrativa Nº 232/16** y **Resolución del MINISTERIO DE MODERNIZACIÓN Nº 95/2016**, se modificaron las competencias establecidas en la estructura originaria perteneciente a la JEFATURA DE GABINETE DE MINISTROS.

INFORME DE AUDITORIA

Del mismo modo y en virtud de lo expuesto, actualmente el MINISTERIO DE MODERNIZACIÓN, la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, la DIRECCIÓN NACIONAL DE GESTIÓN DE LA INFORMACIÓN Y SOPORTE, la DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACIÓN Y FIRMA DIGITAL y la DIRECCIÓN DE FIRMA DIGITAL dependiente de esta última conforman la nueva estructura que entiende en materia de Firma Digital.

Por último, el Decreto Nº 561/16 otorga funciones de Ente Licenciante al MINISTERIO DE MODERNIZACIÓN y a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA respectivamente, y faculta a SINDICATURA GENERAL DE LA NACIÓN a realizar las auditorías previstas en el Capítulo VII de la Ley Nº 25.506.

Plan de Acción

Al día de la fecha, y considerando lo expresado actualmente, no existen incompatibilidades por lo que no se vulnera el principio de control por oposición de intereses.

Asimismo, se ha establecido contacto con la SINDICATURA GENERAL DE LA NACIÓN a fin de iniciar a la brevedad las auditorías a certificadores y sus Autoridades de Registro por parte de dicho organismo, en cumplimiento con lo establecido en el citado Decreto Nº 561/2016

4.2 RESERVADO - COLEGIO DE AUDITORES GENERALES -

SESION DEL 16/11/16

RESERVADO - COLEGIO DE AUDITORES GENERALES -

SESION DEL 16/11/16

- ***"4.3. El nivel de seguridad físico de la oficina donde opera AR ONTI es inferior al que indica la norma, lo que pone en riesgo la seguridad y confidencialidad de la infraestructura de Firma Digital".***

  Se recomienda que la ONTI arbitre los medios necesarios para acondicionar la oficina donde opera la Autoridad de Registro AR ONTI de manera tal de alinearla a lo establecido por la Disposición SsTG 01/2015.

  Comentarios

  La Disposición SsTG N° 1/2015 efectivamente menciona al Nivel 3 como aquel nivel mínimo de seguridad donde se deberá desarrollar las operaciones de la AR. A la fecha existe un control biométrico de acceso a dicha oficina para el personal del área.

  Plan de Acción

  Se procederá a incluir un libro de visitas en la oficina de la AR-ONTI para registrar los ingresos y egresos a la misma.

- ***"4.4. La Dirección de Administración Tecnológica-DAT, no cuenta con soporte energético alternativo que garantice la continuidad del servicio, lo que temporalmente podría afectar la validez de la lista de certificados revocados".***

  Se recomienda que la ONTI gestione la implementación de un sistema de suministro energético alternativo que permita garantizar la continuidad del servicio.

  Comentarios

  Teniendo en cuenta que las instalaciones del edificio administradas por la DAT, no cuentan con soporte energético alternativo, se está instalando la nueva infraestructura de firma digital de la AC-ONTI en ARSAT y su contingencia correspondiente en el datacenter de la AFIP.

  Plan de Acción

  Instalación de la nueva infraestructura de firma digital de la AC-ONTI contemplando las exigencias requeridas de soporte energético alternativo.

- ***"4.5. La política de back-up de PKI cuenta con debilidades en sus procedimientos de ejecución, lo que podría afectar la disponibilidad de la información y sus respectivos servicios".***

  Se recomienda que la ONTI actualice el documento de políticas y procedimientos de back up incorporando un instructivo detallado de las tareas a realizar. Asimismo, que formalice las tareas de pruebas de restauración de las copias de seguridad que se realizan (sugiriéndose realizar al menos DOS (2) pruebas al año). Por último, que arbitre los medios para guardar una copia de la información de PKI fuera del edificio de la ONTI.

  Comentarios

  Deberá perfeccionarse el procedimiento de back-up de la AC-ONTI.

  Plan de Acción

  Se actualizarán los documentos mencionados de políticas y procedimientos de back up.

  Se formalizarán en documentos específicos las pruebas de restauración de copias de seguridad.

- ***"4.6. La Dirección de Innovación Tecnológica no cuenta con un plan de contingencia** que **determine los pasos a seguir ante eventualidades que interrumpan el servicio lo que podría generar inconvenientes para recuperar el servicio ante incidentes".***

  Se recomienda que la ONTI gestione la redacción y aprobación de un procedimiento que describa detalladamente las acciones o pasos a seguir por cada uno de los integrantes, en caso de fallas que provoque una indisponibilidad de servicio.

  Comentarios

  Actualmente se cuenta con un Plan de Contingencia, que deberá ser actualizado en virtud de la nueva estructura del MINISTERIO DE MODERNIZACIÓN.

  Plan de Acción

  Se redactará nuevamente la documentación referida a los procedimientos de contingencia

- ***"4.7. La Dirección de Innovación Tecnológica dependiente de la ONTI no cuenta** con un **sistema de seguimiento de pedidos de soporte, lo que limita la calidad del mantenimiento de los sistemas".***

  Se recomienda que la ONTI gestione la implementación de un sistema de tipo CRM con el fin de poder dar seguimiento, priorización y registro a los pedidos de asistencia técnica de los usuarios.

  Comentarios

  Actualmente los pedidos de soporte son recibidos por correo electrónico o telefónicamente, efectuándose su seguimiento y resolución por los mismos medios con la mayor rapidez posible, obteniéndose un alto grado de satisfacción por parte de los usuarios.

  Plan de Acción

  Se gestionará la implementación de un sistema de seguimiento con las características indicadas a fin de mejorar la calidad de la asistencia brindada.

- ***"4.8. La estructura operativa de la Dirección de Innovación Tecnológica, dependiente de la ONTI no se encuentra formalizada en el organigrama oficial del organismo, y los recursos humanos asignados en esa dirección resultan insuficientes para el cumplimiento de los objetivos del área".***

  Se recomienda que la ONTI formalice la estructura operativa de la Dirección, las funciones y responsabilidades por roles, dimensionándola para que pueda cumplir con sus objetivos y roles de forma eficiente.

  Comentarios

  La ex DIRECCIÓN DE INNOVACIÓN TECNOLÓGICA, hoy denominada DIRECCIÓN DE FIRMA DIGITAL dependiente de la DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACIÓN Y FIRMA DIGITAL de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, tiene a su cargo una Coordinación de Firma Digital. El correspondiente organigrama se encuentra a consulta en la URL: [illegible]

  Plan de Acción

  Se ampliará la información requerida, formalizando la estructura operativa de la Dirección a través de un documento específico, indicando roles, funciones y responsabilidades.

