JEFATURA DE GABINETE DE MINISTROS

SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA

SUBSECRETARIA DE TECNOLOGIAS DE GESTION

OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION

Disposición Nº 1/2014

Bs. As., 7/7/2014

VISTO el Expediente CUDAP: EXP-JGM:0014954/2014, el Decreto Nº 624 de fecha 21 de agosto de 2003 y sus modificatorios, las Resoluciones Nº 41 del 2 de diciembre de 2001 y Nº 27 del 30 de abril de 2002 de la ex SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS, y la Disposición Nº 1 del 24 de Julio de 2013 de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION de la SUBSECRETARIA DE TECNOLOGIAS DE GESTION, de la entonces SECRETARIA DE GABINETE, de la JEFATURA DE GABINETE DE MINISTROS, y

CONSIDERANDO:

Que por el Artículo 1° de la Disposición Nº 1 del 24 de Julio de 2013 de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION de la SUBSECRETARIA DE TECNOLOGIAS DE GESTION de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS se aprobaron los “Estándares Tecnológicos para la Administración Pública Nacional” (ETAPS) Versión 19.0, en materia de tecnologías de información y comunicaciones asociadas.

Que dichos estándares deben ser objeto de revisión periódica, de modo de garantizar que sus contenidos reflejen los últimos adelantos en la materia.

Que conforme a la normativa de aplicación, en particular el Decreto Nº 624/03 y sus modificatorios, compete a esta Oficina Nacional mantener actualizados los estándares sobre tecnologías en materia informática, teleinformática o telemática, telecomunicaciones, ofimática o burótica.

Que por el Artículo 1° de la Resolución Nº 27/02 de la ex SUBSECRETARIA DE LA GESTION PUBLICA se facultó a la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION a aprobar las especificaciones técnicas de los distintos ítems que componen los “Estándares Tecnológicos para la Administración Pública Nacional” (ETAPS) que reemplacen en forma total o parcial a los vigentes, de acuerdo a lo reglamentado por la Resolución Nº 41/01 de la ex SUBSECRETARIA DE LA GESTION PUBLICA.

Que la SUBSECRETARIA DE TECNOLOGIAS DE GESTION de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS ha tomado la intervención de su competencia.

Que la DIRECCION GENERAL DE ASUNTOS JURIDICOS de la SUBSECRETARIA DE COORDINACION ADMINISTRATIVA de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS ha tomado la intervención de su competencia.

Que la presente se dicta en virtud de las facultades conferidas por el artículo 1° de la Resolución Nº 27/02 de la ex SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Por ello,

EL DIRECTOR NACIONAL DE LA OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION

DISPONE:

ARTICULO 1° — Actualízase los “Estándares Tecnológicos para la Administración Pública Nacional” (ETAPS) Versión 19.0 que como Anexo forma parte integrante de la presente, en lo vinculado a los elementos de seguridad identificados con los Códigos SEG-001 y SEG-002, aprobados por la Disposición Nº 1 del 24 de Julio de 2013 de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION de la SUBSECRETARIA DE TECNOLOGIAS DE GESTION de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS.

ARTICULO 2° — El equipamiento, las tecnologías, las guías y lineamientos y los modelos de pliegos no incluidos en el referido Anexo, y que fueran aprobados por Disposición ONTI Nº 1/13, mantienen su código, nombre, vigencia y especificación técnica.

ARTICULO 3° — Las actualizaciones referidas en el artículo 1° de la presente medida, serán de aplicación en toda la Administración Pública Nacional, tanto centralizada como descentralizada, empresas de propiedad del Estado o en las que éste tenga mayoría accionaria, bancos oficiales y Fuerzas Armadas y de Seguridad, con la única salvedad de los organismos comprendidos en el Sistema Científico Nacional.

ARTICULO 4° — A partir de la entrada en vigencia de la presente disposición, los organismos comprendidos dentro de su ámbito de aplicación deberán dar cumplimiento a las especificaciones técnicas establecidas para todas las compras y contrataciones que se propongan celebrar en materia de tecnologías de información y comunicaciones asociadas.

