USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

Programa Regional de USAID de Comercio para CAFTA-DR

Programa Regional de USAID de Comercio para CAFTA-DR

NORMATIVA PARA MANTENER PROTEGIDA LA INFORMACIÓN CONFIDENCIAL DE LOS OPERADORES DE COMERCIO EXTERIOR PARA NICARAGUA.

Contract No. AFP-I-00-04-00002-00

Task Order No. 7

Julio de 2010

Este documento ha sido elaborado por Alejandro García para Chemonics International Inc., bajo el patrocinio de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID).

CONTENIDO

1. Acrónimos **3**

2. Antecedentes **4**

3. Definiciones **6**

4. Alcance del trabajo y actividades **8**

5. Objetivo general **9**

6. Objetivos específicos **10**

7. Definición de lo que constituye información confidencial **11**

8. Base legal **12**

9. Información que es considerada como confidencial **13**

10. Mecanismos de seguridad para proteger la información confidencial **18**

11. Requisitos para solicitudes de información confidencial por parte de otros países miembros del CAFTA-DR **25**

12. Mecanismos para recibir y transmitir información confidencial **28**

13. Divulgación **30**

14. Recursos necesarios **31**

ANEXO 1 ..... **33**

1. ACRÓNIMOS

CAFTA-DR: Tratado de Libre Comercio entre Centroamérica, Estados Unidos y la República Dominicana (sigla en inglés)

CRT: USAID: Regional Trade Program for CAFTA-DR (sigla en inglés)

CAUCA: Código Aduanero Unificado Centroamericano

DGA: Dirección General de Aduanas

RD: República Dominicana

TDR: Términos de referencia

USAID: Agencia de los Estados Unidos para el Desarrollo Internacional (sigla en inglés)

RECAUCA: Reglamento del Código Aduanero Unificado Centroamericano

2. ANTECEDENTES

La República Dominicana, Centroamérica y Estados Unidos de América firmaron el CAFTA-DR el 5 de agosto del 2004. Este Tratado ha sido ratificado por las Cámaras Legislativas de Estados Unidos, Honduras, El Salvador, Guatemala, Nicaragua, República Dominicana y Costa Rica. El mismo entró en vigencia para El Salvador el 1º de marzo del 2006; para Honduras y Nicaragua, el 1º de abril del 2006; para Guatemala, el 1º de julio del 2006; y para República Dominicana, el 1º de marzo del 2007. En Costa Rica, el CAFTA-DR fue aprobado vía referéndum el 7 de Octubre del 2007 y puesto en vigencia el 1º de enero del 2009.

La oficina regional de la USAID/San Salvador firmó un contrato con Chemonics International el 1º de diciembre del 2006 para ejecutar el Programa Regional de Comercio CAFTA-DR (CRT), el cual tiene como objetivo apoyar a los gobiernos firmantes del tratado CAFTA-DR a implementar los requerimientos del mismo, particularmente aquellos relacionados con:

- **Capítulo 4:** Reglas de Origen y Procedimientos de Origen
- **Capítulo 5:** Administración Aduanera

Dentro de este marco, el Programa CRT está apoyando a las aduanas de los países miembros del CAFTA-DR en la adopción de herramientas informáticas y procedimientos mejorados que les permitan incrementar la transparencia y la eficiencia en las operaciones aduaneras.

En los ejercicios de evaluación de cumplimiento que se han realizado, se han detectado deficiencias en los niveles de cumplimiento en lo que respecta a la obligación de mantener procedimientos mediante los cuales se proteja la divulgación y el manejo de información confidencial proporcionada por algún otro país miembro del CAFTA-DR. Esto está especificado en el siguiente artículo del tratado:

"Artículo 5.6: Confidencialidad.

1. *Cuando una Parte proporcione información a otra Parte, de conformidad con este Capítulo y la designe como confidencial, la otra Parte mantendrá la confidencialidad de dicha información. La Parte que proporciona la información podrá requerir garantías por escrito de la otra Parte de que la información se mantendrá en reserva, que será*

usada sólo para los propósitos especificados en la solicitud de información de la otra Parte y que no se divulgará sin la autorización específica de la Parte que proporcionó dicha información.

2. *Una Parte podrá negarse a entregar la información solicitada por otra Parte, cuando esa Parte no ha actuado de conformidad con las garantías señaladas en el párrafo 1.*

3. *Cada Parte adoptará o mantendrá procedimientos mediante los cuales sea protegida de su divulgación no autorizada la información confidencial presentada de conformidad con la administración de la legislación aduanera de la Parte, incluida la información cuya divulgación podría perjudicar la posición competitiva de la persona que la proporciona."*

Estos términos de referencia comprenden las tareas necesarias para que los países miembros del CAFTA-DR puedan hacer un manejo eficiente y seguro de la información confidencial de los operadores de comercio que mantienen y comparten.

3. DEFINICIONES

Dirección General Aduanas:

Dirección de Aduanas, para los efectos de esta normativa, cuando se haga referencia a ésta, se deberá entender la autoridad aduanera de Nicaragua.

