UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

SEGURIDAD EN LAS TRANSACCIONES EN LÍNEA DE COMERCIO ELECTRÓNICO

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

MAESTRO VIRGILIO ERNESTO REYES VÁSQUEZ

PRESENTADO POR:

RENÉ ALEXIS VILLATORO ALAS

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Febrero de 2015

LISTA DE GRAFICOS

INDICE

RESUMEN

El comercio electrónico es un modelo basado en Internet, pues a lo largo del tiempo se ha ido transformando en la principal fuente de comercialización en la red. Así mismo, es un medio de negociación entre las empresas y los usuarios, por consiguiente podemos lograr la igualdad de oportunidades dentro del mercado, en cuanto a brindar sus productos y servicios de manera más cómoda, de fácil acceso; pero también ayudándonos a reducir el factor tiempo y el empleo de muchos recursos. Este beneficio no solo se presta en una sino en varias organizaciones. No obstante, es importante pretender identificar, cuál es el inconveniente más grande que ocurre al momento de verificar, si el uso de este tipo de comercio se vuelve totalmente inseguro o con poca confiabilidad en su manejo. Esto lo analizamos al constatar, la vulnerabilidad que sufre el área empresarial cuando en su sistema de seguridad se compromete información confidencial almacenada en sus servidores tales como: números de tarjeta de crédito, número de cuenta bancaria, datos personales, etc. Cabe mencionar, que para resolver esta problemática tan eminente, es necesario tratar con los protocolos de seguridad porque con ellos resguardamos perfectamente la información de los usuarios, a través de: Cifrado de datos, métodos de autenticación, firewalls entre otros.

PALABRAS CLAVE: comercio electrónico, cifrado de datos, firewalls, métodos de autenticación, protocolos de seguridad.

ABSTRACT

E-commerce is a model based on Internet, because over time is has been transformed into the main source of marketing on the net. Is also a means of negotiation between companies and users, therefore we can achieve equality of opportunity in the market, in terms of providing its products and services more comfortably, for easy access but also helping to reduce the time factor and the use of many resources. This benefit is paid not only once but several organizations. However, it is important to seek to identify, what is the largest problem that occurs at the time of check, if the use of this type of trade becomes totally unsafe or unreliability in its management. This analyzed it to confirm, the vulnerability affecting the business area when in your security system undertakes confidential information stored on their servers such as: numbers of credit card, bank account, personal data, etc. It is noteworthy, that to solve this problem so eminent, is necessary to deal with the security protocols because with them safeguard perfectly users, through information: encrypted data, authentication methods, including firewalls.

KEYWORDS: e-commerce, firewalls, encryption data, firewalls, authentication methods, security protocols.

INTRODUCCION

El presente trabajo de investigación se denomina “SEGURIDAD EN LAS TRANSACCIONES EN LINEA DE COMERCIO ELECTRÓNICO, por esta razón, primero nos vamos a referir a los principios básicos de la implementación de seguridad; en sistemas informáticos, para todos aquellos administradores de servidores, redes y oficiales. Esto con el fin de detectar, donde se encuentran las deficiencias y poder así ejecutarlos de la mejor manera posible.

A continuación, mencionaremos los diferentes tipos de usuarios, para dar un mayor enfoque a la realización de los principios, estos se ejemplifican así: Están los que realizan transacciones en línea, sin fijarse en la protección que muestra el sitio web, también existen otros que no se percatan, si su información personal ha sido clonada y por último los que desconocen si dentro de la red han sido interceptados por un hacker.

En segundo lugar, hoy en día se tiene que estar claro, acerca de las *medidas de seguridad*; porque permite determinar si dentro de este proceso se cuenta con sitios auténticos o no, a fin de preservar los datos sensibles, ya que de no revisarse, la delincuencia cibernética podría llegar aprovecharse de la falta de conocimientos de los usuarios al momento de efectuar la transacción.

En tercer lugar, señalaremos los mecanismos criptográficos en los *sistemas de seguridad* tales como: Los datos cifrados, firmas y certificados digitales. Estos nos facilitan una guía en a cuanto su aplicación certera. Finalmente, analizaremos la consistencia que existe en la negociación vía Internet de todas las entidades involucradas.

Sin esta indagación no podremos detallar la importancia de la confiabilidad que debe existir en el comercio electrónico debido a que la mayoría de personas optan por esta utilización y no por la modalidad tradicional.

¿QUÉ ES LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO?

Es cuando se efectúan transacciones en línea de forma confiable sin que esta sea interceptada por *cibercriminales*. Muchas veces estos intercambios resultan inestables porque se exponen datos personales o cualquier otro tipo de información privada y los clientes se confían suponiendo que solamente en el modelo tradicional se cometen faltas o transgresiones en el proceso de comercialización.

Es así como se complica el desarrollo de la mayoría de empresas y consumidores que ocupan esta modalidad de negociación. Por este motivo, las organizaciones deben adquirir nuevas tecnologías que estén a la vanguardia con el tema de la protección para salvaguardar toda la comunicación digital en su red y poder así evitar riesgos, de lo contrario; existirá el grave peligro que ocurran una cantidad de suplantaciones de identidad y estos sean usados en cuanto a la proliferación de crímenes en Internet, que son perpetrados a través de infraestructuras de redes inseguras.

1. ELEMENTOS DE SEGURIDAD DE LA INFORMACIÓN DE COMERCIO ELECTRÓNICO

La seguridad de la información se ha mantenido sobre los siguientes pilares, ayudando a la construcción de un robusto control de seguridad:

1.1 INTEGRIDAD

Se refiere a que se debe asegurar que los datos no se falsifican o alteran por usuarios no autorizados. Es un hecho que el comercio electrónico simplifica el trato, haciéndolo cada vez más eficaz pero es necesario precisar sobre el primer elemento, pues sin este, no podría existir rectitud en el manejo y se daría lugar a que hayan muestras de falsificaciones inesperadas cuando la información que ha sido ingresada por el cliente en el sitio web, transmite alteraciones o atracos por terceros, lo que provoca un bajo nivel de satisfacción en la ocupación de este modelo que no es el tradicional.

1.2 NO REPUDIO

Se da cuando garantizamos que los beneficiarios del comercio electrónico no puedan negar el intercambio ya finalizado, una vez hayan ejercido cualquier proceso en línea.

1.3 AUTENTICIDAD

Se refiere a la secuencia de pasos que tomamos en cuenta, para llegar a la total verificación de la real identidad de una persona o entidad, basándonos en que los datos que se han recibido del solicitante, correspondan al cliente u empresa sin que se encuentren intermediarios que se hagan pasar por ellos*, (Suplantación de identidad).*

1.4 CONFIDENCIALIDAD

Es aquella donde aseguramos, la fiabilidad del empleo de la información que viaja en la red, ya sea la del usuario que ha solicitado el encargo o la de la empresa que recibe la solicitud del cliente que se ha beneficiado de sus servicios.

1.5 DISPONIBILIDAD

Se refiere a la capacidad que un sitio de comercio electrónico tiene para ser flexible las 24 horas del día, omitiendo interrupciones y en función apropiada; sin importar el momento que se requiera la solicitud, con el fin de alcanzar la satisfacción de necesidades [1].

2. PRINCIPALES PROBLEMAS DE SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Los principales problemas de seguridad que enfrenta el comercio electrónico se basan en tres áreas, la cuales son: Ataques de Hackers, denegación de servicios, virus informáticos y su propagación. Al enfocarnos en estas dificultades podemos prevenir riegos severos y es así como los analizaremos detalladamente.

