

MERCOSUR/CMC/DEC. N° 01/08

**ESPECIFICACIÓN DE CARACTERÍSTICAS TÉCNICAS DE LA
INFRAESTRUCTURA INFORMÁTICA PARA EL INTERCAMBIO
ELECTRÓNICO DE INFORMACIÓN DE OPERACIONES ADUANERAS
MEDIANTE EL SISTEMA DE INTERCAMBIO DE INFORMACIÓN DE LOS
REGISTROS ADUANEROS – INDIRA**

VISTO: El Tratado de Asunción, el Protocolo de Ouro Preto, la Decisiones N° 54/04 y 37/05 del Consejo del Mercado Común.

CONSIDERANDO:

Que el Sistema de Intercambio de Información de los Registros Aduaneros, -en adelante INDIRA-, se encuentra operativo y disponible en los cuatro Estados Partes.

Que se hace necesario establecer las especificaciones técnicas que garanticen el intercambio electrónico seguro, entendiendo como tal aquel que cumple con condiciones de autenticación, confidencialidad, integridad y restricción de acceso.

**EL CONSEJO DEL MERCADO COMÚN
DECIDE:**

Art. 1 – Aprobar las normas sobre “Especificación de Características Técnicas de la Infraestructura Informática para el Intercambio Electrónico de Información de Operaciones Aduaneras Mediante el Sistema INDIRA”, que consta como Anexo y forma parte de la presente Decisión.

Art. 2 - La información transmitida en esta plataforma informática será de uso exclusivo de funcionarios de gobierno especialmente designados cuya identidad sea debidamente autenticada por los sistemas de seguridad propios de cada Aduana.

Art. 3 – Las normas de carácter técnico aprobadas por la presente Decisión y que constan en el Anexo, podrán ser modificadas por Directiva de la Comisión de Comercio del MERCOSUR, como consecuencia de la evolución natural de la tecnología y/o nuevos requerimientos que lo justifiquen.

Art. 4 – Los Estados Partes deberán incorporar la presente Decisión a sus ordenamientos jurídicos internos antes del 01/1/09.

XXXV CMC – San Miguel de Tucumán, 30/VI/08

ANEXO

ESPECIFICACIÓN DE CARACTERÍSTICAS TÉCNICAS DE LA INFRAESTRUCTURA INFORMÁTICA PARA EL INTERCAMBIO ELECTRÓNICO DE INFORMACIÓN DE OPERACIONES ADUANERAS MEDIANTE EL SISTEMA DE INTERCAMBIO DE INFORMACIÓN DE LOS REGISTROS ADUANEROS – INDIRA

Artículo 1°.- Introducción y Objetivos

El presente anexo establece las Normas utilizadas para la conectividad entre aduanas de los Estados Partes, para los sistemas que requieran de transferencia parcial o total de datos, ya sean estos por lotes o en transacciones ON-LINE. Se incluyen también recomendaciones de aplicación de estándares globales y particulares de cada Estado Parte.

El objetivo principal es cubrir todas las normas necesarias para el trabajo de transferencia de datos entre Estados Partes y dar apoyo efectivo a nuevos emprendimientos que requieran conectividad, sin truncar protocolos internos respecto de normas de cada Estado Parte.

Artículo 2°.- Infraestructura

Cada Estado Parte deberá tomar recaudo de las necesidades para la conectividad, según las referencias establecidas en el presente anexo, sin perjuicio de las normas internas que no interfieran con el comportamiento normal de los canales de transferencia de información.

No obstante, la mínima infraestructura exigida es la que puede respaldar la configuración de túneles de seguridad a través de soporte de redes públicas.

2.1. Conectividad a Redes Públicas

Son requisitos de conectividad de cada Estado Parte:

- a. Cada Estado Parte deberá disponer de afiliación y conexión permanente a redes públicas que permitan las configuraciones de túneles referidos en el presente anexo para la transferencia de datos, en tiempo y forma.
- b. Las necesidades específicas de amplitud de estas conexiones deberán

proveerse en la documentación de cada sistema de transferencia de datos.