- ***"4.9. El Ente Licenciante no lleva a cabo con la periodicidad estipulada las auditorías de seguimiento sobre las Autoridades Certificantes y de Registro".***

  Se recomienda que la Autoridad de Aplicación arbitre los medios administrativos, técnicos y presupuestarios para cumplir adecuadamente con las auditorías anuales de seguimiento, según lo establecido en la norma.

  Comentarios

  La SINDICATURA GENERAL DE LA NACIÓN se encuentra facultada por el Decreto 561/2016 a realizar las auditorías previstas en el Capítulo VII de la Ley N° 25.506.

Plan de Acción

Se ha establecido contacto con la SINDICATURA GENERAL DE LA NACIÓN a fin de iniciar a la brevedad las auditorías a certificadores y sus Autoridades de Registro por parte de dicho organismo en cumplimiento de lo establecido en el citado Decreto N° 561/2016.

- ***"4.10. No se encuentran formalizados los acuerdos de niveles de servicio entre los organismos que brindan soporte a la plataforma tecnológica de Firma Digital y a la ONTI".***

Se recomienda que la ONTI formalice acuerdos de niveles de servicio con los prestadores del servicio de housing.

Comentarios.

Con fecha 25 de enero de 2005 se celebró un Convenio Marco entre la AFIP y la entonces SECRETARÍA DE LA GESTIÓN PÚBLICA con fines de colaboración, cooperación y complementación, comprometiéndose a facilitarse mutuamente distintos recursos que sirvan al mejor desarrollo institucional de cada organismo.

Asimismo, con fecha 3 de agosto de 2006, dentro de lo previsto por el citado Convenio Marco, se celebró el Acuerdo Específico Nº 1 por el cual la entonces SECRETARÍA DE LA GESTIÓN PÚBLICA solicitó a la AFIP, autorizando esta última el alojamiento gratuito del equipamiento informático de la SGP, destinado a la administración y mantenimiento de la AC RAIZ y la AC ONTI, en el ambiente de máxima seguridad propiedad de la AFIP.

Por último, con fecha 1 de noviembre de 2007, se formalizó el Acta Complementaria de Ejecución del citado Convenio y del Acuerdo Específico, dejándose expresa constancia que al día de la fecha los mismos gozan de plena vigencia.

- ***"4.11. No se cuenta con una planificación y programación formalizando las reuniones periódicas para el seguimiento y control de los productos y servicios provistos por el proveedor de desarrollo de software, lo que no permite cumplir adecuadamente con el proceso de Gestión de Proveedores de TI, según lo establecen las buenas prácticas relativas a gestión de rendimiento de servicios".***

Se recomienda que la ONTI formalice una agenda de reuniones periódicas de seguimiento a nivel de gestión o coordinación general, en el marco de la gestión de rendimiento del servicio

provisto por DATCO, asegurando que las mismas se lleven a cabo con una periodicidad suficiente para asegurar que se cumplan los niveles de servicio acordados.

Comentarios

a. Se informa que la comunicación con la empresa DATCO es frecuente, debido a que se encuentran a cargo del mantenimiento y la actualización del software de emisión de certificados de la AC ONTI. Si bien no existe una agenda de reuniones programadas, la comunicación se efectúa con un frecuencia de 2 o 3 veces por semana vía correo electrónico o telefónicamente.

b. Asimismo, la firma DATCO provee un sistema de tickets, para realizar el seguimiento y eventual solución de inconvenientes planteados. Dichos tickets se inician enviando un correo electrónico a helpdesk2@datco.net, y posteriormente la firma DATCO informa el número del mismo. Estos tickets pueden ser generados por temas relacionados a infraestructura o software.

c. A la fecha, la DIRECCIÓN DE FIRMA DIGITAL cuenta con una aplicación interna, para agender el seguimiento, donde se registran las pruebas que se realizan sobre la aplicación de firma digital provista por DATCO. Se detectan los errores y/o faltantes y luego se procede al envío de un documento a la empresa, para que en virtud de lo solicitado realicen las correcciones pertinentes.

Plan de Acción

Dadas las condiciones enunciadas precedentemente, consideramos que se cumplen razonablemente los requerimientos de gestión de servicios provistos por el proveedor.

- ***"4.12. No se realizan las reuniones trimestrales de Comisión Asesora para la Infraestructura de Firma Digital, orientadas a generar recomendaciones de mejoras en base a estándares tecnológicos".***

  Se recomienda que la Comisión Asesora formalice la programación anual de reuniones delineando los respectivos temarios y objetivos a cumplir en ellas.

Comentarios

De acuerdo a la Ley 25.506, en el Capítulo VIII "De la Comisión Asesora para la Infraestructura de Firma Digital", en el artículo 35 sobre "Integración y Funcionamiento" se indica que "...Los

IF-2016-00166107-APN-MM

integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez. Se reunirá como mínimo trimestralmente..."

Del mismo modo, el Decreto Reglamentario 2628/02, en su CAPITULO III "DE LA COMISIÓN ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL", recepta los artículos 7 a 10, delimitando la Integración, Ejercicio de Funciones y Consulta Pública.

Posteriormente, el Decreto Nº 160/2004 designa a los integrantes de la COMISIÓN ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL.

Por último, la Resolución JGM N° 435/2004, aprueba el reglamento de funcionamiento de la COMISIÓN ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL.

Finalmente, se informa que desde la designación de los integrantes efectuada por el Decreto Nº 160/2004 no se han renovado ni designado nuevos miembros.

Plan de Acción

Teniendo en cuenta el marco normativo aplicable, y la designación realizada por el Decreto Nº 160/2004, la designación de nuevos integrantes podría interpretarse como una facultad del PODER EJECUTIVO NACIONAL.

- ***"4.13. Se encuentran desactualizados los procedimientos y guías técnicas sobre la plataforma e infraestructura tecnológica de Firma Digital utilizados por el personal de soporte de la ONTI, lo que genera dependencia de personal clave".***

Se recomienda que la ONTI actualice los documentos oficiales de guías y procedimientos técnicos de la plataforma tecnológica de firma digital.

Comentarios

a. Cabe destacar que los documentos referidos, definen un Procedimiento de instalación de SO y configuración de todos los servidores que se encuentran en la infraestructura de firma digital. Si bien dichos documentos datan del año 2010, los servidores siguen en funcionamiento y no fueron cambiados, por lo que todos los procesos definidos en el documento se encuentran vigentes.

b. Los mencionados manuales son de utilización frecuente; por ejemplo para generar e instalar el certificado SSL que se utiliza para la comunicación de los TMG con los sitios WEB.

c. Cabe mencionar que se actualizó el sistema operativo Windows Server 2008 R2 del DPM por Windows Server 2012 R2.

Plan de Acción

Se deja constancia que la plataforma tecnológica no presenta cambios significativos, por lo cual los procedimientos permanecen vigentes. Se tendrá en cuenta la observación al implementar la nueva infraestructura.