2.1 ATAQUES DE HACKERS

Son todas aquellas embestidas que actúan por medio de computadoras ya que son aprovechadas para transgredir a sus primordiales activos, esto lo construyen las personas que acceden a los sistemas sin previa autorización del cliente, haciendo una manipulación ilegal de los recursos de la red. Por ejemplo: estos individuos entran a los servicios de rutina o de monitoreo de tráfico de red con la intención de obtener el host de destino de su víctima, en la cual incluyen el tipo de versión del sistema operativo, escaneo de puertos abiertos en la PC, dirección de MAC, dirección de IP hasta monitorear el tráfico que pasa por la red, eludiendo el firewall [2].

2.2 DENEGACIÓN DE SERVICIO

Es aquel ataque, el cual, genera un gran número de peticiones de servicio o acceso a un sitio web, bombardeando el sistema hasta llegar al punto de colapsar y no responder adecuadamente en el tiempo requerido [4].

2.3 VIRUS INFORMÁTICOS Y SU PROPAGACIÓN

Un *virus* es un conjunto de códigos programables que son insertados en un programa para poder ingresar a un host de forma indebida, por lo que se distribuye en el ordenador con la finalidad de destruir, robar o compartir datos de forma ilegal. Estos son tan eficientes, que pueden auto-programarse y replicarse a sí mismo en una red u ordenador.

El virus se puede difundir mediante el siguiente mecanismo: Cuando es creado por el programador, utilizando un lenguaje ensamblador, luego el usuario abre el programa contaminado y este es insertado en el ordenador, finalmente este se infecta, deshabilitando los dispositivos físicos y robando la información [3]. **Véase figura 2.3.**

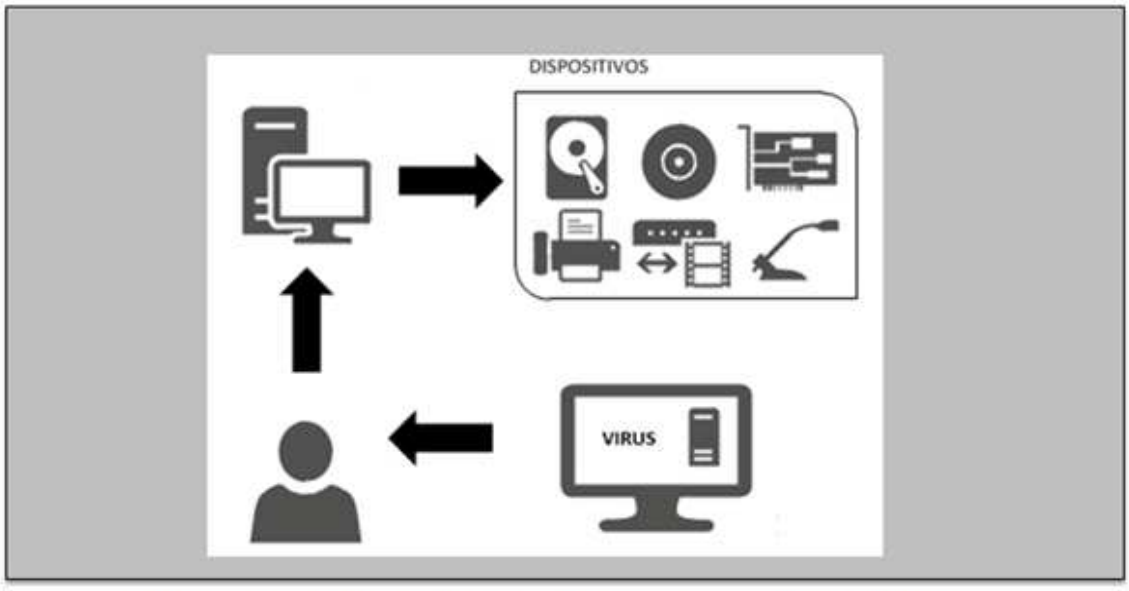


Figura 2.3 *Proceso de inserción de virus en un computador.*
Fuente: Elaboración Propia.

3. NORMAS DE SEGURIDAD DE DATOS DE LA PCI DSS EN TARJETAS DE CRÉDITO

Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. Las PCI DSS

proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales). "A continuación, encontrará una descripción general de los 12 requisitos de las DSS de la PCI." [12]

Norma de seguridad de datos de la PCI: Descripción general de alto nivel.

3.1 CONSTRUIR Y MANTENER UNA RED SEGURA

- Instalar y mantener una correcta configuración del Firewall
- No utilizar los valores predeterminados para las contraseñas del sistema y otros parámetros de seguridad

3.2 PROTEGER LOS DATOS DEL TITULAR DE LA TARJETA

- Proteja los datos del titular de la tarjeta que fueron almacenados
- Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

3.3 MANTENER UN PROGRAMA DE GESTIÓN DE VULNERABILIDADES

- Usar software antivirus y actualizarlo periódicamente
- Desarrollar y mantener programas y sistemas seguros

3.4 IMPLEMENTAR FUERTES MEDIDAS DE CONTROL DE ACCESO

- Restringir el acceso a las partes clave del negocio
- Asignar identificadores únicos para cada persona que tenga acceso a los datos de titulares de tarjetas
- Restringir el acceso físico a los datos de los titulares de tarjetas

3.5 MONITOREAR REGULARMENTE Y HACER PRUEBAS EN LA RED

- Rastrear y monitorear todo el acceso a los recursos de red y datos de titulares de tarjetas
- Probar regularmente los sistemas y los procesos de seguridad

3.6 MANTENER UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Mantener una política que aborde la seguridad de la información para todo el personal

4. TECNOLOGÍA DE SEGURIDAD DEL COMERCIO ELECTRÓNICO

Los métodos tecnológicos que se ocupan para poder proteger los sistemas informáticos de una empresa son: firewalls, *VPN, cifrado de datos simétricos, cifrado de datos asimétricos, firma digital,* escaneo de vulnerabilidades, entre otros. Muchas empresas establecen sus propias medidas de seguridad para proteger sus sistemas de ataques cibernéticos y de este modo alcanzan el aseguramiento de la información de los clientes.

4.1 FIREWALLS

Su objetivo primordial es evitar la entrada no autorizada. Adicional a esto, es un mecanismo de control, que permite el fortalecimiento del tráfico de uno o más paquetes, a través de la red interna y externa con el propósito de encontrar más comunicación entre sí, configurando dispositivos de hardware y software que se resuelve entorno a las políticas de seguridad, construyendo de este modo una barrera en la red interna de la empresa, aislando los paquetes que no cumplen la condición de acceso [3].

En cuanto a las reglas de ingreso podríamos decir, que los protocolos de seguridad incluyen: acceso a la red, acceso a los servicios locales, autenticación de usuarios remotos tanto entrada o salida, regulaciones de cifrado de datos y medidas de protección a los sistemas de gestión. Estos permiten rechazar o aceptar el ingreso, puesto que adaptan dirección de IP de origen y destino y verifican la cabecera del paquete TCT/IP.

Con todo esto se pueden reducir *ataques cibernéticos* y contrarrestar las *vulnerabilidades* en la red, proporcionando así una plataforma más asegurada en las transacciones de comercio electrónico.

Además, otra solución para preservar la red de forma óptima, sería la de implementar una DMZ, **Véase figura 4.1.** El área que esta entre el firewall interno y el firewall externo se denomina zona *desmilitarizada (DMZ)* la cual, sirve para mantener la confiabilidad en la red.