Firmas Digitales:

Las firmas digitales son un mecanismo que permite al receptor de un mensaje verificar la autenticidad del origen de la información, así como verificar la integridad de la información recibida. Una firma digital ofrece asimismo el esquema de "no repudio", lo que significa que una persona que ha firmado un documento no puede negar el hecho de haberlo firmado.

Funcionario Acreditado:

Será el funcionario designado por la autoridad competente de los países miembros del CAFTA-DR para solicitar y/o proporcionar información de carácter confidencial a la Dirección de Aduanas.

Funcionario Autorizado:

Será el funcionario autorizado por la Dirección de Aduanas para recibir y proporcionar información de carácter confidencial de la autoridad competente de los países miembros del CAFTA-DR.

Información clasificada:

Es toda información considerada de carácter confidencial, de uso interno o público (en medios físicos y magnéticos), que está bajo la custodia de funcionarios autorizados por la Dirección de Aduanas.

Información confidencial:

Se entenderá como información confidencial, aquella que está clasificada como información de uso de interno e información confidencial, según los criterios de la clasificación del Manual de Seguridad de la Información del Ministerio de Hacienda.

Llaves:

Una llave es un valor que trabaja con un algoritmo criptográfico para producir un texto cifrado específico; las llaves son básicamente números muy grandes, y su tamaño se mide en bits, y entre más grande es la llave, más seguro es el texto cifrado.

Operadores de Comercio:

Importadores, exportadores, productores, trasportistas, agentes aduaneros, consolidadores y desconsolidadores.

Países miembros del CAFTA-DR:

Países miembros del Tratado de Libre Comercio entre Centroamérica, Estados Unidos de Norteamérica y la República Dominicana.

Propietario de la información:

La Dirección General de Aduanas será la propietaria de la información o a quienes deleguen esta función.

Tratado:

Tratado de Libre Comercio Centro América, Estados Unidos de Norteamérica y República Dominicana (CAFTA- DR, por sus siglas en inglés).

VPN

Virtual Private Network (Red privada virtual, por su sigla en inglés).

4. ALCANCE DEL TRABAJO Y ACTIVIDADES

Para alcanzar el objetivo planteado, se trabajará de manera conjunta con el personal de la División de Fiscalización de la Dirección General de Servicios Aduaneros de Nicaragua en el desarrollo de una normativa para mantener protegida la información confidencial de los operadores de comercio, incluyendo información proporcionada por otros países miembros del tratado, cuya divulgación podría perjudicar la posición competitiva de la persona que la proporciona, así mismo que regule el intercambio de información entre los países miembros. Esta normativa establecerá básicamente lo siguiente:

a. Se redactarán los procedimientos para mantener protegida la información confidencial de los operadores de comercio, incluyendo información proporcionada por otros países miembros del tratado, cuya divulgación a terceros podría perjudicar la posición competitiva de la persona que la proporciona.

b. En la misma normativa se redactará el procedimiento de intercambio de información confidencial entre los países miembros del Tratado.

c. Definición de lo que constituye información confidencial para los efectos del Tratado.

d. Mecanismos de seguridad para proteger la información confidencial.

e. Requisitos para las solicitudes de la información confidencial por parte de los países miembros del CAFTA-DR.

f. Mecanismos para transmitir y recibir información confidencial. Esta información deberá ser eficaz y eficiente al momento de trasmitirla y recibirla.

g. Responsables del procesamiento de la información confidencial.

h. Formalidades a cumplir a través del control del procesamiento de la información confidencial que será trasmitida y recibida.

5. OBJETIVO GENERAL

El objetivo general de esta normativa es el establecer un procedimiento para el adecuado resguardo y seguridad de la información de carácter confidencial, así como el procedimiento para el intercambio de la información entre las autoridades competentes de los países miembros del CAFTA-DR

6. OBJETIVOS ESPECÍFICOS

a) **Disponibilidad:** Asegurar que los funcionarios autorizados tengan acceso a la información confidencial cuando así se requiera.

b) **Integridad:** Garantía de la exactitud y de que la información sea completa, así como los métodos de su procesamiento.

c) **Confidencialidad:** Asegurar que la información es sólo accesible para aquellos funcionarios autorizados.

d) **Autenticidad de los funcionarios autorizados y acreditados:** Asegurar la identidad de los funcionarios autorizados y acreditados que solicitan y proporcionan información clasificada como confidencial.

e) **Autenticidad del origen de los datos:** Asegurar la identidad u origen de los datos.

f) **Trazabilidad de los datos:** Asegurar que en todo momento se podrá determinar quién ha accedió y cuándo se ha accedido a los datos.

7. DEFINICIÓN DE LO QUE CONSTITUYE INFORMACIÓN CONFIDENCIAL

Los artículos 5.6.1, 5.6.2 y 5.6.3 del CAFTA-DR, disponen que es obligación de los países miembros del CAFTA-DR mantener en forma reservada la información designada como confidencial que fue proporcionada por un país miembro del CAFTA-DR.

Por otro lado, el mismo artículo 5.6.1 establece que el país solicitante deberá garantizar al país al que le requiere la información, que ésta se mantendrá en forma reservada; en caso contrario, se podrá negar a proporcionar la misma.