- ***"4.14. Los legajos de las Autoridades Certificantes no cuentan con un soporte digital adecuado para realizar consultas revisiones y actualizaciones".***

  Se recomienda que la ONTI implemente un sistema dedicado a la gestión documental que permita indexar y almacenar los documentos en una base de datos de legajos de fácil acceso. Asimismo, haciendo uso de las herramientas propias de la dirección, impulse las medidas que optimicen los procesos administrativos inherentes a la firma digital, cuyo objetivo principal es la despapelización, de forma tal que no genere el volumen actual de papel, sin dejar de cumplir con la legislación vigente.

Comentarios

El Decreto Nº 561/2016 aprueba la implementación del sistema de Gestión Documental Electrónica —GDE— como sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional. Dicho sistema actúa como plataforma para la implementación de gestión de expedientes electrónicos.

Asimismo, la documentación de los suscriptores de los certificados de firma digital, luego de su aprobación es escaneada y conservada en el sistema de la aplicación de PKI, para su posterior consulta por los Oficiales de Registro, de forma digitalizada, y firmada digitalmente por el Oficial de Registro que ha aprobado la solicitud del certificado.

Plan de Acción

Con el objetivo de fortalecer la tarea de minimizar la utilización de documentos basados en papel, sin menoscabo alguno a la seguridad jurídica, y a los fines de dar cumplimiento con el Decreto N° 561/16 que aprueba el sistema de GESTIÓN DOCUMENTAL ELECTRÓNICA (GDE), los nuevos procesos de licenciamiento deberán realizarse en formato digital y tramitarse en dicho sistema.

- ***"4.15. El Sistema de Registro de Firma Digital en el que se registra la información personal de los subscriptores de Firma Digital de AC-ONTI admite que puedan no cargarse datos que son considerados imprescindibles, lo que atenta contra la completitud de la información allí almacenada" (sic).***

Se recomienda que la ONTI rediseñe la base de datos de la aplicación que registra y almacena los datos de los usuarios de la AC, a fin de que se reflejen los datos considerados obligatorios, la optimización de tipos de datos y las buenas prácticas de diseño y uso de tipos de datos definidas por el desarrollador del motor de base de datos.

Comentarios

Considerando que la auditoría alcanzó el período comprendido entre el 31/07/2014 y el 31/07/2015, teniendo en cuenta que *"...las tareas de campo se desarrollaron de septiembre a diciembre de 2015"*, cabe destacar las siguientes aclaraciones:

a. Durante el transcurso del período mencionado, hasta mayo de 2015 los certificados eran emitidos conforme la **Decisión Administrativa Nº 6/2007** y en cumplimiento de la "Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado" de la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI) aprobada por la **Resolución de la ex SECRETARÍA DE LA GESTIÓN PÚBLICA Nº 227/2010**.

b. Asimismo, dicha Política de Certificación de la AC ONTI aprobada por la **Resolución ex SGP Nº 227/2010**, tenía un perfil de certificado distinto al actualmente vigente, que contenía diferentes campos.

INFORME DE AUDITORIA

Posteriormente, la **Decisión Administrativa Nº 927/2014 (De fecha 30/10/2014)**, entre otros cambios significativos, incorpora la Política Única de Certificación, y establece un perfil único de certificado interoperable entre certificadores licenciados, con lo cuál no pueden agregarse campos a los perfiles aprobados en dicha Decisión Administrativa.

Del mismo modo, la **Disposición SsTG Nº 7/2015 (De fecha 10/09/2015)** aprueba las "ACLARACIONES TÉCNICAS ESPECÍFICAS PARA LA DECISIÓN ADMINISTRATIVA Nº 927/2014".

Por último, la **Disposición SsTG Nº 11/2014** aprueba la adhesión a la POLÍTICA ÚNICA DE CERTIFICACIÓN de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI).

c. Al respecto, y a la fecha coexisten certificados emitidos bajo la Política de Certificación aprobada por la Resolución ex SGP Nº 227/2010 que actualmente se encuentran vigentes, con aquellos aprobados en conformidad de la POLÍTICA ÚNICA DE CERTIFICACIÓN aprobada por la **Disposición SsTG Nº 11/2014**. En particular, respecto al campo CUIT, debe aclararse que el mismo sólo resulta obligatorio a partir de la vigencia de la nueva Política única de Certificación, con lo cual algunos certificados tendrán el campo CUIT.

Sin otro particular, le saludo atentamente.

A LA SEÑORA
AUDITORA GENERAL DE LA NACIÓN
CDORA. VILMA N. CASTILLO
S_____/_____D

IF-2016-00396107-APN-MM

Auditoría General de la Nación

INFORME DE AUDITORIA

República Argentina Poder Ejecutivo Nacional
2016 - Año del Bicentenario de la Declaración de la Independencia Nacional

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2016-00396107-APN-MM

Buenos Aires, Lunes 25 de Julio de 2016

Referencia: CUDAP: EXP-S01: 0292293/2016 -- ACLARACIONES AL INFORME DE LA AUDITORI GENERAL DE LA NACIÓN

El documento fue importado por el sistema GEDO con un total de 14 pagina/s.

Andrés Horacio Ibarra
Ministro
Ministerio de Modernización

Auditoría General de la Nación

INFORME DE AUDITORIA

República Argentina Poder Ejecutivo Nacional
2016 - Año del Bicentenario de la Declaración de la Independencia Nacional

Providencia

Número: PV-2016-08596412-APN-MM

Buenos Aires, Lunes 25 de Julio de 2016

Referencia: EXP-S01: 0081584/2016

AUDITORIA GENERAL DE LA NACION

Habiendo sido suscripta por parte del Sr. Ministro de Modernización, la acción al Informe de la Auditoría General de la Nación, respecto del "Proyecto de Informe de Si Informática", elevo los presentes actuados para su conocimiento y a los efectos que estime correspon

PATO RUBEN ANDRES
Coordinador
Ministerio de Modernización

INFORME DE AUDITORIA

ANEXO II – Análisis de los comentarios del auditado

A continuación se presenta el análisis realizado por esta AGN para cada uno de los comentarios del auditado