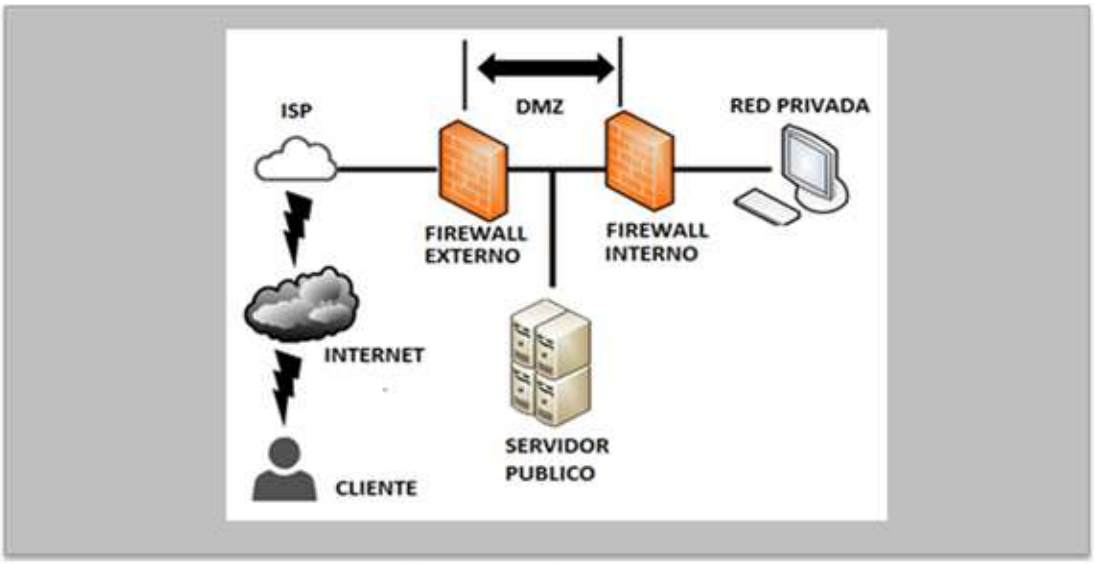


Figura 4.1 *Diagrama de configuración de Firewall con DMZ.*
Fuente: Elaboración Propia.

En esta arquitectura, hay dos firewalls: uno entre Internet y el DMZ y el otro, interno entre la DMZ y la red interna. Todos los servidores públicos se colocan en el DMZ. Así es posible tener reglas de firewalls que admitan el acceso garantizado a los servidores públicos, porque el firewall interior puede restringir todas las conexiones de entrada [4].

4.2 VPN

Mejor conocido como la Red Virtual Privada, que sus siglas en inglés significan: “Virtual Private Network”. Esto atiende, a la infraestructura de red pública, por medio de la tecnología de "túnel", para lograr una red de transmisión segura de datos privados, con la diferencia que toda la información que viaja en este, está cifrada logrando la defensa en la transmisión de sus datos.

Las organizaciones utilizan redes privadas virtuales (VPNs) para crear una conexión de red privada de extremo a extremo (túnel) sobre redes de terceros, tales como Internet o extranets. El túnel elimina la barrera de la distancia y permite que los usuarios remotos tengan acceso a recursos de la red central. Sin embargo, las VPNs no garantizan que la información se mantenga segura mientras atraviesa el túnel. Por este motivo, se aplican métodos criptográficos modernos a las VPNs, con el fin de establecer conexiones seguras de redes privadas de extremo a extremo.

El VPN, utiliza los siguientes protocolos de autenticación: Punto a punto (PPP), por contraseña (PAP), Desafío Handshake, Authentication Protocol (CHAP), Autenticación de

contraseña de Shiva, por desafío mutuo Microsoft (MS-CHAP), Protocolo de autenticación (EAP), Microsoft Punto a Punto Algoritmo de cifrado (MPPE), Protocolo de seguridad de Internet (IPSec), Mecanismo de paquetes Protocolo (SPAP) [5]

4.2.1 PROTOCOLO RECOMENDADO (IPSEC)

El protocolo IP Security (IPsec) proporciona el framework para configurar VPNs seguras y es utilizado con frecuencia a través de Internet para conectar sucursales de oficinas, empleados remotos y socios comerciales. Es una forma confiable de mantener la privacidad de las comunicaciones a la vez que se optimizan las operaciones, se reducen costos y se permite una administración flexible de la red.

Es posible implementar VPNs de sitio a sitio seguras, entre un sitio central y uno remoto, utilizando el protocolo IPsec. IPsec puede también ser utilizado en túneles de acceso remoto, para el acceso de trabajadores a distancia. La aplicación Cisco VPN Client es un método para establecer una VPN de acceso remoto con IPsec. Además de IPsec, puede utilizarse el protocolo Secure Sockets Layer (SSL) para establecer conexiones de acceso remoto VPN. **Véase figura 4.2.1**

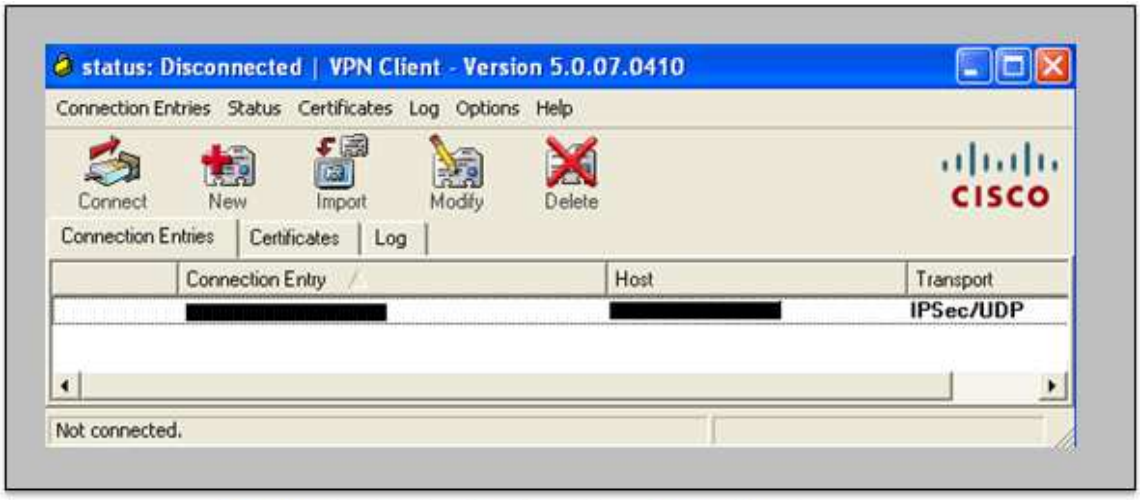


Figura 4.2.1 Aplicación Cisco VPN Cliente.
Fuente: Elaboración Propia.

Las VPNs con SSL son apropiadas para poblaciones de usuarios que requieren control de acceso por aplicación o por servidor, o acceso desde estaciones de trabajo no provistas por la empresa. Las VPNs con SSL no son un reemplazo completo de las VPNs con IPsec. [13]

4.2.2 IMPORTANCIA DE UTILIZAR (IPSEC)

IPSec provee la flexibilidad para soportar el acceso seguro de todos los usuarios, sin importar desde qué host intenten establecer la conexión. Esta flexibilidad permite que las

compañías extiendan sus redes empresariales seguras para cualquier usuario autorizado, proveyendo así conectividad de acceso remoto a recursos corporativos desde cualquier host conectado a Internet.