Aunado a lo anterior, y para los efectos del artículo 5.6 del Tratado, podríamos definir como información confidencial la que proviene de los operadores de comercio, que guarda relación con la aplicación de las reglas de origen establecidas en el capítulo cuarto del Tratado, así como con las resoluciones anticipadas establecidas en el artículo 5.10 del Tratado, o con una actividad ilegal relacionada con la legislación o regulaciones que rijan las importaciones de un país miembro del CAFTA-DR, y la cual no se compartirá ni revelará con y a terceros, excepto que se tenga expresa autorización del país miembro del CAFTA-DR que la proporcionó, o cuando ha sido requerido por orden judicial.

8. BASE LEGAL

Como base legal para la aplicación de la presente normativa, se ha tomado en cuenta la legislación nacional e internacional referente al CAFTA-DR, y que implica la implantación de forma explícita de medidas de seguridad para conservar y proporcionar la información de carácter reservado.

a. Tratado de Libre Comercio entre Centro América, Estados Unidos y República Dominicana (por sus siglas en ingles, CAFTA-DR), en sus Artículos 3.24, 4.20, 5.5.3, 5.5.4, literales a, b, c, y d, 5.5.6, 5.5.7 y 5.10.

b. CAUCA, en sus Artículos 16, 30,31 y 35.

c. RECAUCA, en sus Artículos 26 literal (c), 167 y 309.

d. Código Penal de la República de Nicaragua, artículo 275 y 276.

e. Ley Creadora de la Dirección General de Servicios Aduaneros y Reforma a la Ley Creadora General de Ingresos, Ley No. 339, aprobada el 9 de marzo de 2000 y publicada en la Gaceta No. 69 del 6 de abril de 2000.

9. INFORMACIÓN QUE ES CONSIDERADA COMO CONFIDENCIAL

En vista del riesgo que puede constituir para la DGA cuando la información confidencial que es obtenida a través de terceros, y conforme a lo dispuesto en los Artículos 3.24, 4.20, 5.5.3, 5.5.4, literales (a), (b), (c), y (d), 5.5.6, 5.5.7 y 5.10 del Tratado, se considerará como información de carácter confidencial lo siguiente:

9.1. Información relacionada con resoluciones anticipadas, articulo 5.10 del Tratado, procedimiento.

9.1.1. Valoración

a) Valor en aduana de determinadas mercancías que serán importadas por un operador aduanero.

b) Nombre y domicilio de los vendedores.

c) Nombre y domicilio de los proveedores de insumos.

d) Nombre o razón social y domicilio del representante del vendedor o vendedores que negocian sus mercancías en El Salvador.

e) Nombre y domicilio de las empresas vinculadas.

f) Datos de contrato internacional de compra-venta, representación, distribución o exclusividad, suscrito entre la(s) empresa(s) salvadoreña(s) y su vendedora.

g) Formas de pago de la mercancía o de los aspectos relacionados con la negociación, tales como:

1. Cotización del pedido de las mercancías.
2. Confirmación de precios emitidos por el proveedor.
3. Contrato de compra-venta.
4. Factura comercial proforma.
5. Lista de precios de exportación.
6. Copia de las transferencias monetarias, cartas de crédito o la forma de pago utilizadas para la adquisición de las mercancías.
7. Declaración de importación o documento equivalente.

9.1.2. Reglas de origen

a) El nombre completo, denominación o razón social y domicilio del importador, exportador y productor de la mercancía objeto de la solicitud.

b) Nombre y domicilio de los proveedores de los materiales.

c) La información necesaria para calcular el valor ajustado respecto a la transacción del productor de la mercancía, ajustado sobre la base FOB o CIF.

d) La información necesaria para calcular el valor de cada uno de los materiales no originarios y materiales de origen desconocido utilizados en la producción de la mercancía, sobre la base CIF o FOB.

e) La descripción de todos los materiales originarios utilizados en la producción de la mercancía.

f) La descripción y valor de los accesorios, repuestos y herramientas, si éstos vienen acompañando a las mercancías.

g) Descripción de los contendores y materiales de embalaje con las que las mercancías serán embarcadas.

h) Información sobre el control de inventarios que el solicitante de la resolución anticipada tiene implementada (PEPS, UEPS o Promedios).

i) Si la resolución anticipada implica el uso del método del costo neto de la industria automotriz, se deberá conservar como reservada la siguiente información:

1. La relación de todos los costos del producto, el período y otros datos relevantes para la determinación del costo total de la mercancía.
2. La relación de todos los costos excluidos, que deberán disminuirse del costo de la mercancía, para determinar el costo neto de la misma.
3. La información necesaria para calcular el valor de cada uno de los materiales no originarios y materiales de origen desconocido utilizados en la producción de la mercancía.
4. La base de asignación de costos y gastos.
5. El periodo en el cual deberá efectuarse el cálculo del costo neto.

9.1.3. Mercancía reimportada después de su reparación o alteración

a) Especificaciones técnicas o comerciales de la mercancía.

b) Descripción del proceso de reparación o alteración.

c) Datos de las partes, repuestos, o bienes destinados al mantenimiento o reparación de las mercancías.

d) Si el proceso de reparación o alteración destruye las características esenciales de la mercancía o crea una nueva o comercialmente diferente

e) Si el proceso de reparación o alteración transforma la mercancía no terminada en una mercancía terminada.