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
4.1. La ONTI opera como Ente Licenciante y como Certificador Licenciado simultáneamente, resultando dicha situación incompatible en virtud de vulnerar el principio de control por oposición de intereses.	La infraestructura de la Firma Digital de la República Argentina, conforme la normativa en la materia, prevé que el Ente Licenciante (AC-Raíz) realice auditorías operativas a los Certificadores Licenciados (AC) con el objeto de verificar que su funcionamiento se corresponda con las disposiciones vigentes (Dec. Adm. 6/07, Cap. VIII, art 32º). A la fecha de cierre de los trabajos de campo, y en base a entrevistas y análisis de documentación recabada, se pudo determinar que la Dirección de Innovación Tecnológica dependiente de la ONTI es la encargada de llevar adelante la función citada en el párrafo precedente.	Con la creación del MINISTERIO DE MODERNIZACIÓN (Decreto Nº 13/15, modificatorio de la Ley de Ministerios Nº 22.520) y la nueva estructura conformada por: Decreto Nº 151/15, modificatorio del Decreto Nº 357/2002; Decreto Nº 13/16, modificatorio del Decreto Nº 357/2002; Decisión Administrativa Nº 232/16 y Resolución del MINISTERIO DEMODERNIZACIÓN Nº 95/2016, se modificaron las competencias establecidas en la estructura originaria perteneciente a la JEFATURA DE GABINETE DE MINISTROS. Del mismo modo y en virtud ., delo expuesto, actualmente el MINISTERIO DE MODERNIZACIÓN, la SECRETARÍADE	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	Cabe señalar que por Dto. 1028/03 se disolvió el Ente Administrador de Firma Digital, decretándose que su accionar sería llevado por la Oficina Nacional de Tecnologías de Información. Por otra parte, y mediante Res. Nº 227/10 se resuelve en su art. 2º: "Otorgar la Licencia para operar como Certificador Licenciado a la Oficina Nacional de Tecnologías de Información..., ordenándose su inscripción en el Registro de Certificadores Licenciados". De acuerdo a lo expuesto, la Dirección de Innovación desempeña una doble función. Por un lado como personal que cumple tareas delegadas por el Ente Licenciante y por el otro como prestador de servicios y soporte en su rol de Autoridad Certificante. Aun obedeciendo a un mandato legal, esta doble intervención vulnera la independencia que requiere todo control.	MODERNIZACIÓN ADMINISTRATIVA, la DIRECCIÓNNACIONAL DE GESTIÓN DE LA INFORMACIÓN Y SOPORTE, la DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACIÓN Y FIRMA DIGITAL y la DIRECCIÓN DE FIRMA DIGITAL dependiente de esta última conforman la nueva estructura que entiende en materia de Firma Digital. Por último, el Decreto Nº 561/16 otorga funciones de Ente Licenciante al MINISTERIO DE MODERNIZACIÓN y a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA respectivamente, y faculta a la SINDICATURA GENERAL DE LA NACIÓN a realizar las auditorías previstas en el Capítulo VII de la Ley N° 25.506. **Plan de Acción** Al día de la fecha, y considerando lo expresado actualmente, no existen incompatibilidades por lo que no se vulnera el principio de control por oposición de intereses. Asimismo, se ha establecido contacto con la SINDICATURA GENERAL DE LA NACIÓN a fin de iniciar a la brevedad las auditorías a certificadores y sus Autoridades de Registro por	

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
		parte de dicho organismo, en cumplimiento con lo establecido en el citado Decreto N° 561/2016.	
4.2	**RESERVADO – COLEGIO DE AUDITORES**	**GENERALES – SESIÓN DEL** 16/11/16	

Auditoría General de la Nación

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	RESERVADO – COLEGIO DE AUDITORES	GENERALES – SESIÓN DEL 16/11/16	

Auditoría General de la Nación

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	RESERVADO – COLEGIO DE AUDITORES	GENERALES – SESIÓN DEL 16/11/16	

Auditoría General de la Nación

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	RESERVADO – COLEGIO DE AUDITORES	GENERALES – SESIÓN DEL 16/11/16	

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	RESERVADO – COLEGIO DE AUDITORES	**GENERALES – SESIÓN DEL** 16/11/16	
4.3. El nivel de seguridad física de la oficina donde opera AR ONTI es inferior al que indica la norma, lo que pone en riesgo la seguridad y confidencialidad de la infraestructura de Firma Digital.	La Disposición SSTG 01/2015 determina que las Autoridades de Registro deben operar en una oficina que cumpla con una serie requisitos de seguridad, denominados de "Nivel 1". Entre otros requisitos, uno de ellos estipula que se deberá establecer un control y el registro de los ingresos y egresos, e impedir el acceso físico de toda persona ajena a la AR que no se haya registrado previamente". Durante las tareas de campo se verificó que el ingreso a las oficinas no era controlado ni registrado, ni se encontró evidencias de la existencia de un Libro de Visitas. Esto impide que quede registrado quien visita un área donde se trabaja con información sensible y confidencial. La falta de registros de ingreso y egreso y controles de Nivel 1 vulnera las normas de	**Comentarios** La Disposición SsTG Nº 1/2015 efectivamente menciona al Nivel 1 como aquel nivel mínimo de seguridad donde se deben desarrollar las operaciones de la AR. A la fecha existe un control biométrico de acceso a dicha oficina para el personal del área. **Plan de Acción** Se procederá a incluir un libro de visitas en la oficina de la AR-ONTI para registrar los ingresos y egresos a la misma.	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	seguridad establecidas, lo que pone en riesgo la seguridad y confidencialidad de la infraestructura de Firma Digital.		
4.4. La Dirección de Administración Tecnológica-DAT, no cuenta con soporte energético alternativo que garantice la continuidad del servicio, lo que temporariamente podría afectar la validez de la lista de certificados revocados.	La Dirección de Administración Tecnológica de la Jefatura de Gabinete de Ministros provee el Data Center para los Equipos de Procesamiento de Datos, Telecomunicaciones, Seguridad Informática y otros Sistemas de Soporte. Este servicio brindado a todas las áreas de la Jefatura de Gabinete de Ministros, tiene por propósito mantener un ambiente de operación apropiado. Así mismo, brinda el servicio de housing para los servidores de procesamiento de datos de Firma Digital. Actualmente, el respaldo energético del Data Center está compuesto por dos equipos de UPSs con una autonomía conjunta de aproximadamente dos horas. Este tiempo resulta suficiente como para realizar un apagado normal de todos los equipos en caso de cortes de energía superiores a las dos horas. Sin embargo, la DAT no cuenta con un soporte	**Comentarios** Teniendo en cuenta que las instalaciones del edificio administradas por la DAT, no cuentan con soporte energético alternativo, se está instalando la nueva infraestructura de firma digital de la AC-ONTI en ARSAT y su contingencia correspondiente en el data center de la AFIP. **Plan de Acción** Instalación de la nueva infraestructura de firma digital de la AC-ONTI contemplando las exigencias requeridas de soporte energético alternativo.	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	energético de instancia superior (grupo electrógeno); debido a restricciones edilicias que dificultan su emplazamiento, según lo manifestado por el auditado. El riesgo de no contar con el respaldo de un grupo electrógeno es que, ante cortes prolongados de energía, resulta imposible asegurar la continuidad del servicio en los aplicativos de Firma Digital, debiendo recurrirse entonces al sitio alternativo. El proceso más crítico que se podría afectar tras una interrupción del servicio es el de actualización y publicación de la lista de revocación. En efecto, tras la denuncia de baja de un certificado, la indisponibilidad del servicio antes descripto podría impedir el bloqueo de la firma (lo que puede conducir a tomar por válidas firmas que en ese momento deberían encontrarse bloqueadas).		
4.5. La política de back-up de PKI	La Dirección de Innovación Tecnológica cuenta con un documento que detalla los alcances de	**Comentarios** Deberá perfeccionarse el procedimiento de back-	La respuesta del organismo no contradice las