Las VPNs con IPsec permiten un acceso seguro a todas las aplicaciones cliente-servidor de la organización. Además, las VPNs con SSL no soportan el mismo nivel de seguridad criptográfica soportado por las VPNs con IPsec. Mientras que las VPNs con SSL no pueden reemplazar a las VPNs con IPsec, en muchos casos son complementarias, ya que resuelven diferentes problemas. Este enfoque complementario permite que un solo dispositivo resuelva todos los requisitos de los usuarios de acceso remoto.

4.3 TECNOLOGÍA DE CIFRADO DE DATOS

El cifrado de datos es la tecnología de hardware o software, que se utiliza para poder transformar la información en texto plano a texto cifrado, que puede ser leído únicamente por el emisor o el receptor del mensaje, para evitar que los documentos sean accedidos por terceros no autorizados.

4.3.1 CIFRADO DE DATOS SIMÉTRICOS

El cifrado de datos simétricos, es un protocolo criptográfico donde tanto el emisor como el receptor manejan la misma llave para cifrar y descifrar la información de forma certera [1].

Para establecer la comunicación de forma fiable, el emisor y el receptor necesitan compartir su llave y conservarla en un lugar fiable, ya que si uno de ellos pierde la llave, les será difícil poder comunicarse. **Véase figura 4.3.1**

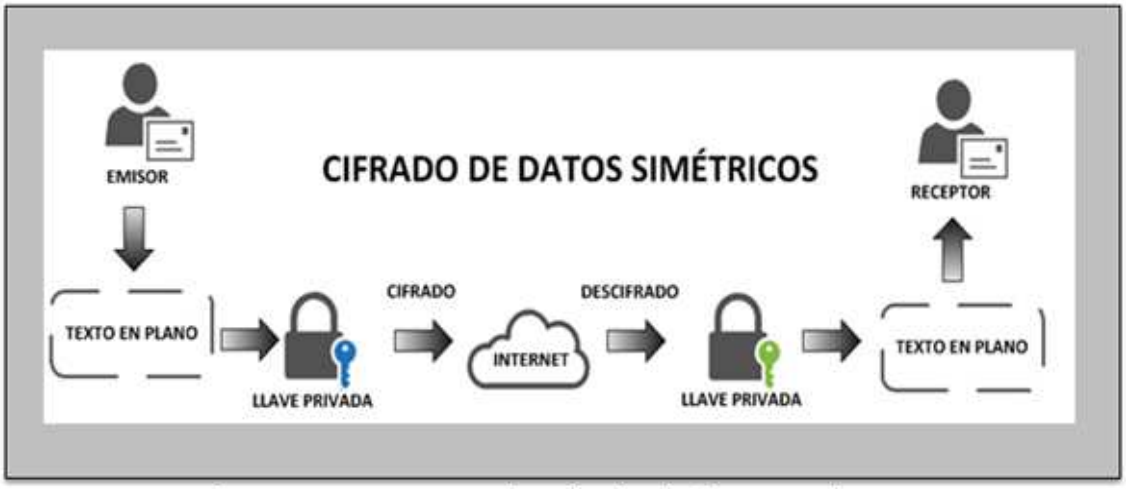


Figura 4.3.1 *Proceso de cifrado de datos simétricos. Fuente: Elaboración Propia.*

4.3.1.1 ALGORITMOS COMUNES PARA CIFRADO DE DATOS SIMÉTRICOS

4.3.1.2 DES (DATA ENCRYPTION STANDARD*)*

Su arquitectura está basada en un sistema monoalfabético, donde un algoritmo de cifrado aplica sucesivas permutaciones y sustituciones al texto en claro. En un primer momento la información de 64bits se somete a una permutación inicial, y a continuación se somete a una permutación con entrada de 8 bits, y otra de sustitución de entrada de 5 bits, todo ello constituido a través de un proceso con 16 etapas de cifrado. [4].

El algoritmo DES usa una clave simétrica de 64bits, los 56 primeros bits son empleados para el cifrado, y los 8 bits restantes se usan para comprobación de errores durante el proceso. La clave efectiva es de 56 bits, por tanto, tenemos 2^{56} combinaciones posibles, por lo que la fuerza bruta se hace casi imposible.

VENTAJAS:

- Es uno de los sistemas más empleados y extendidos, por tanto es de los más probados.
- Implementación sencilla y rápida.

DESVENTAJAS:

- No se permite una clave de longitud variable, es decir, no se puede aumentar para tener una mayor seguridad.
- Es vulnerable al criptoanálisis diferencial (2^{47} posibilidades) siempre que se conozco un número suficiente de textos en claro y cifrados.
- La longitud de clave de 56 bits es demasiado corta, y por tanto vulnerable, no es recomendable utilizarlo. Actualmente DES ya no es un estándar, debido a que una empresa española sin fines de lucro llamado Electronic Frontier Foundation (EFF) construyo en Enero de 1999 una máquina capaz de probar las 2^{56} claves posibles en DES y romperlo sólo en tres días con fuerza bruta

DES fue el algoritmo criptográfico estándar; pero en la actualidad hasta un PC de escritorio puede romperlo. Hoy en día se prefiere usar AES.

4.3.1.3 3DES (TRIPLE DATA ENCRYPTION STANDARD)

Se basa en aplicar el algoritmo DES tres veces, la clave tiene una longitud de 128 bits. Si se cifra el mismo bloque de datos dos veces con dos llaves diferentes (de 64 bits), aumenta el tamaño de la clave.

El 3DES parte de una llave de 128 bits, que es divida en dos llaves, A y B.

Al recibir los datos, aplicamos el algoritmo DES con la llave A, a continuación se repite con la llave B y luego otra vez con la llave A (de nuevo).

3DES aumenta de forma significativa la seguridad del sistema de DES, pero requiere más recursos del ordenador.

Existe una variante del 3DES, conocida como DES-EDE3, con tres claves diferentes y una longitud de 192bits, consiguiendo un sistema mucho más robusto.

4.3.1.4 RC5

Se aplican operaciones XOR sobre los datos, pudiendo ser de 32, 64 o 128 bits. Permite diferentes longitudes de clave, y un número variable de iteraciones (la seguridad del cifrado aumenta exponencialmente cuanto mayor número de iteraciones), también funciona como un generador de número aleatorios, sumándoles a los bloques de texto rotados mediante la XOR.

4.3.1.5 IDEA (INTERNATIONAL DATA ENCRIPTIÓN ALGORITHM)

Aplica una clave de 128 bits sin paridad a bloques de datos de 64 bits, y se usa tanto para cifrar como para descifrar.

Se alteran los datos de entrada en una secuencia de iteraciones parametrizadas, con el objetivo de producir bloques de salida de texto cifrado de 64 bits. IDEA combina operaciones matemáticas como XOR, sumas con acarreo de módulo 2^{16} y multiplicaciones de módulo $2^{16}+1$, sobre bloques de 16 bits.

Según numerosos expertos criptográficos, IDEA es el mejor algoritmo de cifrado de datos existente en la actualidad ya que existen 2^{128} claves privadas que probar mediante el ataque de fuerza bruta.

4.3.1.6 AES (ADVANCED ENCRYPTION STANDARD)

Este algoritmo es el más conocido entre los usuarios de routers en la actualidad, ya que WPA opera con AES como método de cifrado. Este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128bits, de 192 bits y de 256 bits.