9.1.4. Cupos de mercancías asignados en base a Certificados Comerciales (CFF)

a) Clasificación arancelaria de las mercancías.

b) Descripción de las mercancías.

c) Cantidad aproximada que se pretende importar.

d) Lugar de nacimiento y crianza del pollo del cual derivan los muslos y piernas.

e) Lugar en donde se procesan las mercancías.

f) Si va ser objeto de trasbordo, señalar el nombre del tercer país.

g) Si va ser facturada por tercer país, señalar el nombre de éste.

9.2. Información relacionada con los Procedimientos de Verificación de Origen, artículo 4.20 del Tratado, procedimiento PRT-007, "Realización de Investigaciones Preliminares de Origen u otras Peticiones"

a) Contenido de certificados de origen.

b) Contenido de respuestas a cuestionarios.

c) Proceso de producción de la mercancía.

d) La información técnica de las mercancías objeto de una visita de verificación.

e) La descripción completa de los materiales no originarios, utilizando información como facturas, manual del usuario, catálogos, croquis, bosquejos, documentos de ingeniería, contratos, examen físico que permita clasificar los materiales a nivel de subpartida arancelaria (seis dígitos) o a nivel de fracción arancelaria (ocho dígitos).

f) El precio realmente pagado o por pagar consignado en los documentos aduaneros que sustenten las facturas comerciales, las órdenes de compra, los cheques, etc.

g) La lista de materiales utilizados en la producción de las mercancías que fueron objeto de verificación de origen.

h) Las listas de los proveedores de los materiales empleados en la fabricación de las mercancías.

i) Las facturas de compra, las guía de embarque, los cheques bancarios y cualquier nota de crédito de las mercancías objeto de verificación.

j) Las marcas de los materiales utilizados en la producción de las mercancías.

9.3. Información relacionada con los Procedimientos de Verificación de Origen Textil y del Vestido, según el artículo 3.24 del Tratado.

9.3.1. El contenido de la respuesta de algún requerimiento de información a un importador relacionado con:

a) Lista de materiales usados en la producción del textil o del vestido sujeta a verificación.

b) Clasificación arancelaria de materiales.

c) Nombre y dirección de los proveedores de materiales.

d) Descripción narrativa del proceso de producción.

e) Lugar donde se llevan a cabo todas las operaciones.

9.3.2. La notificación realizada a un productor sobre la intención de practicar una verificación de origen.

9.3.3. La solicitud de cooperación de la autoridad aduanera o competente del país de exportación para practicar la visita de verificación.

9.3.4. La información contenida en el acta de visita de verificación, consistente en:

a) La fecha en que fue establecida la empresa visitada.

b) Si se trata de una persona jurídica, los nombres de las personas que forman parte del consejo de administración.

c) Los datos de las sucursales de la empresa visitada, tales como su ubicación y su razón social.

d) El tipo de bienes que la empresa produce.

e) Qué cantidad y qué tipo de maquinaria tiene la empresa.

f) Si la empresa subcontrata parte de su producción a un tercero.

g) Si la empresa se acoge a los regímenes de perfeccionamiento activo.

h) La capacidad mensual de producción de la empresa.

i) La cantidad empleados que están involucrados en la producción de la mercancía (KTS, corte, costura, control de calidad, acabado, embalaje, etc.).

j) Los registros de insumos.

k) Precios de los insumos utilizados en la producción de la mercancía.

l) Registros de producción de las prendas de vestir acabadas.

m) Lista de proveedores.

n) Tarjetas de registro de los empleados y nómina.

9.4. Información referente a una actividad ilegal relacionada con la legislación o regulaciones que rijan las importaciones o exportaciones de Nicaragua.

a) Evidencia histórica de incumplimiento de las leyes o regulaciones que rigen las importaciones por parte de algún fabricante, productor u otra persona involucrada en el movimiento de mercancías del territorio aduanero nicaragüense al territorio aduanero de otro país miembro del CAFTA-DR.

b) Evidencia histórica de que alguna o todas las personas involucradas en el movimiento de mercancías desde el territorio aduanero nicaragüense hasta el territorio de otro país miembro del CAFTA-DR, para un sector de productos específicos, no ha cumplido con las leyes o regulaciones establecidas en Nicaragua, que rigen las importaciones.

10. MECANISMOS DE SEGURIDAD PARA PROTEGER LA INFORMACIÓN CONFIDENCIAL

Este capítulo describe los principales mecanismos de seguridad de la Información "clasificada", tales como: la guarda y custodia de la misma, las responsabilidades de los funcionarios de Dirección General de Servicios Aduaneros, los diversos algoritmos para el cifrado de datos, protocolos para la protección de mensajes, el intercambio de llaves, así como los mecanismos que garanticen la autenticidad, integridad y confidencialidad de la información en un sistema involucrado con el intercambio de información entre los miembros del CAFTA-DR.