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
cuenta con debilidades en sus procedimientos de ejecución, lo que podría afectar la disponibilidad de la información y sus respectivos servicios.	las políticas y procedimientos para la ejecución de back-ups de resguardo de la base de datos y aplicativos de PKI. De las tareas de auditoría surge que aquél documento detalla qué bases de datos y aplicativos deben ser resguardados, pero no especifica cuál es el procedimiento para hacerlo. Además, se ha detectado que no se llevan a cabo procedimientos de pruebas de restauración de back-ups para comprobar la efectividad de los respaldos obtenidos, en caso de tener que responder con ellos ante una contingencia. Por último se ha podido verificar que los back-up se realizan en discos externos que se guardan en una caja ignífuga ubicada dentro de la propia Dirección de Innovación Tecnológica, no contemplando la guarda de una copia de los back-ups fuera del edificio, de acuerdo a lo que indican las buenas prácticas de seguridad de la	up de la AC-ONTI. **Plan de Acción** Se actualizarán los documentos mencionados de políticas y procedimientos de back up. Se formalizarán en documentos específicos las pruebas de restauración de copias de seguridad.	observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorías.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	información. De las observaciones levantadas en los procedimientos de back-ups se desprenden los siguientes riesgos: • Ante un posible incidente edilicio en las oficinas de ONTI (ejemplo: incendio), no se cuenta con copias alternativas de los resguardos de información para reestablecer el servicio. • Si no se realizan pruebas de restauración de los back-ups no se puede garantizar un adecuado restablecimiento de la disponibilidad de la información y sus respectivos servicios. • Si en la documentación de políticas y procedimientos de back-ups no se detallan los instructivos de cómo se deben realizar las tareas de resguardo de información, se depende de personal crítico para la realización de esta tarea.		
4.6. La Dirección de Innovación	Tanto AC-ONTI como AC-Raíz brindan servicios desde una infraestructura que cuenta con	**Comentarios** Actualmente se cuenta con un Plan de	La respuesta del organismo no contradice las

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
Tecnológica no cuenta con un plan de contingencia que determine los pasos a seguir ante eventualidades que interrumpan el servicio, lo que podría generar inconvenientes para recuperar el servicio ante incidentes.	mecanismos de restablecimiento factibles. Sin embargo, los mismos no se encuentran debidamente documentados y formalizados. Toda organización debe contar con un plan unificado, con instrucciones claras y precisas de cómo proceder ante eventualidades que interrumpan parcial o totalmente el servicio brindado. La falta de formalización de estos planes puede provocar inconvenientes para recuperar el servicio, y genera dependencia sobre el personal especializado en realizar la tarea.	Contingencia, que deberá ser actualizado en virtud dela nueva estructura del MINISTERIO DE MODERNIZACIÓN. **Plan de Acción** Se redactará nuevamente la documentación referida a los procedimientos de contingencia.	observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorias.
4.7. La Dirección de Innovación Tecnológica dependiente de la ONTI no cuenta con un sistema de seguimiento de pedidos de soporte,	La Dirección de Innovación Tecnológica de ONTI realiza tareas de soporte al usuario para una serie de sistemas. Entre estos se destacan por un lado el sistema que administra a los usuarios poseedores de una Firma Digital brindada por ONTI, ya sea directamente o a través de sus Autoridades de Registro; y por otro el sistema que utilizan otras Autoridades Certificantes para	**Comentarios** Actualmente los pedidos de soporte son recibidos por correo electrónico o telefónicamente,efectuándose su seguimiento y resolución por los mismos medios con la mayor rapidezposible, obteniéndose un alto grado de satisfacción por parte de los usuarios. **Plan de Acción**	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
lo que limita la calidad del mantenimiento de los sistemas.	interactuar con la Autoridad Certificante Raíz. Cuando los usuarios se encuentran con un inconveniente o deben realizar alguna consulta al soporte técnico, se contactan telefónicamente o vía correo electrónico con la Dirección de Innovación Tecnológica. El número de contacto está asociado a todos los teléfonos del personal asignado a esta tarea, por lo que las llamadas recibidas se derivan a todos ellos en forma simultánea. Los pedidos de asistencia no se registran en ningún medio o sistema, ya sea por parte del agente que recibió el pedido inicialmente o por quien lo reemplace, lo que dificulta su seguimiento, imposibilita la realización de análisis históricos sobre problemas frecuentes y reduce la eficiencia de la tarea de mantenimiento. Tal y como indican las buenas prácticas, cada pedido de soporte debería registrarse en un sistema que permita identificar en forma unívoca cada solicitud, tanto para hacer un seguimiento del estado de los pendientes,	Se gestionará la implementación de un sistema de seguimiento con las características indicadas a fin de mejorar la calidad de la asistencia brindada.	auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	como para servir de base de conocimiento y acelerar así la tarea de los agentes. Podría también ser abierta al usuario con el fin de disminuir la cantidad de contactos entrantes (llamadas y correos electrónicos), para medir el nivel de servicio o conocer los pedidos activos. El no contar con un sistema de estas características conlleva el riesgo de no resolver el inconveniente de algunos usuarios, o no darle la prioridad adecuada. Asimismo, la falta del sistema imposibilita o dificulta la distribución correcta de las tareas entre los agentes que corresponda, e impide la identificación de problemas recurrentes a los fines de brindar soluciones más eficientes.		
4.8. La estructura operativa de la Dirección de Innovación Tecnológica, dependiente de la ONTI, no se	El organigrama oficial de la Jefatura de Gabinete de Ministros expone su estructura hasta el nivel de Dirección. En consecuencia, la Dirección de Innovación Tecnológica que depende de la ONTI no cuenta con un organigrama formalmente definido, ni se encuentran formalizados los perfiles, las	**Comentarios** La ex DIRECCIÓN DE INNOVACIÓN TECNOLÓGICA, hoy denominada DIRECCIÓN DE FIRMADIGITAL dependiente de la DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACIÓN Y FIRMA DIGITAL de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