- c. Cada Estado Parte deberá prever la amplitud de conectividad necesaria para el funcionamiento de las transferencias de datos que realice. Se deberá informar en todos los casos, con suficiente antelación, los problemas de amplitud, tanto totales como parciales a los Estados Partes involucrados en las transferencias de datos.
- d. Los cambios que pudieran ocurrir a causa de cambios en la conectividad de cada Estado Parte a las redes públicas deberán ser informados a los demás Estados Partes, para prever con anticipación cambios en configuraciones.

2.2. Soporte físico de Conectividad

Se define como Soporte Físico de Conectividad a los equipos necesarios para conectividad a redes públicas, capaces de soportar las configuraciones de seguridad que se explican en el presente.

Los referidos equipos deberán cumplir con los siguientes requisitos:

- a. Los citados equipos deberán ser capaces de soportar las configuraciones citadas en el Artículo 3 del presente anexo, sin perjudicar los parámetros de amplitud de conectividad necesarios para tal efecto.
- b. Cada Estado Parte deberá hacer previsión constante de “Tolerancia a Fallos” y “Redundancia de Funcionamiento” de los citados equipos. Una situación de indisponibilidad de acceso por cambios programados deberá ser informada con suficiente antelación.

Artículo 3.- Configuraciones de Conectividad

Los Estados Partes acuerdan utilizar métodos estandarizados de transferencia de información que permitan cuidar los siguientes aspectos:

- *Transferencia Física de Paquetes*: cada Estado Parte deberá proveer sistemas de conectividad de acuerdo a las recomendaciones establecidas en el Artículo 2 relativas a la conexión a la red pública seleccionada como soporte de transmisión y la selección, instalación y configuración adecuada del soporte físico de conectividad.
- *Configuraciones Mínimas y Recomendaciones de Seguridad de Transferencia de Datos*: establecidas en este anexo según las cuales se deben cumplir normas necesarias para preservar la seguridad en la transferencia de datos y las demás que puedan ser implantadas de mutuo acuerdo.
- *Definiciones de Acceso a Aplicaciones*: definen los protocolos que serán

utilizados para publicar aplicaciones.

Los ítems de Configuraciones de Conectividad referidos en este artículo deberán cumplir los siguientes requisitos / respetar las siguientes condiciones:

3.1. Transferencia Física de Paquetes

Se designa como Red Pública a “INTERNET” (RFC0774), y según este ítem, cada Estado Parte deberá realizar todas las provisiones necesarias para conectividad, incluyendo el manejo individual de contratos con proveedores (ISP-Internet Service Provider). Bajo esta situación, se utilizará el protocolo TCP/IP (RFC0791 y RFC0793) como soporte general a las transferencias de información.

Cada Estado Parte deberá poseer una identificación relativa a la Red Pública, denominada “*Dirección IP Pública*” que será provista a los demás Estados Partes para las configuraciones citadas en el punto 3.2. de este Artículo.

Cada Estado Parte deberá realizar su propio estudio de necesidades de amplitud de conectividad, denominado en este caso como “Ancho de Banda” de acuerdo a necesidades internas, haciendo la correspondiente reserva para transferencias de datos citadas en este documento.

Cualquier previsión de “Tolerancia a Fallos” o “Redundancia” será gestionada por cada Estado Parte, con previsión de infraestructura, citada en el Artículo 2.2.b. o a través de acuerdos con los citados proveedores de servicios de Internet.

3.2. Configuraciones y Recomendaciones de Seguridad de Transferencia de Datos

Tomando en cuenta la elección de Redes Públicas y el citado protocolo TCP/IP como soporte de transferencia de datos, se decide utilizar “Túneles protegidos” para transferencia de datos.

El protocolo que deberá ser utilizado es el IPSec (RFC2401). Cada Estado Parte deberá informar los parámetros utilizados variables de conectividad, en tanto que algunos serán fijos para lograr la estandarización de los procedimientos de configuración.