El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de bucles de cifrado basado en operaciones matemáticas (sustituciones no lineales de bytes, desplazamiento de filas de la matriz, combinaciones de las columnas mediante multiplicaciones lógicas y sumas XOR en base a claves intermedias).

AES tiene 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits y 14 rondas para llaves de 256 bits. En el año 2006, los mejores ataques conocidos fueron el 7 rondas para claves de 128 bits, 8 rondas para llaves de 192 bits, y 9 rondas para claves de 256 bits. [13]

4.3.2 CIFRADO DE DATOS ASIMÉTRICOS

Llamado también tecnología de clave pública. Es un algoritmo que requiere del manejo de dos claves relacionadas matemáticamente para leer la información. Sin embargo se compone de la siguiente manera: una *llave pública* PK y una *llave privada* SK. La primera, es la que está cifrada pues una vez el emisor envía al receptor la información, este utiliza la llave privada para descifrar los datos remitidos. Asimismo es públicamente disponible para cualquier persona. Cabe resaltar, que la segunda, es aquella que se encuentra descifrada y es exclusivamente adquirida por su propietario [6].

El algoritmo RSA (Rivest-Shamir-Adleman) fue creado en los setenta. El RSA abarca una llave de 1024 bits de cifrado, con una longitud de 512 bits. El problema al utilizar este tipo de algoritmo, es que al momento de cifrar y descifrar una gran cantidad de datos, lo realiza de forma lenta por la cantidad de paquetes enviados. Es recomendable utilizar RSA cuando se envía datos sensibles a través de una red insegura como Internet.

4.3.2.1 ALGORITMOS DE DATOS ASIMÉTRICOS

De los algoritmos que usan llave pública o son asimétricos como también se le conocen entre los más populares se encuentran:

- Diffie-Hellman
- ElGamal
- Algoritmo de ordenamiento

- **DIFFIE-HELLMAN**

Fue el primer algoritmo de llave pública inventado. El algoritmo puede ser usado para la distribución de llaves, pero no para cifrar o descifrar mensajes. Su seguridad reside en la dificultad de calcular logaritmos discretos en un campo finito.

- **ELGAMAL**

Es un algoritmo, procedimiento o esquema de cifrado basado en problemas matemáticos de logaritmos discretos. Usado en la criptografía asimétrica. ElGamal consta de tres componentes: el generador de claves, el algoritmo de cifrado, y el de descifrado.

- **ALGORITMO DE ORDENAMIENTO**

Es un algoritmo que pone elementos de una lista o un vector en una secuencia dada por una relación de orden, es decir, el resultado de salida ha de ser una permutación o reordenamiento de la entrada que satisfaga la relación de orden dada. Las relaciones de orden más usadas son el orden numérico y el orden lexicográfico. Los ordenamientos eficientes son importantes para optimizar el uso de otros algoritmos (como los de búsqueda y fusión) que requieren listas ordenadas para una ejecución rápida. [14]

4.4 TECNOLOGÍA DE AUTENTICACIÓN

4.4.1 FIRMA DIGITAL

Es un mecanismo criptográfico que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico firmado a través de la red. Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión, requiere del algoritmo HASH, porque contiene 128 bits para cifrar y descifrar la información del emisor y el receptor, de esta forma se puede verificar la autenticación e integridad y la ventaja es que no puede ser duplicada o falsificada [7].

Ejemplo:
La empresa “X” necesita enviar documentos que contienen la firma y sello del gerente a la organización “Y”, proyectándose a cerrar un contrato multimillonario, la compañía “X” desea asegurarse que la documentación que se trasladará por una red abierta insegura (Internet), llegue de cualquier forma a la empresa “Y” asegurando así la autenticación e integridad de la información, la empresa “X” tendrá que realizarlo. **Véase figura 4.4.1**

Figura 4.4.1 *Proceso de firma Digital.*
Fuente: Elaboración Propia.

El procedimiento de la figura anterior se explica así:

1. El emisor adjunta el contracto, por medio del e-mail.

2. Se ingresa el correo electrónico en un programa que genera un algoritmo llamado, *“Función HASH”,* la cual convierte el mensaje en una cadena de dígitos (5d9f3f2a2a1c7c17dd082a7).

3. El emisor maneja su llave privada para cifrar el HASH o su firma digital creada, donde nadie puede falsificarla ya que necesita de ella para difundirla.

4. El emisor cifra el correo electrónico y la firma, disponiendo de la llave publica del receptor, originando de tal modo un sobre digital.

5. Este sobre es trasladado por un canal inseguro (Internet) al receptor.

6. El recibe el sobre del emisor, descifra la información enviada con su llave privada que contiene la firma.

7. El receptor ocupa la llave pública del emisor para descifrar la firma.

8. Se ingresa el correo electrónico a enviar en un programa creando un algoritmo llamado función HASH que descifra el mensaje.

9. El receptor compara la información, y si esta coincide significa que es auténtica e integra.

   Como segundo ejemplo tenemos:

   La modernización en El Salvador va evolucionando día con día, por tal motivo la Dirección General de Aduanas (DGRA), ha establecido un sistema de declaración virtual donde importadores y exportadores harán sus declaraciones desde cualquier parte del mundo aplicando su firma digital. Este sistema de cobró entró en vigencia el 28 de Enero de 2014 con el nombre de **Sistema Teledespacho** [8]**.** ***Véase Anexo****.*

4.5 CERTIFICADO DIGITAL

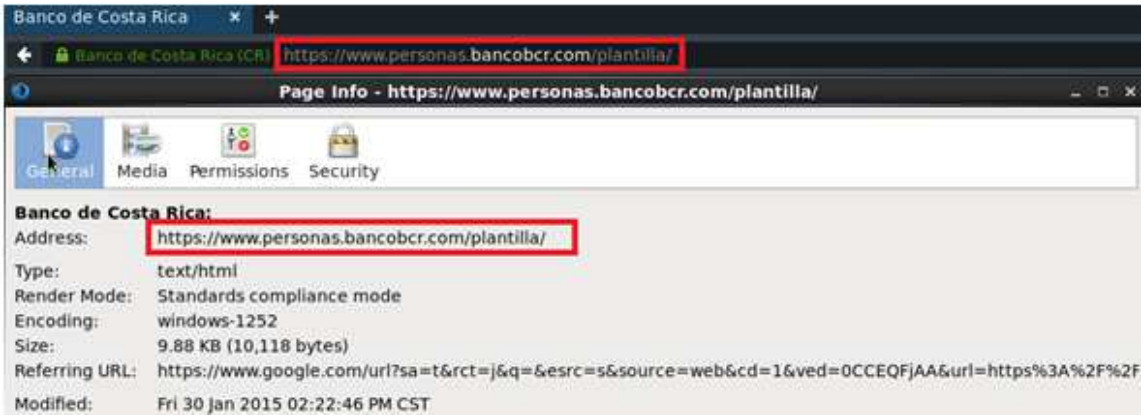
Un certificado digital es un documento electrónico el cual valida la identidad de una entidad (persona, empresa, programa) y asocia esa identidad a una llave pública, que establece comunicación por medio de la red de datos entre dos autoridades, su función es similar a una identidad en la vida real. **Véase figura 4.5**

Figura 4.5 *Protección de transacciones por medio de Secure Socket Layer. Fuente: Certificados digitales SSL y TLS (OWASP).*