10.1. Áreas responsables de conservar la información confidencial

De conformidad con la Ley 239, Ley creadora de la Dirección General de Servicios Aduaneros y su Reglamento, decreto 20-2003, las áreas competentes para conservar la información confidencial serán las siguientes:

a) Departamento de Verificación de Origen

Área responsable de conservar la información relacionada con los procedimientos de verificación de origen de las mercancías.

b) Dirección Técnica Aduanera

Área responsable de conservar la información relacionada con el contenido de las resoluciones anticipadas.

c) División de Fiscalización

Área responsable de conservar la información referente a las sanciones de tipo administrativo y tributario impuestas a los operadores de comercio exterior.

d) División de Asuntos Jurídicos

Área responsable de conservar la información referente a las sanciones de tipo penal impuestas a los operadores de comercio exterior.

e) División de Tecnología

Área responsable de conservar la información relativa a las operaciones de comercio exterior en las diferentes bases de datos que conforma el sistema Aduanero.

10.2. Responsabilidad de las diferentes direcciones y departamentos referente a la seguridad de la información y de la documentación.

Principales responsabilidades para mantener y conservar la información de carácter confidencial:

a) Cumplir y hacer cumplir a los funcionarios a su cargo las disposiciones sobre seguridad de la información confidencial contenidas en esta normativa y otras disposiciones.

b) Los funcionarios que incumplan las disposiciones establecidas sobre la seguridad de la información estarán sujetos a acciones disciplinarias establecidas en las disposiciones legales y técnicas vigentes.

c) Asegurar que los funcionarios a su cargo reciban el correspondiente entrenamiento sobre medidas de seguridad relacionadas con la información y documentación de carácter confidencial.

d) Analizar y evaluar con el personal a su cargo las medidas de seguridad establecidas para proteger la información y documentación de carácter confidencial.

e) Dar a conocer al área competente de la Dirección de Aduanad hechos que puedan constituir delitos o infracciones relacionados con la revelación no autorizada de la información confidencial.

10.3. Responsabilidad de los funcionarios que dependen de las diferentes direcciones y departamentos sobre la seguridad de la información y documentación.

a) Los auditores, administradores de aduana, aforadores y demás funcionarios que dependen de las direcciones, delegaciones y administraciones de aduanas serán responsables de proteger la información y documentación que tengan a su cargo.

b) A los funcionarios que dependen de las distintas direcciones, delegaciones y administraciones de aduanas que tengan acceso a la información

clasificada como confidencial, les es prohibido suministrarla sin la autorización correspondiente.

c) Los funcionarios que incumplan con las disposiciones establecidas sobre la seguridad de la información estarán sujetos a las acciones disciplinarias establecidas en la legislación nacional.

d) Los expedientes que contengan información confidencial descritas en el numeral 6º de la presente normativa, tienen que estar debidamente resguardados independientemente que no estén en uso o posesión de los funcionarios que dependan de las diferentes direcciones, delegaciones y administraciones de aduanas.

10.4. Control de ingreso y egreso de personas a las jefaturas y al Archivo General

10.4.1. De conformidad con el lineamento 9.4. de Seguridad Física y Ambiental del Manual de Seguridad de la Información del Ministerio de Hacienda, se deberán tomar las siguientes medidas:

a) Establecer un perímetro de seguridad (puertas de entrada, paredes, etc.) para proteger las áreas que contengan información y sus recursos de tratamiento.

b) Controles de acceso a toda oficina, centro de procesamiento de datos y áreas de trabajo que contengan información confidencial o sensible. Todos estos sitios deben estar físicamente restringidos para limitar el acceso a aquellos que quieran acceder a la información.

c) Establecer los controles, procedimientos y protección física adecuados cuando empleados o terceros efectúen trabajos en áreas que contengan información confidencial o sensible.

10.4.2. No estará permitido el ingreso a las jefaturas a los funcionarios anteriormente mencionados que no dependan de las mismas: el acceso no autorizado deberá ser previa autorización de las jefaturas de las áreas correspondientes.

10.4.3. Los funcionarios que pertenezcan a las áreas técnicas donde se maneja y resguarda la información confidencial no permitirán el acceso a funcionarios y técnicos que no cuenten con la autorización de las jefaturas.

10.5. Medidas de seguridad para conservar y resguardar la información clasificada como confidencial o de uso interno en forma impresa

De conformidad con el procedimiento de seguridad normativo de la Clasificación y Marcado de la Información, PRSN-010 del Ministerio de Hacienda, se deberán tomar las siguientes medidas:

a) Los documentos físicos deberán estar ordenados en expedientes, los cuales deberán de llevar impresa en su carátula la siguiente leyenda: **"INFORMACIÓN CONFIDENCIAL".**

b) Aquellos funcionarios a quienes les hayan sido asignado expedientes firmarán en forma física o electrónica un acuse de recibo asumiendo el compromiso de custodiarlos y de guardar la debida discreción sobre el contenido de los mismos.

c) Los expedientes deberán archivarse en gavetas, las cuales deberán estar en todo momento aseguradas bajo llave.

d) La consulta de los expedientes se realizará bajo los siguientes lineamientos:

1. En el caso de funcionarios de la Dirección de Aduanas adscritos a otras jefaturas, podrán solicitar los expedientes para su consulta previa autorización del Director, Subdirector General de Aduanas, jefe del área responsable u otro funcionario autorizado expresamente.
2. En el caso de personas jurídicas o individuales, los expedientes podrán ser consultados por ellos o por sus representantes, debiendo tener acreditada su personalidad en los autos de determinado procedimiento.
3. Queda estrictamente prohibido proporcionar información a personas que no tengan legitimación dentro de los procedimientos seguidos ante la Dirección General y a los funcionarios que no tengan a su cargo dichos expedientes; en caso contrario, se harán las sanciones correspondientes.