ARTICULO 5° — Las actualizaciones referidas en el artículo 1° de la presente medida, se publicarán en el sitio web de la JEFATURA DE GABINETE DE MINISTROS (www.jefatura.gov.ar) a fin de facilitar su utilización por parte de los distintos usuarios.

ARTICULO 6° — La presente Disposición entrará en vigencia a partir del día siguiente al de su publicación.

ARTICULO 7° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — PEDRO JANICES, Director Nacional, Oficina Nacional de Tecnologías de Información.

ANEXO

ELEMENTOS DE SEGURIDAD (SEG-E)

Consideraciones Preliminares

Las páginas siguientes contienen los pliegos de especificaciones técnicas que deberán utilizarse para la adquisición de equipamiento. El organismo deberá completar el mismo del siguiente modo:

1. Se deberán elegir los opcionales (ver más abajo, en “Notas”, las consideraciones sobre los tipos de opcionales q y m) que más se adecuen a las necesidades del organismo, eliminando aquellas especificaciones no seleccionadas. Por ejemplo:

✓ Plataformas soportadas

☒ Windows XP/Vista/7/2003/2008 Server (*opción seleccionada*)

☐ ~~Linux (opcional)~~ (*opción no seleccionada. eliminar*)

2. Las especificaciones no deben ser transcriptas al pie de la letra, puesto que contienen comentarios para la realización del pliego definitivo que no deben figurar en la especificación final. A modo de ejemplo, debajo figuran en color rojo aquellos textos que no deben incluirse en la versión
final:

a. Notas: [Nota: Un escáner de 30 ppm se debería considerar para grandes volúmenes de trabajo...];

b. Aclaraciones <entre signos>: [❑ Unix <indicar versión de ser necesario... SCO, AIX, UX. etc.>];

c. Secciones en las que se debe completar con información: [...el edificio sede de ... *(ORGANISMO)*... sito en ... *(DIRECCIÓN)*... de esta Capital Federal...].

Notas:

Se recuerda tener en cuenta las siguientes consideraciones:

Se recuerda tener en cuenta las siguientes consideraciones:

✓ Opción Múltiple: Cuando alguno o varios elementos se encuentren precedidos por viñetas del tipo ❑, ello significa que se puede elegir una o varias de las opciones indicadas.

✓ Opción mutuamente excluyente: Cuando alguno o varios elementos se encuentren precedidos por viñetas del tipo ❍, ello significa que se puede elegir sólo una de las opciones mostradas.

✓ Todas las características que se detallan a continuación son datos tomados del promedio de los equipos que actualmente se ofrecen en el mercado. El organismo deberá tomarlas como referencia, adoptando para cada elemento las opciones que más se adecuen a sus necesidades.

✓ Para el caso en que el organismo requiera especificar algún ítem con características que no se encuentran dentro de las presentadas en este ETAP, deberá adjuntar la justificación correspondiente al requerimiento solicitado en la nota de solicitud de dictamen técnico.

Dispositivos Criptográficos - TOKEN (Windows)

SEG-001

Dispositivos criptográficos con las siguientes características:

Presentación:

√ Carcasa de protección compuesta de un material robusto, resistente al agua y firmemente sellado a fin de no permitir el ingreso de líquidos.
√ Características de ‘tamper-evident’.
√ Interfase USB estándar tipo A, versión 1.1 o superior.
√ Debe tener un LED indicador de actividad.

Características Técnicas:

√ Tecnología Plug-and-Play para facilitar su utilización con aplicaciones cliente.
√ Debe permitir implementar ‘Doble Factor’ de autenticación, es decir que es necesario a tal fin poseer el dispositivo criptográfico y una contraseña.
√ Autenticación interna (on-board).
√ Permitir la obtención del número de serie del dispositivo criptográfico mediante la API PKCS# 11.
Nota para los organismos: En el marco de la Infraestructura de Firma Digital creada por la Ley Nº 25.506 y sus normas complementarias, la certificación FIPS 140-2 Nivel1/2 o superior puede ser requerida en algunas Políticas de Certificación, por lo que si el uso al que se destinará el TOKEN se encuentra entre los establecidos por las referidas normas, este opcional debe incluirse en la especificación técnica. Si el dispositivo se utilizará como un simple dispositivo criptográfico, este opcional no es obligatorio.