4.5.1 COMPROBACIÓN DE VALIDEZ DE UN CERTIFICADO

4.5.1.1 TRES CONDICIONES PARA QUE EL CERTIFICADO SEA VÁLIDO Y ACEPTADO POR EL NAVEGADOR

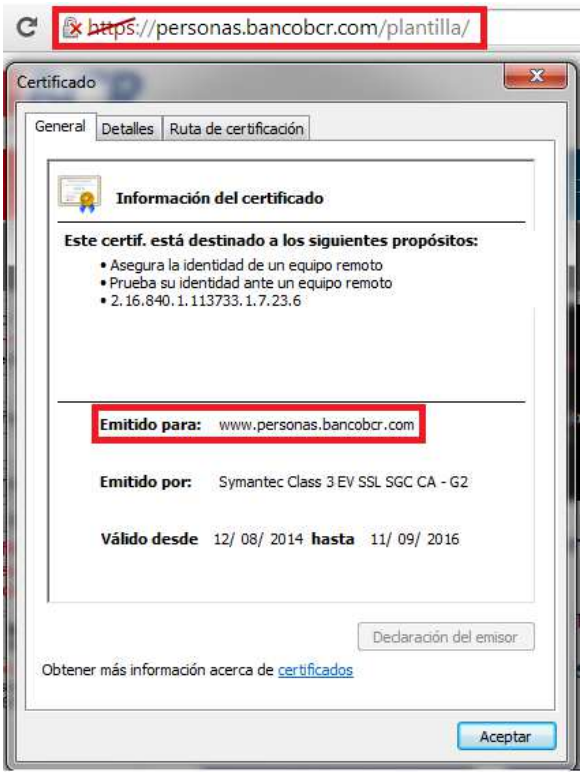
1. **El nombre común CN (Common Name), debe coincidir con la dirección URL que el usuario digita en el navegador.**



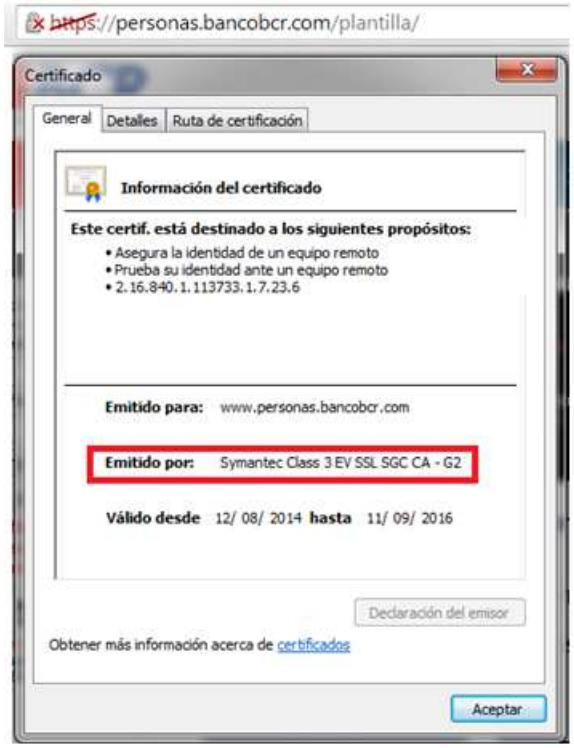
Si el CN no coincide con el certificado de seguridad del sitio web, mostrara una advertencia que informa que la conexión no es privada y que es posible que estén intentando robar su información. [15]

Se puede acceder al sitio web a pesar de la advertencia.

Verificando el CN del certificado como usuario

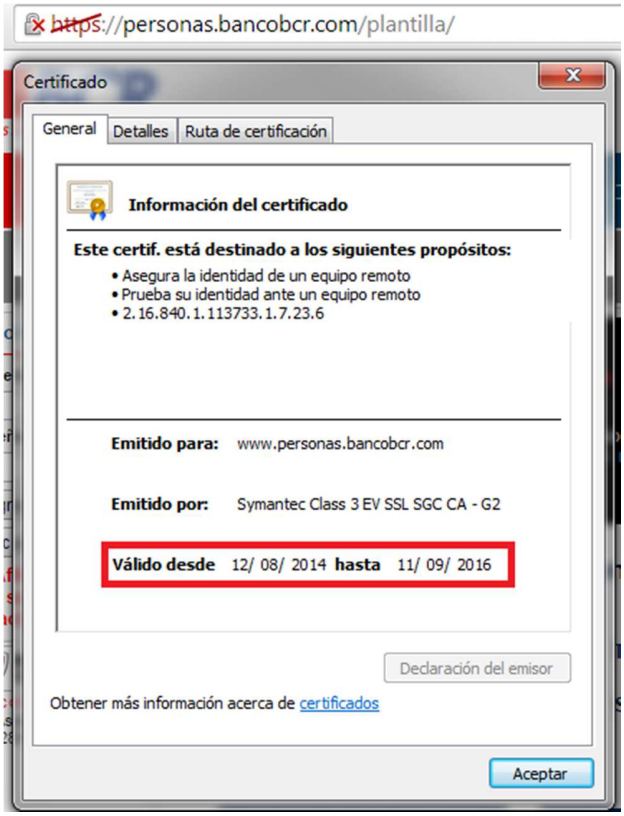


2. **El certificado debe estar firmado por una EC (Entidad Certificadora) válida**



Entidades certificadores registradas en el navegador Firefox:
Preferencias → Avanzado → Cifrado → Ver Certificados

3. **El periodo de validez del certificado**



Siguiendo estos pasos el usuario final puede comprobar la validez de un certificado digital. [15]

4.5.2 TIPOS DE CERTIFICADOS

A. **Los Personales;** son aquellos que exclusivamente proporcionan certificados a un solo usuario, sirve para comprobar la identidad de una persona electrónicamente a la hora de realizar sus transacciones en línea.

B. **Los De Software;** es aquel que las empresas utilizan para demostrar a sus clientes o proveedores que el software sea legítimo, legal y autorizado [9].

4.5.3 CENTRO DE CERTIFICACIÓN DE CA (CERTIFICATE AUTHORITY)

EL ***CA***, es una entidad que emite y revoca certificados digitales, el personal puede ponerse en contacto con el CA para reconocer y comparar la verdadera identidad o si por el contrario es falsa [10].

Según la norma internacional CCITT X.509, el formato interno de un certificado incluye los siguientes puntos: **Véase figura 4.5.3**

1. Nombre del propietario.
2. Clave pública del propietario.
3. Número de serie y fecha de emisión y caducidad.
4. La identidad de la autoridad de certificación que lo ha emitido
5. La firma de la autoridad de certificación (Nombre de la autoridad certificadora, usando su clave privada)
6. El correo electrónico del titular (opcional).

Figura 4.5.3 Proceso de solicitud del certificado.
Fuente: Elaboración Propia.

4.6 PROTOCOLO DE SEGURIDAD DE LAS TRANSACCIONES

Consiste en resguardar la información del usuario, por medio de algoritmos de protección de datos, para mantener seguro los canales de comunicación entre el emisor y el receptor.

4.6.1 CAPA DE SOCKETS SEGUROS (SECURE SOCKET LAYER, SSL) Y SEGURIDAD DE LA CAPA DE TRANSPORTE (TRANSPORT LAYER SECURITY, TLS)

SSL/TLS sirven para cifrar la comunicación del cliente servidor, por lo que permite la seguridad en las transacciones de tarjetas de crédito e información personal, cambiando la URL de HTTP a HTTPS [11].