encuentra formalizada en el organigrama oficial del organismo, y los recursos humanos asignados en esa dirección resultan insuficientes para el cumplimiento de los objetivos del área.	funciones y las responsabilidades del equipo de trabajo que integra dicha dirección. A partir de entrevistas realizadas durante las tareas de campo se detectó que, si bien se cubren las demandas operativas del área, se produce un solapamiento de roles, funciones y responsabilidades, de lo que se desprende que los recursos humanos que componen el equipo de trabajo son insuficientes para cubrir los roles que demandan las actividades y servicios que brinda la dirección. Cabe destacar que la Ley 25.506, en el artículo 21, inciso v, determina como obligaciones del certificador licenciado, "Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación". La falta de formalización de roles, funciones y responsabilidades por perfil y la insuficiencia de recursos conduce al solapamiento de responsabilidades y de actividades. Esta situación dificulta el cumplimiento de las tareas	MINISTERIO DE MODERNIZACIÓN, tiene a su cargo una Coordinación de Firma Digital. El correspondiente organigrama se encuentra a consulta en la URL:http://mapadelestado.modernizacion.gob.ar/sitio/ministerios/modernizacion/organigrama/modernizacion.pdfc **Plan de Acción** Se ampliará la información requerida, formalizando la estructura operativa de la Dirección a través de un documento específico, indicando roles, funciones y responsabilidades.	evaluaran en futuras auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	propias de la oficina, como las relativas al control (al respecto, véase observación siguiente).		
4.9. El Ente Licenciante no lleva a cabo con la periodicidad estipulada las auditorías de seguimiento sobre las Autoridades Certificantes y de Registro.	De acuerdo a lo normado en el artículo 33 de la Ley 25.506, y según lo establecido en la Decisión Administrativa Nro. 927/2014, el Ente Licenciante (AC-Raíz) debe realizar en períodos anuales las auditorías de seguimiento y control sobre las Autoridades Certificantes y sobre las Autoridades de Registro habilitadas y en activa operación. De las tareas realizadas surge que el Ente Licenciante no cumple con este aspecto de la normativa vigente. Los únicos organismos auditados fueron las Autoridades Certificantes de AFIP y ANSES, auditándolas sólo una vez desde que están operativas (hace 8 años), quedando pendientes las auditorías de todas las Autoridades Certificantes privadas, siendo la más antigua Encode S.A., que opera desde 2012.	**Comentarios** La SINDICATURA GENERAL DE LA NACIÓN se encuentra facultada por el Decreto 561/2016 a realizarlas auditorías previstas en el Capítulo VII de la Ley N° 25.506. **Plan de Acción** Se ha establecido contacto con la SINDICATURA GENERAL DE LA NACIÓN a fin de iniciar a la brevedad las auditorías a certificadores y sus Autoridades de Registro por parte de dicho Organismo en cumplimiento de lo establecido en el citado Decreto N° 561/2016.	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	La Subsecretaría de Tecnologías de Gestión no cuenta con una estructura operativa técnica propia que le permita cumplir con los procesos de auditoría requeridos en la norma y, a su vez, con las actividades diarias. Por otro lado, de acuerdo a lo manifestado por el auditado, la estructura operativa que tiene a cargo el trabajo de campo en estas auditorías no cuenta con el debido presupuesto a los efectos de cubrir los gastos requeridos para el traslado de los recursos asignados a estas auditorías. La falta de auditorías de seguimiento sobre las Autoridades Certificantes y de Registro operativas debilita el control que la ONTI, en su carácter de Ente Licenciante, debe ejercer sobre las entidades que certifica.		
4.10. No se encuentran formalizados los acuerdos de niveles de servicio entre los organismos que	La infraestructura tecnológica que brinda servicios al entorno operativo de Firma Digital, tanto a nivel del Ente Licenciante (AC-Raíz) como a nivel de la Certificador Licenciado (AC-ONTI) se encuentra implementada en modalidad housing en los siguientes	**Comentarios.** Con fecha 25 de enero de 2005 se celebró un Convenio Marco entre la AFIP y la entonces SECRETARÍA DE LA GESTIÓN PÚBLICA con fines de colaboración, cooperación y complementación, comprometiéndose a facilitarse mutuamente	El acuerdo mencionado no permite el aseguramiento de la disponibilidad ni de la calidad del servicio. Por lo tanto se mantiene la observación.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
brindan soporte a la plataforma tecnológica de Firma Digital y a la ONTI.	organismos: • ANSES para la contingencia de AC-ONTI • AFIP para el sitio principal de AC-Raíz • DAT - Dirección de Administración Tecnológica – para el soporte de telecomunicaciones, energía y refrigeración para el HSM principal AC-ONTI. El servicio de housing que estos organismos brindan a la plataforma de Firma Digital, tiene por objetivo principal disponer dentro de sus propios Data Center de un espacio en el cual se alojan los servidores, los equipos de comunicaciones y redes, y equipos de seguridad informática propiedad de ONTI. Este cofre o espacio se ofrece garantizando el cumplimiento de las normas de seguridad física que debe tener un Data Center de alta disponibilidad de servicio. A partir de entrevistas realizadas y de las inspecciones realizadas a los Data Center pertinentes, se pudo constatar que, si bien las condiciones generales del servicio de housing se	distintos recursos que sirvan al mejor desarrollo institucional de cada organismo. Asimismo, con fecha 3 de agosto de 2005, dentro de lo previsto por el citado Convenio Marco, se celebró el Acuerdo Específico Nº 1 por el cual la entonces SECRETARÍA DE LA GESTIÓN PÚBLICA solicitó a la AFIP, autorizando esta última el alojamiento gratuito del equipamiento informático de la SGP, destinado a la administración y mantenimiento de la ACRAIZ y la AC ONTI, en el ambiente de máxima seguridad propiedad de la AFIP. Por último, con fecha 1 de noviembre de 2007, se formalizó el Acta Complementaria de Ejecución del citado Convenio y del Acuerdo Específico, dejándose expresa constancia que al día de la fecha los mismos gozan de plena vigencia.	