❑ Contar con certificación FIPS 140-2 Nivel 1 o superior que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

❑ Contar con certificación FIPS 140-2 Nivel 2 o superior, que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

❑ Contar con certificación FIPS 140-2 Nivel 3 o superior que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

Aplicaciones Soportadas:

√ Windows logon (opcional)
√ Clientes de e-mail:

- Microsoft Outlook / Outlook Express & Internet Explorer,

Especificaciones Técnicas del producto:

√ Plataformas soportadas

- Windows Vista/7/8/8.1 o superior

- Windows 2003/2008 Server R2 o superior

√ APIs y estándares soportados

- PKCS#11 v2.01 o superior,

- Microsoft Crypto API (CAPI) 2.0 o superior,

- Microsoft PC/SC (Personal Computer Smart Card),

- SSL v3,

- IPSec/IKE

√ Tamaño de memoria de al menos 32 Kbytes.
√ Deberá soportar las siguientes funciones criptográficas (on board)

- Algoritmo de Generación Aleatoria de Números (RNG)

√ La generación aleatoria de números debe realizarse por hardware e internamente en el dispositivo.

Nota para los organismos: La opción de que el Generador de Números Aleatorios (RNG) esté certificado por FIPS-186-2 brinda mayor seguridad en el caso de que se opere con claves asimétricas del tipo DSA, ya que en este caso, un RNG vulnerable compromete la clave privada. Por lo tanto, salvo en entornos donde la seguridad es crítica, seleccionar esta opción podría restringir innecesariamente el espectro de oferentes posibles.

❑ Debe estar certificado por FIPS-186-2.

- Generación interna, operación, almacenamiento y administración de claves criptográficas asimétricas del tipo RSA (1024 bits o superior), DSA o superior.

- Generación de claves simétricas: Generación interna, y operación de claves criptográficas simétricas del tipo Triple DES, AES o superior.

- Almacenamiento de certificados X509v3.

- Capacidad de exportación de Certificados Digitales x509 v3

- Algoritmo de Hash: Funciones de hash seguro del tipo SHA-1, SHA-2, o superior.

Características administrativas y de uso:

√ Los dispositivos deberán contar con sus respectivas licencias de uso (de corresponder) y los correspondientes drivers y aplicativos necesarios para su funcionamiento.
√ Deberá contar con software asociado que permita definir usuarios administradores y usuarios comunes, formateo del dispositivo para restaurar a valores de fábrica.
√ No deberá tener posibilidad de exportar la clave privada, ni hacer copias de la misma.

OTRAS:

Deberá ser un producto vigente, con soporte técnico y no poseer fecha de discontinuidad de fabricación al momento de efectuarse la presentación de solicitud de homologación.

El oferente deberá garantizar también soporte de actualización de los drivers y firmware del dispositivo, sin costo alguno para el organismo, durante un período no inferior a <indicar> años a partir de la fecha de compra del mismo.

El oferente deberá brindar servicio de soporte a los usuarios poseedores de dispositivos.

Deberá tratarse de dispositivos criptográficos del fabricante cuya marca y modelo y versión de hardware y firmware coincida con la marca, y modelo y versión declarada en las correspondientes Certificaciones FIPS 140, no pudiendo ser dispositivos criptográficos del tipo OEM (Original Equipment Manufacturer).

El oferente deberá entregar el software, los manuales y demás documentación, preferentemente en idioma español, o en su defecto, en idioma Inglés.

Adicionalmente, el oferente deberá acompañar:

• Detalle de los números de serie de los dispositivos criptográficos que componen cada uno de los lotes reservados por el fabricante, incluyendo además de los números de serie, la marca, modelo, versión de “software”, de “firmware” y de “hardware”, así como el número de certificación FIPS correspondiente.