3.2.a. Parámetros Fijos

- Red Pública Internet
- Protocolo base, TCP/IP
- IPSec
 - Algoritmo de Encriptación 3DES (RFC1851)
 - Algoritmo de Hash MD5 (RFC1321)
 - Método de Autenticación Pre-Share (Contraseñas compartidas por anticipado)
 - Intercambio de Claves 1024bits

- Set de transformación ESP-3DES-MD5-tunnel
- Establecimiento del SA ipsec-isakmp

3.2.b. Parámetros Variables

- Dirección Relativa Única de la Red Pública (Dirección IP Pública de Internet)
- Dirección Relativa Única de los Servidores de Aplicaciones (Dirección IP)

3.3. Definiciones de Acceso a Aplicaciones

Una vez montado el esquema de Seguridad de Conectividad, las aplicaciones pueden utilizar los enlaces establecidos entre los Servidores de Aplicaciones. Los Protocolos informáticos utilizados entre Aplicaciones se encuentran fuera del ámbito de aplicación de estas normas por razones obvias de flexibilidad de implantación.

No obstante, se recomiendan las siguientes medidas de seguridad:

3.3a. Ámbito de conectividad

Cada Estado Parte deberá analizar e implantar las medidas de seguridad de los accesos a los servicios que publica, así como sus accesos a los servicios de los demás Estados Partes. Debido a que las normas orientan los procedimientos para realizar Transferencias de Datos entre Servidores de Aplicaciones, el esquema de restricciones de redes se ve facilitado, pero igualmente se deberán tomar las debidas precauciones.

Obviando los esquemas comunes de Desarrollo y Homologación de Sistemas Informáticos de Transferencia de datos, se recomienda restringir los accesos a los Servidores de Aplicaciones específicos al ámbito de Sistemas del MERCOSUR.

3.3.b. Ámbito de Restricción de Protocolos de Aplicación

Los Sistemas actuales de Transferencia de Datos permiten la identificación adecuada de Protocolos de Transferencia de Datos de Redes. No obstante, se recomienda prestar atención a la seguridad de los siguientes protocolos:

HTTP(RFC2616): Protocolo utilizado para las transacciones actuales. Se sugiere la restricción del mismo a las Transferencias de Datos específicas, desde y hacia cada Estado Parte.

HTTPS(RFC2660): Protocolo recomendado. Se sugiere la implantación de certificaciones digitales internas para Transferencia de Datos específica. De igual manera se recomienda restringir su uso al ámbito exclusivo de Servicios de Aplicaciones del MERCOSUR.

FTP(RFC0959): Protocolo para transferencia exclusiva de archivos entre Estados Partes, cuyo propósito es exclusivamente referencial y no transaccional. Se recomienda el cuidado de Amplitud de Conectividad (Ancho de Banda), cuando se utilice este protocolo, así como la aplicación de las restricciones adecuadas.

FTPS(RFC2228): Protocolo Recomendado. Permite también la implantación de certificaciones digitales. Se recomienda también el cuidado de Amplitud de Conectividad (Ancho de Banda), cuando se utilice este protocolo, así como la aplicación de las restricciones adecuadas.

Artículo 4.- Procedimiento para el ingreso de un nuevo Estado Parte al Intercambio de Información de los Registros Aduaneros (INDIRA):

En el supuesto de que se concretara el ingreso de un nuevo Estado Parte al MERCOSUR, el país adherente deberá cumplir con el siguiente procedimiento:

1. Nombrar responsables técnicos y comunicarlos al Comité Técnico N° 2 de la Comisión de Comercio del MERCOSUR para incluirlos en la correspondiente lista autorizada de responsables.
2. Preparar la infraestructura técnica para el intercambio de informaciones.
3. Actualizar la Tabla DUAM (que contiene la descripción y formato de los datos que se intercambian mediante el sistema INDIRA) con las informaciones disponibles en su país y distribuirla a los demás Estados Partes.
4. Intercambiar las siguientes informaciones con los demás países:
 - Código de País (ej: 105=Brasil)
 - Nombre del Servidor Web (ej: http://webservices.serpro.gov.br/WS_INDIRA/services/WSIndira)
 - Archivo con formato csv conteniendo la Tabla de Países, con nomenclatura y código de países XX, donde XX es la sigla del nuevo país.
 - Criterios de validación de sus declaraciones de importación y exportación.
 - Prueba de tres declaraciones de importación y tres declaraciones de exportación.
5. Desarrollar las aplicaciones y consensuar con los demás Estados Partes la fecha de prueba y puesta en producción de la nueva versión del sistema, incluyendo al nuevo Estado Parte.