

Tema	Auditoria de Gestión
Año y norma aprobatoria del informe	Res 264/2016
Jurisdicción	Nacional
Organismo de control	Auditoria General de la Nación
	ONTI-OFICINA NACIONAL DE TECNOLOGIA DE INFORMACION
Objetivo	Firma Digital en el Estado Argentino
Período analizado	Desde 31/07/2014 al 31/07/2015
Año en que se realizó	Setiembre a Diciembre 2015
Fuente	http://www.agn.gov.ar/files/informes/2016_264info.pdf

OBJETO

La Auditoría General de la Nación efectuó una evaluación del estado de las tecnologías de información en el ámbito de la ONTI –OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION referida a la “firma digital en el Estado Argentino”. El período auditado abarcó desde el 31/07/2014 al 31/07/2015. El informe fue aprobado por Resolución 264 del 16 de noviembre de 2016.

SINTESIS

¿Qué es la “firma digital”?

Es un procedimiento matemático que requiere información exclusiva del firmante y que, aplicado a un documento digital, le otorga validez al mismo. En nuestro país está regulada por la Ley 25.506. Es a los soportes digitales lo que la firma holográfica a los documentos en papel.

A nivel informático, se trata de un pequeño archivo denominado “código hash” que se genera al aplicarlo al documento a ser firmado. La validez del “código hash” reposa en su autenticidad otorgada por un doble proceso de encriptación y desencriptación que se genera con una doble clave: una privada (que solo conoce el firmante) y una pública que la recibe el destinatario del documento o archivo y se usa para desencriptar el código hash. De este modo el destinatario puede constatar la validez de la firma recibida.

Ahora bien, para asegurar que el emisor o firmante sea quien dice ser, es decir para evitar sustituciones de identidades, se emiten Certificados Digitales expedidos por instituciones facultadas al efecto que se denominan Autoridades Certificantes o Certificadores Licenciados que son también Autoridades de Registro porque quedan asentados ahí quienes poseen firma digital quienes a su vez deben ser previamente autorizados o certificados por una Autoridad Certificante Raíz y Ente Licenciente.

Todo este proceso, está normado por la mencionada Ley 25.506 que derogó el Decreto 427/98. La Oficina Nacional de Tecnologías de Información (ONTI) es quien regula, promueve y verifica el proceso de firma digital.

Observaciones efectuadas por los auditores:

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”. Recordemos que el ONTI concentra entonces las funciones de Autoridad Certificante Raíz y de Autoridad Certificante.

El Decreto 2628/02 reglamenta la Ley de Firma Digital y crea el Ente Administrador de Firma Digital quien debía supervisar la actividad de los certificadores licenciados y otorgar las licencias. Sin embargo, en el año 2003 se disuelve dicho Ente Administrador y sus funciones pasan a la ONTI generando una incompatibilidad que AGN señala como observación ya que dicha oficina ya era Autoridad Certificante.

2.El nivel de seguridad física de la oficina donde opera la Autoridad de Registro ONTI (donde se entregan los certificados de firma digital) es inferior al que indica la norma, lo que pone en riesgo la seguridad y confidencialidad de la infraestructura de Firma Digital.

Durante las tareas de campo se verificó que el ingreso a las oficinas no era controlado ni registrado, ni tampoco se constato la existencia de un libro de Visitas, esto impide que quede registrado quien visita un área donde se maneja información sensible, de hecho la norma establece que los requisitos de seguridad serán los de NIVEL 1.

3.La Direccion de Administracion Tecnológica 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.

Esta área brinda el servicio de housing para los servidores de procesamientos de datos de Firma Digital. Según señalaron a la auditoría, existen restricciones edilicias que dificultan el emplazamiento de un grupo electrógeno. Señala AGN que el mayor riesgo es que ante un corte prolongado de energía se puede afectar la generación de los listados de firmas revocadas con el peligro de que puedan ser tomadas como válidas firmas que deberían encontrarse bloqueadas.

4.La política de back up de PKI (Public Key Infrastructure-Infraestructura de clave pública), cuenta con debilidades en sus procedimientos que podrían afectar la disponibilidad de información y sus respectivos servicios. La auditoria verificò que este documento especifica que bases de datos y aplicativos deben ser resguardados pero no especifica el procedimiento a seguir para hacerlo, además no hay procedimientos de prueba de restauración de back up. Además no se guardan copias de back up, fuera del edificio.

5.El Ente Licenciante no lleva a cabo con la periodicidad estipulada las auditorias de seguimiento sobre las autoridades certificadoras y de registro.

Según la Ley 25.506 la Autoridad Raíz o Ente Licenciante debe efectuar controles anuales sobre las Autoridades Certificadoras. Hasta la fecha de la auditoría solamente habían sido controlados las Autoridades Certificadoras de AFIP y ANSES (las únicas habilitadas en el Estado) y ninguna de las Autoridades Certificadoras privadas, de estas últimas la más antigua es ECODE que opera desde 2012. En tanto ANSES y AFIP fueron auditadas solo una vez en los ocho años que operan como certificadoras.

6.Se encuentran desactualizados los procedimientos sobre la plataforma de Firma Digital utilizadas por el personal de soporte de ONTI lo que genera dependencia de personal clave.

AGN señala “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”.

7.Los legajos de autoridades certificadoras no cuentan con un soporte digital adecuado para realizar consultas, revisiones y actualizaciones.

Los auditores señalan que los trámites de habilitación de Autoridades Certificadoras se efectúan en formato papel y que la gestión documental en este formato “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”.