10.6. Medidas de seguridad para conservar información almacenada en la base de datos

El principal riesgo que presenta la información almacenada en las bases de datos es que esta sea interceptada por terceros con avanzados conocimientos informáticos, y que podrían intervenir directamente en las correspondientes bases de datos

Consecuentemente, la información confidencial almacenada en bases de datos o documentos digitalizados requiere de un mecanismo de alta seguridad tecnológica que garantice que esté disponible sólo para los funcionarios autorizados por la Dirección de Aduanas.

Aunado a lo anterior, la Dirección de Aduanas ha estado utilizando la tecnología VPN para intercambiar información con los países de la región, lo cual ha traído óptimos resultados, dado que la seguridad de la misma queda garantizada con el uso de estos dispositivos. Cabe mencionar que, dependiendo el tipo de acuerdo o convenio de intercambio de información, se utiliza un procedimiento en particular.

La principal ventaja que ofrece el uso de esta tecnología es la confiablidad en los datos, a través de obtención de la encriptación. En este proceso se codifican los datos de tal manera que sólo la computadora de destino puede descifrar la información.

El protocolo de encriptación que se recomienda es el "IPsec-Internet Protocol Security", el cual proporciona una seguridad mejorada con características tales como algoritmos de encriptación más fuertes y autenticación más comprensiva. Este protocolo tiene dos modos de encriptación: túnel y de transporte. En el caso del modo de túnel, se encripta el encabezado y la carga de cada paquete, mientras que el método de transporte solo encripta la carga o contenido de los paquetes.

10.6.1. Mecanismos de uso de credenciales

Los esquemas de seguridad del sistema deben incluir un mecanismo usual de credenciales de usuario (nombre de usuario y contraseña) para el acceso, y un extenso conjunto de roles y atributos sobre la información para cada usuario.

Para mayor seguridad de la información, se recomienda un mecanismo de doble autentificación (nombre de usuario y contraseña) para el acceso a la base de datos, el cual permita mantener un estricto control.

El esquema de doble autentificación está formado por dos pares de credenciales de usuario que consisten en:

1. *Credenciales de acceso al sistema:* El nombre de usuario y contraseña que cada usuario utiliza para autentificarse en el sistema. Las mismas son conocidas por cada usuario y por el administrador.

2. *Credenciales de conexión a la base de datos:* El nombre de usuario y la contraseña para el acceso ("login") correspondiente a la base de datos. Estas credenciales deben ser conocidas sólo por el administrador de la base de datos.

    a) Las credenciales son almacenadas de forma encriptada en la base de datos, usando algoritmos para el cifrado de la información. La información de las credenciales de usuario siempre se cifra, nunca se manipula la misma de forma textual (sin encriptar), por lo cual, la única forma de acceder a las credenciales de un usuario es poseer el algoritmo y las llaves privadas de cifrado que se encuentran seguras, almacenadas de forma compleja en el código compilado de los módulos del sistema.

    b) El uso de credenciales de conexión a la base de datos para cada usuario por separado permite, además, definir un mecanismo de roles y permisos de acceso a la información confidencial almacenada en la base de datos.

10.7. Responsabilidad de los funcionarios de la Dirección de Aduanas en el uso de contraseñas

1. La entrega de las credenciales al usuario (nombre de usuario y contraseña) debe realizarse mediante un procedimiento que obligue al usuario a

cambiar la contraseña en el inicio de sesión, lo que garantiza que solamente él conoce la contraseña.

2. Se debe informar a los funcionarios autorizados acerca de la selección y empleo de sus contraseñas, para garantizar que las mismas tienen una calidad mínima frente a intentos de acceso.
3. Se debe concienciar a los funcionarios autorizados de la confidencialidad de la contraseña, y de que la revelación de la misma supone una suplantación de su identidad digital, que puede tener repercusiones (administrativas) disciplinarias y penales.

10.8. Las medidas sobre la responsabilidad de los funcionarios autorizados en el uso de sus contraseñas, se regulará como a continuación se indica:

1. Se debe requerir a los funcionarios autorizados buenas prácticas de seguridad en la selección y empleo de sus contraseñas.
2. Para el mecanismo de autenticación de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y, mientras estén vigentes, se almacenarán de forma ininteligible.
4. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
5. La asignación de contraseñas debería ser controlada por un proceso de dirección formal.
6. Los sistemas de contraseñas deberán asegurar la calidad de las mismas.