• Declaración debidamente firmada por el proveedor señalando que posee la capacidad de brindar soporte técnico a los usuarios de los dispositivos criptográficos comercializados por un período no inferior a TRES (3) años.

• Nota original del fabricante de los dispositivos la que, de tratarse de persona extranjera, deberá contar con la pertinente legalización consular o, en su caso con la apostilla, conforme a la Convención de La Haya, según el siguiente texto:

“Por cuanto [indicar apellido y nombre completo del fabricante], en el carácter de fabricante de los Dispositivos Criptográficos marca [indicar marca] modelo [indicar modelo] y sus licencias de “software” correspondientes, con domicilio en [agregar dirección completa del fabricante], por medio de la presente informamos a Uds. que hemos procedido a reservar inicialmente para la Infraestructura de Firma Digital de la República Argentina y/o los usuarios finales ante la Infraestructura de Firma Digital de la República Argentina, cuyos números de serie están incluidos en el siguiente rango [ingresar el rango].

Asimismo, por la presente autorizamos a [nombre del solicitante que pretende su incorporación como proveedor], con domicilio en [indicar dirección completa del solicitante en la República Argentina] a comercializar en la República Argentina a los usuarios finales ante cualquier entidad que conforme la Infraestructura de Firma Digital de la República Argentina solamente los dispositivos criptográficos Marca ..... Modelo ....., cuyos números de serie se encuentren comprendidos dentro del rango descripto anteriormente como lote reservado para la Infraestructura de Firma Digital de la República Argentina, así como a prestar los servicios de soporte técnico de dichos dispositivos”.

• Modalidad mediante la cual brindará soporte técnico a los usuarios de los dispositivos criptográficos comercializados.

Dispositivos criptográficos con las siguientes características:

Presentación:

√ Carcasa de protección compuesta de un material robusto, resistente al agua y firmemente sellado a fin de no permitir el ingreso de líquidos.
√ Características de 'tamper-evident'.
√ Interfase USB estándar tipo A, versión 1.1 o superior.
√ Debe tener un LED indicador de actividad.

Características Técnicas:

√ Tecnología Plug-and-Play para facilitar su utilización con aplicaciones cliente.
√ Debe permitir implementar 'Doble Factor' de autenticación, es decir que es necesario a tal fin poseer el dispositivo criptográfico y una contraseña.
√ Autenticación interna (on-board).
√ Permitir la obtención del número de serie del dispositivo criptográfico mediante la

API PKCS# 11.

Nota para los organismos: En el marco de la Infraestructura de Firma Digital creada por la Ley Nº 25.506 y sus normas complementarias, la certificación FIPS 140-2 Nivel 1/2 o superior puede ser requerida en algunas Políticas de Certificación, por lo que si el uso al que se destinará el TOKEN se encuentra entre los establecidos por las referidas normas, este opcional debe incluirse en la especificación técnica. Si el dispositivo se utilizará como un simple dispositivo criptográfico, este opcional no es obligatorio.

❑ Contar con certificación FIPS 140-2 Nivel 1 o superior que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

❑ Contar con certificación FIPS 140-2 Nivel 2 o superior, que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

❑ Contar con certificación FIPS 140-2 Nivel 3 o superior que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

Especificaciones Técnicas del producto:

√ Plataformas soportadas

- Linux

√ APIs y estándares soportados

- PKCS#11 v2.01 o superior,

- SSL v3,

- IPSec/IKE

√ Tamaño de memoria de al menos 32 Kbytes.
√ Deberá soportar las siguientes funciones criptográficas (on board)

- Generación interna, operación, almacenamiento y administración de claves criptográficas asimétricas del tipo RSA (1024 bits o superior), DSA o superior.

- Generación de claves simétricas: Generación interna, y operación de claves criptográficas simétricas del tipo Triple DES, AES o superior.

- Almacenamiento de certificados X509v3.

- Capacidad de exportación de Certificados Digitales x509 v3.

- Algoritmo de Hash: Funciones de hash seguro del tipo SHA-1, SHA-2, o superior.