Asimismo, se necesitan en los navegadores web para completar las operaciones requeridas de trading, poniendo una clave pública y la otra clave de dos métodos de cifrado privado.

El protocolo de seguridad SSL ofrece tres servicios principales:

1. *Garantizar la legalidad del cliente y el servidor;* ya que el uso de la tecnología y confiabilidad del certificado CA de terceros permite al cliente y al servidor que conozcan la identidad uno del otro, con el fin de verificar que el titular del certificado es el usuario legítimo. SSL requiere un titular del certificado digital para el intercambio del apretón de manos (handshakes) entre el servidor y el cliente.

2. *Ocupa cifrado de datos;* pues oculta la información que el cliente ingresa por medio del navegador web para ser almacenada en el servidor. El cliente y el servidor intercambian certificados digitales para garantizar la confidencialidad e integridad de sus datos y la autenticación sus certificados digitales. **Véase figura 4.6.1**

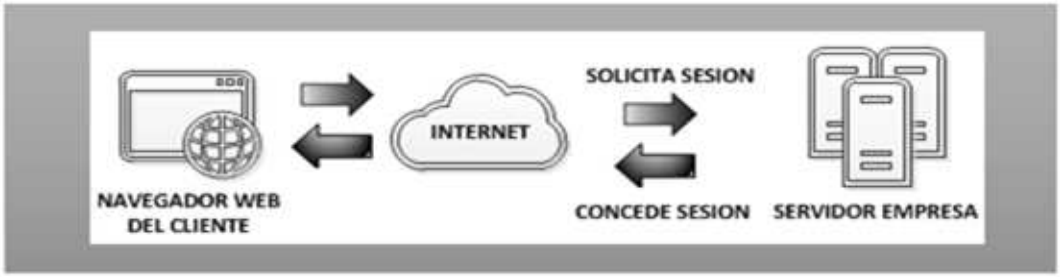


Figura 4.6.1 Proceso de solicitud del certificado.
Fuente: Elaboración Propia.

3. *Mantener la integridad de los datos;* el protocolo SSL utiliza las funciones Hash, para proporcionar un servicio de información segura que se establece entre el canal del cliente y del servidor por lo que transmite los datos certeramente.

Ejemplo de aplicaciones que utilizan SSL/TLS:

- SSL VPN Client
- Portal de Office 365
- FTP server
- Telnet server
- Directorio de Servicios Server (LDAP)
- Los programas desarrollados con Developer Kit para aplicaciones Java y los clientes que utilizan Toolkit IBM para Java
- Aplicativos web (cliente-servidor) que utilizan el protocolo HTTPS (puerto 443)
- OpenVPN

4.7 RECOMENDACIONES PARA CIFRADO DE DATOS Y BUENAS PRÁCTICAS EN LA TECNOLOGIA DE AUTENTICACION

En general, se deben seguir las siguientes recomendaciones al momento de utilizar algoritmos de cifrado:

Para algoritmos simétricos:

- Un tamaño de clave de 128 bits es suficiente para la mayoría de aplicaciones.
- Considerar 168 o 256 bits para sistemas que realicen grandes transacciones financieras.

Para algoritmos asimétricos:

No usar tamaños de clave excesivos a menos que sepa que los necesitará, recuerde que entre más grande sea la clave, mayor es el procesamiento de la máquina. Tener en cuenta:

- Para la mayoría de aplicaciones personales usar claves de 1280 bits.
- Para aplicaciones seguras es aceptable una clave de 1536 bits.
- Para aplicaciones altamente protegidas se debe usar claves de 2048 bits.

Hashes:

- Los tamaños de hash de 128 bits son suficientes para la mayoría de aplicaciones.
- Considere 168 o 256 bits para sistemas altamente seguros.

Recomendaciones según INTECO (Instituto Nacional de Tecnología de la Comunicación) respecto a las tecnologías de autenticación: [16]

Administradores:

- Elección adecuada del tipo de credencial
- Prevención frente a ataques de fuerza bruta
- Sistemas secundarios seguros
- Requisito de verificación de identidad real
- Establecer una buena política de elección de identificadores de usuario
- Exigir complejidad de las credenciales
- Comprobación de credenciales en el registro
- Establecer medidas de seguridad ante cambios de credenciales
- Transmisión cifrada
- No aportar más información de la debida sobre los usuarios
- Autenticación basada en certificados

Usuarios:

- Utilizar contraseñas robustas
- No compartir ni poner al alcance de otros las credenciales
- Utilizar diferentes contraseñas para cada servicio
- Modificar las contraseñas regularmente
- Configurar adecuadamente las opciones de seguridad
- Contactar con el administrador en caso de incidente
- Gestión segura de certificados

5. ANTECEDENTES LEGISLATIVOS DEL COMERCIO ELECTRONICO EN EL SALVADOR

En los temas como la imposición de gravámenes, regulaciones a la que debe estar sometida cualquier actividad comercial, la protección al consumidor, propiedad intelectual así como la legalidad de las transacciones, no son tratados en la legislación actual con referencias directas al comercio electrónico, sin embargo contemplan algunos aspectos que pueden convertirse en facilitadores o inhibidores del comercio electrónico, contenidos en: La ley de impuesto a la transferencia de bienes muebles y a la prestación de servicios, ley de banco y entidades financieras, ley de protección al consumidor.

5.1 LEY DE BANCO

5.1.1 OPERACIONES DE CRÉDITO ENTRE BANCOS

Art. 60.- Las operaciones activas y pasivas que efectúen los bancos y otras instituciones a través de las cuentas que se manejen en el Banco Central, podrán realizarse mediante **intercambio electrónico** de datos. Para tal efecto, tendrán validez probatoria los registros o bitácoras contenidas en los sistemas informáticos, las impresiones que reflejen las transacciones efectuadas por los mismos registros de firmas digitales o de números de identificación personal de los participantes autorizados en dichos sistemas. Las certificaciones extendidas, por el funcionario autorizado por el Banco Central para llevar registros y controles de lo anteriormente referido, tendrán fuerza ejecutiva contra la parte que incumplió. Las instrucciones que dicten los bancos al Banco Central, serán de carácter irrevocable.

5.2 LEY DE IMPUESTO

5.2.1 HECHOS GENERADORES

Art. 3.- Constituyen hechos generadores del impuesto, los débitos en cuentas de depósitos y las órdenes de pago o transferencias correspondientes a: a) Pagos de bienes y servicios mediante el uso de cheque y tarjeta de débito, cuyo valor de transacción u operación sea superior a US$ 750.00; b) Los pagos por medio de **transferencias electrónicas** cuyo valor de transacción u operación sea superior a US$ 750.00; c) Las transferencias a favor de terceros, bajo cualquier modalidad o medio tecnológico, cuyo valor de transacción u operación sea superior a US$ 750.00; d) Los desembolsos de préstamos de cualquier naturaleza, incluyendo los pagos o transferencias de fondos que por cuenta del tarjeta habiente se efectúen al comercio o institución afiliada al Sistema de Tarjeta de Crédito; e) Las operaciones realizadas entre las entidades del Sistema Financiero, en base a cualquier tipo de instrucción de sus clientes o por su propio interés. Los hechos generadores anteriores se entienden ocurridos y causado el impuesto cuando se efectúe el pago, transferencia o desembolso. Las transferencias de recursos al exterior estarán gravadas con el presente impuesto, las cuales se encuentran comprendidas en los literales b) y c) de este artículo.