11. REQUISITOS PARA SOLICITUDES DE INFORMACIÓN CONFIDENCIAL POR PARTE DE OTROS PAÍSES MIEMBROS DEL CAFTA-DR

11.1. Registro de los funcionarios autorizados por los Países miembros del CAFTA-DR para manejar la información confidencial

En el ámbito de cooperación entre los miembros del CAFTA-DR, los titulares de las autoridades competentes de los países adscritos al tratado deberán acreditar por escrito ante el Director General de Servicios Aduaneros de Nicaragua a los funcionarios autorizados para solicitar y recibir la información de carácter confidencial, para lo cual deberán de proporcionar los siguientes datos:

1. Autoridad competente solicitante.
2. Nombre del funcionario que se solicita su acreditación.
3. Cargo que ostenta.
4. Documento de identidad del funcionario del país solicitante.
5. Área de la Autoridad Competente a la que pertenece el funcionario.
6. Dirección de correo electrónico.

i. Una vez que se haya recibido la solicitud de acreditación, el Director General de Servicios Aduaneros emitirá una notificación, ya sea por escrito o por vía electrónica, en el que se tenga por acreditado al funcionario del país miembro del CAFTA-DR para solicitar y recibir la información de carácter confidencial.

ii. El funcionario acreditado deberá llenar y firmar el formulario, adjunto a la notificación emitida por el Director General de Servicios Aduaneros.

iii. La Dirección General de Servicios Aduaneros otorgará los accesos correspondientes al funcionario o funcionarios, notificándoles su usuario y contraseña, la cual deberá cambiarse de manera obligatoria la primera vez.

iv. Sera responsabilidad del Director General de Servicios Aduaneros comunicar oportunamente cuando se revoque la autorización del funcionario acreditado e informar de inmediato a la División de Informática para deshabilitar los accesos correspondientes.

11.2 Solicitudes de información

Los funcionarios acreditados ante la Dirección General de Servicios Aduanas de Nicaragua deberán contar con un usuario y un password para poder tener acceso al sistema informático.

La solicitud de información deberá ser enviada en el formato previamente establecido por la Dirección General de Servicios Aduaneros la cual contendrá los siguientes datos:

11.2.1. Contenido de la solicitud

1. Nombre del funcionario acreditado por la Dirección General de Servicios Aduaneros para suministrar la información de carácter confidencial.
2. Cargo que ostenta ante la autoridad aduanera que solicita la información confidencial.
3. Número de teléfono del funcionario solicitante.
4. Correo electrónico.
5. Número de notificación en que la Dirección General de Servicios Aduanero, acreditó al funcionario para solicitar y recibir información de carácter confidencial.
6. Fecha en que fue acreditado por la Dirección General de Servicios Aduaneros.
7. Señalar en el recuadro correspondiente el tema sobre el que se solicita información:

    a) Verificación de Origen, Artículo 4.20 del Tratado.
    b) Verificación de Origen Textil y Vestido, Artículo 3.24 del Tratado.
    c) Resoluciones anticipadas, Artículo 5.10

d) Sospecha razonable de una actividad relacionada con la legislación o regulaciones que rijan las exportaciones o importaciones efectuadas en la República de Nicaragua.

8. Señalar los propósitos para los que será usada la información confidencial solicitada.

9. Si se cuenta con la información, se deberá de precisar el número de expediente, nombre del importador, exportador, su registro tributario, fecha de emisión del acto administrativo, el o los documentos que se solicitan.

10. Descripción de la mercancía y su código arancelario.

11. Fecha de la solicitud.

12. MECANISMOS PARA RECIBIR Y TRANSMITIR INFORMACIÓN CONFIDENCIAL

12.1 Recepción de las solicitudes de información

Debido a que en el Internet la información viaja a través de un medio completamente inseguro, es necesario establecer protocolos de comunicación que hagan dicho proceso de intercambio de información completamente seguro. Esto se logra cifrando la información durante el tiempo que viaja de un extremo a otro del proceso de comunicación. Para el caso de la Dirección General de Servicios Aduaneros, se realizará de la siguiente manera:

1. El formato de la solicitud de información confidencial del país miembro del CAFTA-DR se realizará a través a través de la VPN previamente autorizada y configurada por los especialistas de cada institución.

2. Una vez recibida la notificación a través de un correo autorizado por la Dirección General de Servicios Aduaneros, se gestionará con las áreas involucradas para proporcionar la información requerida, en conformidad a los procedimientos de seguridad establecidos por la Dirección General de Servicios Aduaneros.

3. Las áreas involucradas en proporcionar la información realizarán el proceso de recopilación de la misma, debiendo enviar ésta a través de notas, reportes, informes, u otros (esta información deberá de estar debidamente firmada por el Director General o la persona que él mismo autorice) a la persona autorizada por la Dirección General de Servicios Aduaneros. El término para la entrega de la documentación requerida será no mayor a los diez días, pudiendo solicitarse al Director General de Servicios Aduaneros prórrogas debidamente justificadas.