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	cumplen razonablemente, los servicios no se encuentran formalizados en documentos y/o actas donde queden asentados los acuerdos de niveles de servicios ofrecidos por los organismos prestadores del servicio, y los requeridos por la ONTI, para garantizar la demanda de disponibilidad tecnológica que necesitan los procesos operativos de Firma Digital. De este modo no se cuenta con una herramienta que permita a ambas partes medir el nivel de calidad del servicio en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc., como indican las mejores prácticas al respecto, y lo que deriva en una administración informal del servicio de locación de los activos tecnológicos de la ONTI.		
4.11. No se cuenta con una planificación y programación formalizando las	En el marco del servicio provisto por DATCO S.A., orientado a brindar soporte tecnológico a los procesos de Firma Digital (Pliego de Bases y Condiciones Particulares, Expediente Nro.	**Comentarios** a. Se informa que la comunicación con la empresa DATCO es frecuente, debido a que se encuentran a cargo del mantenimiento y la	Si bien el organismo informa tener contacto frecuente con el proveedor, este es reactivo, y no planificado, sin

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
reuniones periódicas para el seguimiento y control de los productos y servicios provistos por el proveedor de desarrollo de software, lo que no permite cumplir adecuadamente con el proceso de Gestión de Proveedores de TI, según lo establecen las buenas prácticas relativas a gestión de rendimiento de servicios.	CUDAP: EXP-JGM 12169/2014 del 14-7-2014), es responsabilidad de la Dirección de Innovación Tecnológica de ONTI realizar el seguimiento y control de los servicios y productos provistos. A partir de las entrevistas realizadas y en función del análisis y revisión de la documentación provista por el auditado, se ha detectado que a nivel operativo, el seguimiento sobre los niveles y performance de los servicios se realiza en forma continua. No obstante, dentro del esquema de trabajo no se encuentran previstas reuniones periódicas de seguimiento a nivel coordinación general, cuyo objetivo sea evaluar la performance y la calidad del servicio y el estado actual de las carteras de trabajo, para medir los grados de avances de los requerimientos de ONTI sobre el aplicativo, tomar acciones correctivas ante los desvíos detectados y obtener nuevos compromisos formales de parte del proveedor. La falta de reuniones periódicas de seguimiento	actualización del software de emisión de certificados de la AC ONTI. Si bien no existe una agenda de reuniones programadas, la comunicación se efectúa con un frecuencia de 2 o 3 veces por semana vía correo electrónico o telefónicamente . b. Asimismo, la firma DATCO provee un sistema de tickets, para realizar el seguimiento y eventual solución de inconvenientes planteados. Dichos tickets se inician enviando un correo electrónico a helpdesk2@datco.net, y posteriormente la firma DATCO informa el número del mismo. Estos tickets pueden ser generados por temas relacionados a infraestructura o software. c. A la fecha, la DIRECCIÓN DE FIRMA DIGITAL cuenta con una aplicación interna, para agenciar el seguimiento, donde se registran las pruebas que se realizan sobre la aplicación de firma digital provista por DATCO. Se detectan los errores y/o faltantes y luego se procede al envío de un documento a la empresa, para que en virtud de lo solicitado realicen las correcciones pertinentes. **Plan de Acción**	que quede formalmente registrado en el organismo el contacto sostenido con el proveedor, lo que impide una adecuada gestión de las tareas que realiza el mismo. Esto dificulta el control de los niveles de servicio acordado. Por lo tanto se mantiene la observación realizada por esta auditoría.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	con el proveedor a nivel de coordinación general, no permiten cumplir adecuadamente con el proceso de Gestión de Proveedores de TI, según lo establecen las buenas prácticas relativas a gestión de rendimiento de servicios.	Dadas las condiciones enunciadas, precedentemente, consideramos que se cumplen razonablemente los requerimientos de gestión de servicios provistos por el proveedor.	
4.12. No se realizan las reuniones trimestrales de Comisión Asesora para la Infraestructura de Firma Digital, orientadas a generar recomendaciones de mejoras en base a estándares tecnológicos.	Según lo establecido en la Ley 25.506, en el Decreto 2628/2002 y en la Resolución 435/2004, regularmente debe reunirse una "Comisión Asesora para la Infraestructura de Firma Digital", conformada por especialistas en la materia. El objetivo principal de dichas reuniones es generar y emitir recomendaciones por iniciativa propia o a solicitud de la Autoridad de Aplicación de la Ley 25.506 (Ley de Firma Digital), en materia de estándares tecnológicos, sistema de auditoría, requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados y otros aspectos que le sean requeridos. Del relevamiento realizado surge que la	**Comentarios** De acuerdo a la Ley 25.506, en el Capítulo VIII "De la Comisión Asesora para la Infraestructura de Firma Digital", en el artículo 35 sobre "Integración y Funcionamiento" se indica que "... Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez. Se reunirá como mínimo trimestralmente.... ". Del mismo modo, el Decreto Reglamentario 2628/02, en su CAPITULO III "DE LA COMISIÓNASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL", recepta los artículos 7 a 10,delimitando la Integración, Ejercicio de Funciones y Consulta Pública. Posteriormente, el Decreto Nº 160/2004 designa	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	Comisión Asesora para la Infraestructura ha sido designada por el Poder Ejecutivo. No obstante ello, se incumple con lo establecido normativamente respecto de la periodicidad de las reuniones. Según la ley de Firma Digital, la comisión debe reunirse al menos una vez cada 3 meses. Sin embargo, el trabajo de campo realizado señala que sólo se reunieron una vez. Al no realizarse las reuniones de Comisión Asesora para la Infraestructura, se carece de los productos y herramientas que dicha Comisión debe generar en términos de soporte y asesoramiento a los titulares o potenciales titulares de certificados.	a los integrantes de la COMISIÓN ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL. Por último, la Resolución JGM N° 435/2004, aprueba el reglamento de funcionamiento de la COMISIÓN ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL. Finalmente, se informa que desde la designación de los integrantes efectuada por el Decreto Nº 160/2004 no se han renovado ni designado nuevos miembros. **Plan de Acción** Teniendo en cuenta el marco normativo aplicable, y la designación realizada por el Decreto Nº 160/2004, la designación de nuevos integrantes podría interpretarse como una facultad del PODER EJECUTIVO NACIONAL.	
4.13. Se encuentran desactualizados los procedimientos y guías técnicas sobre la plataforma e infraestructura tecnológica de Firma	Los documentos que describen los procedimientos técnicos de la ONTI sobre la plataforma e infraestructura tecnológica de Firma Digital fueron generados en septiembre de 2010, y no se cuenta con versiones actualizadas a la fecha de cierre de esta auditoría. Dichos documentos abarcan los	**Comentarios** a. Cabe destacar que los documentos referidos, definen un Procedimiento de Instalación de SO y configuración de todos los servidores que se encuentran en la infraestructura de firma digital. Si bien dichos documentos datan del año 2010, los servidores siguen en funcionamiento y no	En la respuesta del organismo se reconoce el cambio del sistema operativo, lo cual se considera un cambio significativo, que refuerza la necesidad observada de