- Algoritmo de Generación Aleatoria de Números (RNG).

√ La generación aleatoria de números debe realizarse por hardware e internamente en el dispositivo.

Nota para los organismos: La opción de que el Generador de Números Aleatorios (RNG) esté certificado por FIPS-186-2 brinda mayor seguridad en el caso de que se opere con claves asimétricas del tipo DSA, ya que en este caso, un RNG vulnerable compromete la clave privada. Por lo tanto, salvo en entornos donde la seguridad es crítica, seleccionar esta opción podría restringir innecesariamente el espectro de oferentes posibles.

❑ Debe estar certificado por FIPS-186-2.

Características administrativas y de uso:

√ Los dispositivos deberán contar con sus respectivas licencias de uso (de corresponder) y los correspondientes drivers y aplicativos necesarios para su funcionamiento.
√ Deberá contar con software asociado que permita definir usuarios administradores y usuarios comunes, formateo del dispositivo para restaurar a valores de fábrica.
√ No deberá tener posibilidad de exportar la clave privada, ni hacer copias de la misma.

OTRAS:

Deberá ser un producto vigente, con soporte técnico y no poseer fecha de discontinuidad de fabricación al momento de efectuarse la presentación de solicitud de homologación. El oferente deberá garantizar también soporte de actualización de los drivers y firmware del dispositivo, sin costo alguno para el organismo, durante un período no inferior a <indicar> años a partir de la fecha de compra del mismo.

El oferente deberá brindar servicio de soporte a los usuarios poseedores de dispositivos.

Deberá tratarse de dispositivos criptográficos del fabricante cuya marca y modelo y versión de hardware y firmware coincida con la marca, y modelo y versión declarada en las correspondientes Certificaciones FIPS 140, no pudiendo ser dispositivos criptográficos del tipo OEM (Original Equipment Manufacturer).

El oferente deberá entregar el software, los manuales y demás documentación, preferentemente en idioma español, o en su defecto, en idioma Inglés.

Adicionalmente, el oferente deberá acompañar:

• Detalle de los números de serie de los dispositivos criptográficos que componen cada uno de los lotes reservados por el fabricante, incluyendo además de los números de serie, la marca, modelo, versión de “software”, de “firmware” y de “hardware”, así como el número de certificación FIPS correspondiente.

• Declaración debidamente firmada por el proveedor señalando que posee la capacidad de brindar soporte técnico a los usuarios de los dispositivos criptográficos comercializados por un período no inferior a TRES (3) años.

• Nota original del fabricante de los dispositivos la que, de tratarse de persona extranjera, deberá contar con la pertinente legalización consular o, en su caso con la apostilla, conforme a la Convención de La Haya, según el siguiente texto:

“Por cuanto [indicar apellido y nombre completo del fabricante], en el carácter de fabricante de los Dispositivos Criptográficos marca [indicar marca] modelo [indicar modelo] y sus licencias de “software” correspondientes, con domicilio en [agregar dirección completa del fabricante], por medio de la presente informamos a Uds. que hemos procedido a reservar inicialmente para la Infraestructura de Firma Digital de la República Argentina y/o los usuarios finales ante la Infraestructura de Firma Digital de la República Argentina, cuyos números de serie están incluidos en el siguiente rango [ingresar el rango].

Asimismo, por la presente autorizamos a [nombre del solicitante que pretende su incorporación como proveedor], con

domicilio en [indicar dirección completa del solicitante en la República Argentina] a comercializar en la República Argentina a los usuarios finales ante cualquier entidad
que conforme la Infraestructura de Firma Digital de la República Argentina solamente los dispositivos criptográficos Marca… Modelo… cuyos números de serie se encuentren comprendidos dentro del rango descripto anteriormente como lote reservado para la Infraestructura de Firma Digital de la República Argentina, así como a prestar los servicios de soporte técnico de dichos dispositivos".

• Modalidad mediante la cual brindará soporte técnico a los usuarios de los dispositivos criptográficos comercializados.

e. 14/07/2014 Nº 48670/14 v. 14/07/2014