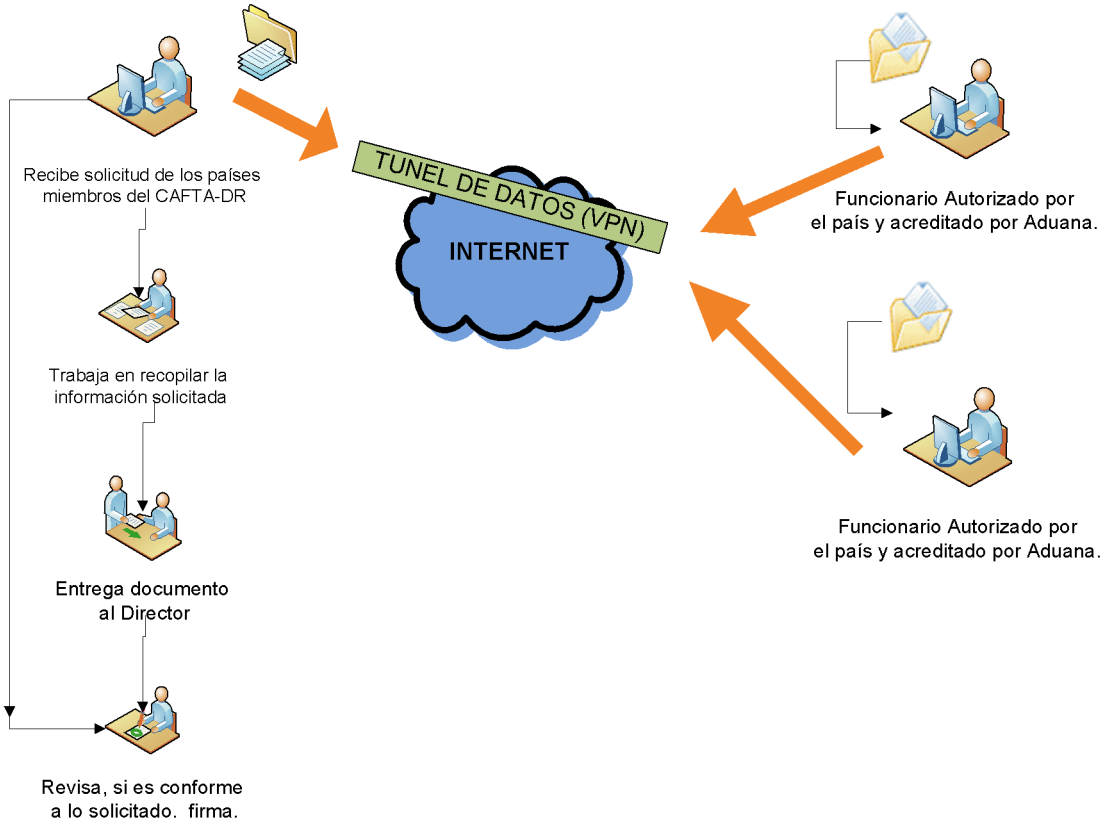
4. El funcionario autorizado por la Dirección General de Servicios Aduaneros realizará el proceso de digitalización de los documentos; una vez finalizado dicho proceso, lo publicará en la página web diseñada para estos casos.

5. El funcionario acreditado recibirá automáticamente una notificación a través de un correo automático generado por la página web, de que la información ya se encuentra disponible para ser extraída y consultada.

6. De igual forma, el acreditado deberá revisar la bandeja de entrada, donde está el requerimiento solicitado y deberá contestar dentro de la misma página web.

7. Si se requieren de copias de documentos físicos, éstos se enviarán en sobre a través de empresas Courier con acuse de recibo.

PROCESO DE SOLICITUD Y RECEPCION DEL INTERCAMBIO DE INFORMACION CONFIDENCIAL ENTRE LOS PAISES MIEMBROS DEL CAFTA-DR



13. DIVULGACIÓN

La Dirección General de Aduanas dará a conocer, a través de nota a las autoridades competentes de los países miembros del CAFTA-DR, los presentes lineamientos, para que, en los términos del artículo 5.6, se garantice la confidencialidad de la seguridad de la información que se les proporcione por parte de la Dirección de Aduanas.

14. RECURSOS NECESARIOS

Se recomienda como herramienta tecnológica para este procedimiento la plataforma SharePoint.

ANEXO 1

DIRECCIÓN GENERAL SERVICIOS ADUANEROS

Gobierno de Reconciliación y Unidad Nacional
El Pueblo, Presidente!

2010: AÑO DE LA SOLIDARIDAD
Viva Nicaragua Libre!

Solicitud de Información Confidencial

Datos del funcionario acreditado

1. Nombre del funcionario acreditado por la Dirección General de Servicios Aduaneros para recibir información de carácter confidencial._____.

2. Cargo: _____.

3. Teléfono: _____. 4.- Correo Electrónico: _____.

5. Número de notificación de la Dirección General de Servicios Aduaneros: _____.	6. Fecha de acreditación:____/____/_____

7. Señalar en el recuadro correspondiente el tema a que se refiere la solicitud de información:

- ▼ Verificación de Origen, artículo 4.20 del Tratado
- ▼ Verificación de Origen Textil y Vestido, artículo 3.24 del Tratado.
- ▼ Resoluciones anticipadas, artículo 5.10
- ▼ Sospecha razonable de una actividad relacionada con la legislación o regulaciones que rijan las exportaciones o importaciones efectuadas en la República de Nicaragua

8. Propósito específico para los cuales se solicita la información:
9. Precisar la documentación que se solicita cuando se tengan los datos
10. Descripción de la mercancía y código arancelario
11. Fecha de solicitud ____/____/_____
12. Adquiero el compromiso establecido en la Notificación de Acreditación, de no divulgar la información a terceros que no estén debidamente autorizados. _____ Nombre y firma del funcionario acreditado por la Dirección General de Servicios Aduaneros