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
Digital utilizadas por el personal de soporte de la ONTI, lo que genera dependencia de personal clave.	siguientes temas: • Plataforma Tecnológica: Requerimientos a nivel de negocio, de usuario, de seguridad y de operación. Infraestructura de la solución PKI 2.0, Inventario de equipos, Arquitectura de procesadores, Configuración del Software, Arquitectura de Red, Bases de Datos (Diccionario de datos, DER, etc.) • Plan de Contingencia y Procedimiento de la Declaración de Contingencia • Documentación para la instalación de servidores y aplicativos • Documentación sobre los aplicativos provistos por la empresa DATCO para el soporte de los procesos y procedimientos de Firma Digital. A partir de entrevistas realizadas y del análisis y revisión de la documentación provista por el auditado, se concluye que los documentos son suficientes y cuentan con un alcance adecuado en relación a los aspectos que conforman la plataforma e infraestructura tecnológica de	fueron cambiados, por lo que todos los procesos definidos en el documento se encuentran vigentes. b. Los mencionados manuales son de utilización frecuente; por ejemplo para generar e instalar el certificado SSL que se utiliza para la comunicación de los TMG con los sitios WEB. c. Cabe mencionar que se actualizó el sistema operativo Windows Server 2008 R2 de IDPM por Windows Server 2012 R2. **Plan de Acción** Se deja constancia que la plataforma tecnológica no presenta cambios significativos, por lo cual los procedimientos permanecen vigentes. Se tendrá en cuenta la observación al implementar la nueva Infraestructura.	actualización de documentación. Por lo tanto se mantiene la observación, mientras que las mejoras realizadas en función del Plan de Acción mencionado se evaluaran en futuras auditorias. Es una buena práctica mantener actualizados los manuales de procedimientos, independientemente de la envergadura del cambio.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	Firma Digital. No obstante, la brecha existente entre la documentación vigente y la infraestructura actualmente instalada no permite dar un adecuado soporte al personal técnico a cargo de la administración de la plataforma tecnológica de Firma Digital. Esto genera una dependencia de personal clave para la realización de ciertas tareas, dificultando que las mismas sean llevadas a cabo en su ausencia, o ante la incorporación de personal .		
4.14. Los legajos de las Autoridades Certificantes no cuentan con un soporte digital adecuado para realizar consultas, revisiones y actualizaciones.	En el marco de los procedimientos administrativos de la Subsecretaría de Tecnologías de Gestión, los legajos de las Autoridades Certificantes que administra la Dirección de Innovación Tecnológica se gestionan en formato impreso. Durante las tareas de campo se relevaron legajos correspondientes a habilitación y seguimiento de Autoridades Certificantes. Como parte del circuito administrativo los legajos pasan por diferentes sectores, tanto dentro de la Subsecretaria de Tecnologías de	**Comentarios** El Decreto N2 561/2016 aprueba la implementación del sistema de Gestión Documental Electrónica -GDE- como sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional. Dicho sistema actúa como plataforma para la implementación de gestión de expedientes electrónicos. Asimismo, la documentación de los suscriptores de los certificados de firma digital, luego de su aprobación es escaneada y conservada en el	La respuesta del organismo no contradice las observaciones realizadas por esta auditoría, por lo tanto de se mantienen las mismas. Los cambios realizados en el Plan de Acción propuesto se evaluaran en futuras auditorias.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	Gestión como de la Autoridad Certificante pertinente. Ante cada corrección requerida en la cadena de verificación documental, el procedimiento contempla la reimpresión completa del documento antecedente, lo que deriva en una multiplicación exponencial de documentos, hecho que se pudo constatar mediante inspección ocular Cabe señalar que la Ley de Firma Digital establece en su Artículo 48 que: "El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la Firma Digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.". Y luego agrega que: "En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de Firma Digital a la totalidad de las	sistema de la aplicación de PKI, para su posterior consulta por los Oficiales de Registro, de forma digitalizada, y firmada digitalmente por el Oficial de Registro que ha aprobado la solicitud del certificado. **Plan de Acción** Con el objetivo de fortalecer la tarea de minimizar la utilización de documentos basados en papel, sin menoscabo alguno a la seguridad jurídica, y a los fines de dar cumplimiento con el Decreto Nº 561/16 que aprueba el sistema de GESTIÓN DOCUMENTAL ELECTRÓNICA (GDE), los nuevos procesos de licenciamiento deberán realizarse en formato digital y tramitarse endicho sistema.	

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
	leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156." La gestión de documentos actual deriva en legajos voluminosos, lo que además de dificultar su acceso, eleva los costos de archivo y gestión documental. Si bien se cuenta con los documentos escaneados, su accesibilidad es poco eficiente y redunda en una contradicción entre la realidad de los procedimientos administrativos de la oficina y el principio de despapelización que da impulso al desarrollo de la Firma Digital.		
4.15. El Sistema de Registro de Firma Digital en el que se registra la información personal de los subscriptores de Firma Digital de AC-ONTI, admite que	En la base de datos de AC-ONTI se almacenan los datos personales de todos los subscriptores a su servicio de Firma Digital. Muchos de estos datos deben estar almacenados de forma obligatoria. Sin embargo, estos campos están configurados de forma tal que pueden quedar vacíos. Durante las tareas de campo, en una inspección a una copia de respaldo de la base	**Comentarios** Considerando que la auditoría alcanzó el período comprendido entre el 31/07/2014 y el31/07/2015, teniendo en cuenta que "... las tareas de campo se desarrollaron de septiembre a diciembre de 2015", cabe destacar las siguientes aclaraciones: a. Durante el transcurso del período mencionado,	El diseño actual de la base de datos, para no modificar registros existentes almacenados de acuerdo a las necesidades de información establecidas por Resoluciones Administrativas anteriores, permite la

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
puedan no cargarse datos que son considerados imprescindibles, lo que atenta contra la completitud de la información allí almacenada.	de datos activa, se pudo comprobar que utilizando esta debilidad de diseño, una serie de subscriptores no contaban con uno o más de estos datos obligatorios (por ejemplo CUIT), a pesar de que estos datos son confirmados personalmente ante la Dirección de Innovación Tecnológica previo a la emisión del certificado. Por otra parte, hay campos que utilizan formatos de datos ineficientes o no recomendados por las buenas prácticas de diseño de bases de datos. La base de datos debe contar con un diseño tal que impida la carga de datos de formato distinto al esperado, y que exija la carga de datos que son considerados imprescindibles. Estas fallas de diseño acarrean el riesgo de no contar con información fidedigna en el momento de requerirse.	hasta mayo de 2015 los certificados eran emitidos conforme la Decisión Administrativa Nº 6/2007 y en cumplimiento de la "Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado" de la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI), aprobada por ,la Resolución de la ex SECRETARÍA DE LA GESTIÓN PÚBLICA Nº 227/2010. b. Asimismo, dicha Política de Certificación de la AC ONTI aprobada por la Resolución ex SGP Nº 227/2010, tenía un perfil de certificado distinto al actualmente vigente, que contenía diferentes campos. Posteriormente, la Decisión Administrativa Nº 927/2014 (De fecha 30/10/2014),entre otros cambios significativos, incorpora la Política Única de Certificación, y establece un perfil único de certificado interoperable entre certificadores licenciados, con lo cual no pueden agregarse campos a los perfiles aprobados endicha Decisión Administrativa.	existencia de campos vacíos (null). De esta forma, es posible cargar nuevos datos sin completar otros que en la actualidad son obligatorios. Teniendo en cuenta la existencia de distintas formas de superar este inconveniente, sin la necesidad de hacer que los campos obligatorios pueda dejarse en blanco en la base de datos, se mantiene la observación.

INFORME DE AUDITORIA

N° de Observación	Observación	Respuesta ONTI	Comentario AGN
		Del mismo modo, la Disposición SsTG Nº 7/2015 (De fecha 10/09/2015) aprueba las "ACLARACIONES TÉCNICAS ESPECÍFICAS PARA LA DECISIÓN ADMINISTRATIVA Nº 927/2014". Por último, la Disposición SsTG Nº 11/2014 aprueba la adhesión a la POLÍTICA ÚNICADE CERTIFICACIÓN de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI). c. Al respecto, y a la fecha coexisten certificados emitidos bajo la Política de Certificación aprobada por la Resolución ex SGP Nº 227/2010 que actualmente se encuentran vigentes, con aquellos aprobados en conformidad de la POLÍTICA ÚNICADE CERTIFICACIÓN aprobada por la Disposición SsTG Nº 11/2014. En particular, respecto al campo CUIT, debe aclararse que el mismo solo resulta obligatorio a partir de la vigencia de la nueva Política única de Certificación, con lo cual algunos certificados tendrán el campo CUIT.	