

ANEXO 5

ESPECIFICACIONES TECNICAS DE SEGURIDAD Y REGISTRO DE LLAVES O FIRMAS DIGITALES

(A ser provisto por el despachador de aduana)

DISTRIBUCION

SOLO UN EJEMPLAR PARA EL SERVICIO NACIONAL DE ADUANAS

El ejemplar debe fotocopiar en papel blanco, tamaño oficio, de 32 cms de alto por 21,5 cms de ancho.

Sin embargo, se aceptarán reproducciones procesadas computacionalmente, debiendo respetarse el tipo de letra (Arial), espacios y márgenes que se señalan en el modelo adjunto.

ESPECIFICACIONES TECNICAS DE SEGURIDAD Y REGISTRO DE LLAVES O FIRMAS DIGITALES

Para la formalización de las destinaciones aduaneras mediante el sistema de transmisión electrónica de datos, se ha establecido en:

1. El Manual de Procedimientos Operativos para la Transmisión Electrónica presente, que los usuarios de aduana, sin perjuicio de las responsabilidades establecidas en la Ordenanza de Aduana y penales que procedan, incluidas las que contempla la Ley N° 19.223, serán directamente responsables, además, de todas las destinaciones formalizadas electrónicamente que se hayan transmitido con su firma digital registrada ante el Servicio Nacional de Aduanas.
2. En el numeral 2, subcapítulo II, capítulo V, del Manual señalado, que el mensaje CUSDEC será el medio válido para formalizar las destinaciones aduaneras a que se refiere el inciso segundo del artículo 71 de la Ordenanza de Aduanas.
3. En el numeral 5 y 6, capítulo II del Manual de Procedimientos Electrónicos, que el Servicio Nacional de Aduanas deberá conservar en archivo magnético la declaración numerada por éste, preservando su integridad e inviolabilidad, la que servirá de base para los efectos de las revisiones y/o fiscalizaciones que procedan. Asimismo, los usuarios de aduana autorizados a formalizar las destinaciones aduaneras por el sistema de transmisión electrónica de datos, deberán mantener en sus archivos magnéticos las destinaciones legalizadas electrónicamente por el plazo establecido en el número 3 del artículo 226 de la Ordenanza de Aduanas.

Los usuarios que solicitan autorización para Transmitir Electrónicamente alguna destinación aduanera, se compromete a cumplir con las especificaciones técnicas sobre normas de seguridad y firmas digitales que siguen:

1. **Integridad de secuencia:** asegurar que los mensajes generados por el usuario de aduana tengan un número de identificación único.
2. **Integridad de contenido:** asegurar que el contenido del mensaje generado sea el mismo que el recepcionado por el Servicio Nacional de Aduanas.
3. **Autenticación de origen:** verificar con certeza la identidad proclamada por el transmisor de una destinación aduanera.
4. **No repudiación de origen:** evitar que el usuario niegue la formalización de una destinación aduanera efectuada por medio del sistema de transmisión electrónica de datos ante el Servicio de Aduanas.
5. **No repudiación de recepción:** evitar que el Servicio Nacional de Aduanas niegue la recepción de una destinación aduanera formalizada por el despachador de aduana.

Los servicios **Integridad de contenido**, **Autenticación de origen** y **No repudiación de origen**, serán implementados mediante la **Firma digital**. Dicha firma cumplirá con las siguientes características técnicas y de confidencialidad:

1. Su valor se calculará con algoritmos de hash y este valor será encriptado usando algoritmos de llave pública y privada.
2. Para asegurar la validez de las llaves, necesarias en la firma digital, el usuario de aduana creará personalmente la llave privada y pública que utilizará, mediante el programa generador de llaves que provea la Red de Valor agregado por él escogida.

3. La llave privada y pública junto a su certificado resultante, será mantenida por el usuario en un medio magnético, sin perjuicio de la obligación que pesa sobre la Red de Valor Agregado de almacenar la llave pública para su posterior difusión.
4. En el evento que el usuario de aduana reemplace el par de llaves que utilice en la transmisión electrónica de las destinaciones aduaneras, dará cuenta inmediata de esta circunstancia y entregará el medio magnético en que mantenga el anterior par de llaves

Para los efectos de registrar la **Firma digital** en el servidor de archivos, la llave pública será retirada por el Servicio Nacional de Aduanas de los sistemas de la Red de Valor Agregado de que se trate, mediante los mensajes de servicio que esta última provea. Del mismo modo, el usuario retirará la llave pública del Servicio Nacional de Aduanas, a fin de registrarla en sus sistemas computacionales.

Los servicios de **Integridad de secuencia** y de **No repudiación de recepción**, serán implementados cuando el Servicio Nacional de Aduanas lo requiera, de la siguiente forma:

1. La **Integridad de secuencia**, incorporando un número correlativo agregado automáticamente por el sistema a fin de que el receptor verifique que la secuencia este correcta. En caso de fallar la secuencia lo registrará en un archivo.
2. La **No repudiación de recepción** se implemente mediante la generación del denominado mensaje AUTACK. Este mensaje, dirigido al originador del mensaje, contendrá el número del mensaje recibido, el estatus de recepción -- bueno, certificado inválido, firma inválida, originante desconocido, etcétera --, identificación del receptor y su firma.

El usuario que suscribe se obliga a cumplir con las normas de seguridad y registro de llaves o de firmas digitales, conforme a las especificaciones técnicas que anteceden. Adicionalmente, se obliga a efectuar las acciones necesarias para que sus socios, apoderados y auxiliares hagan lo propio en esta materia.

DIRECTOR NACIONAL DE ADUANAS

USUARIO DE TRANSMISION ELECTRONICA

Nombre: _____

Rut : _____

Valparaíso, ____ de _____ de ____.-