5.2.2 CAPÍTULO II RETENCIÓN DE IMPUESTO PARA EL CONTROL DE LA LIQUIDEZ

Art. 10.- Los sujetos mencionados en el artículo 6 de esta Ley efectuarán una retención en concepto de impuesto para el control de la liquidez del 0.25% o su equivalente del 2.5 por mil, sobre el monto de los depósitos, pagos y retiros en efectivo, cuyo valor por transacción individual o acumulación mensual exceda de US$ 5,000.00. Los hechos generadores anteriores se entienden ocurridos y causado el impuesto cuando se efectúe el depósito, pago o retiro en efectivo. Serán aplicables las obligaciones establecidas en el artículo 7 de la presente Ley; asimismo la exención de la retención de impuesto para el control de la liquidez para los sujetos y entidades citados en el artículo 4, literal e). Son sujetos pasivos en carácter de contribuyentes, los que realicen depósitos, pagos o retiros en efectivo. Los agentes de retención entregarán a los contribuyentes constancia del impuesto retenido individual o acumulado, de acuerdo a los requisitos y procedimientos que establezca la Administración Tributaria. Dicha constancia tendrá carácter de intransferible. La retención de impuesto por control de liquidez efectivamente enterada, será acreditable contra cualquiera de los impuestos que administra la Administración Tributaria dentro del plazo de dos años, contado a partir de la fecha de la respectiva retención. Para los efectos de la acreditación, **las declaraciones se presentarán en medios electrónicos**. El contribuyente que no acredite o compense el impuesto y el excedente del mismo, de acuerdo a lo dispuesto en el inciso anterior, perderá el derecho a hacerlo en los ejercicios posteriores. Los agentes de retención deberán retener la alícuota al sujeto que realice el depósito, pago o retiro del efectivo. En ningún caso se dejará de pagar el impuesto.

5.3 LEY DE PROTECCIÓN

5.3.1 PRÁCTICAS ABUSIVAS

Art. 18.- Queda prohibido a todo proveedor: a) Condicionar la venta de un bien o la prestación de un servicio a la adquisición de otro, salvo que por la naturaleza de los mismos sean complementarios, que sean parte de las ofertas comerciales o que por los usos y costumbres sean ofrecidos en conjunto; b) Condicionar la contratación a que el consumidor firme en blanco letras de cambio, pagarés, facturas o cualquier otro documento de obligación, u otro considerado como anexo del contrato; salvo que, tratándose de títulos valores, los requisitos omitidos los presuma expresamente la ley. Para los efectos de este literal, las letras de cambio y pagarés deberán contener como mínimo el nombre del deudor, el monto de la deuda, la fecha y lugar de emisión. c) Efectuar cobros indebidos, tales como cargos directos a cuenta de bienes o servicios que no hayan sido previamente autorizados o solicitados por el consumidor. En ningún caso el silencio podrá ser interpretado por el proveedor como señal de aceptación del cargo de

parte del consumidor; d) Negar al consumidor servicios de mantenimiento o de repuestos de piezas de un bien, solamente por no haberlo adquirido en ese establecimiento; e) Discriminar al consumidor por motivos de discapacidad, sexo, raza, religión, edad, condición económica, social o política; f) Realizar gestiones de cobro difamatorias o injuriantes en perjuicio del deudor y su familia, así como la utilización de medidas de coacción físicas o morales para tales efectos; g) Compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización del consumidor. h) Utilizar cualquier maniobra o artificio para la consecución de alza de precios o acaparamiento de: alimentos, artículos de primera necesidad y de servicios esenciales; (2) i) Negarse a detallar el destino de todo pago que efectúe el consumidor; j) Imputar o registrar los pagos hechos por el consumidor, con una fecha posterior a aquélla en la que efectivamente se hizo; k) Prorrogar o renovar automáticamente un contrato de plazo determinado sin el consentimiento del consumidor expresado por escrito; salvo que lo dispuesto en este literal ya esté regulado en otras leyes especiales; l) Cobrar cargos por pago extemporáneo, cuando en la fecha ultima de pago las oficinas o establecimientos del proveedor se encuentren cerradas por tratarse de días no hábiles, días feriados, caso fortuito, fuerza mayor o por cualquier otra circunstancia que sea responsabilidad del proveedor, **como la falta de funcionamiento de los sistemas electrónicos de cobros**; en todos los casos, la fecha de pago se prorrogará para el siguiente día hábil. m) Cobrar por servicios no prestados, salvo en el caso de los cobros mínimos de acceso a los servicios públicos. (2) Cuando se formalicen contratos en los cuales se utilicen letras de cambio, pagarés o cualquier otro documento de obligación, como una facilidad para reclamar el pago que deba efectuar el consumidor, deberá hacerse constar tal circunstancia en el instrumento respectivo. En estos casos, si el consumidor pagare no estando vencido el documento, el proveedor deberá deducir de su importe el descuento calculado al tipo de interés pactado en éste o al tipo de interés legal, en su caso.

5.3.2 PLAZOS Y NOTIFICACIONES

Art. 104.- Los términos a que se refiere esta ley comprenderán solamente los días hábiles. Las notificaciones podrán realizarse **utilizando cualquier medio técnico, sea electrónico**, magnético o cualquier otro, que posibilite la constancia por escrito **y ofrezca garantías de seguridad y confiabilidad**. De la misma forma podrá citar, solicitar informes y en general efectuar toda clase de acto de comunicación procesal.

El comercio electrónico, ya existe en El Salvador desde hace un buen tiempo atrás pero; lastimosamente no se contempla ninguna ley que ampare a la seguridad en las transacciones de dicho comercio, de este modo podemos decir, que a este tema no se le toma la suma importancia, puesto que si no existe alguna regulación que ampare las

instituciones gubernamentales o empresas privadas, esto se prestara cada da más a crímenes informáticos.

Como podemos ver en la leyes anteriores, se muestran artículos que si bien es cierto no nos hablan detalladamente sobre el comercio electrónico, pero se deben realizar transacciones por medios electrónicos que sea capaces de ejecutar una trasferencia segura y confiable. Por lo que es necesario que se implementen procesos adecuados que nos permitan asegurar la calidad de los servicios y tengan la capacidad de detectar acciones fraudulentas que obstaculicen el excelente funcionamiento de los mismos.

5.4 EL COMERCIO ELECTRÓNICO SIN REGULACIÓN EN EL SALVADOR

Según la nota publicada el 7 de Febrero de 2009 en el salvador.com, cita literalmente la siguiente información con respecto al tema del CE:

“Algunos almacenes locales ya permiten hacer compras en línea; empresas de telefonía ofrecen recarga de saldo en sus páginas web y enviando mensajes de texto en donde autoriza el cobro de servicios como el envío de salmos, bromas, compra de ring-tones y participación en rifas y sorteos. Pero si quiere hacer un reclamo o no está satisfecho con lo que recibió, ¿quién podrá defenderlo?”.

Salvo la Defensoría del Consumidor, que ha establecido límites y alcances de la actuación de las empresas locales, el comercio electrónico como tal no está regulado. Si quisiéramos llevar adelante un juicio mercantil, por una transacción que se realizó vía electrónica, ningún juez aceptará como válidos los documentos impresos de las comunicaciones, y mucho menos de los correos enviados y recibidos.

Esas transacciones comerciales que ya pueden realizarse, aunque son legales, "falta regularlas adecuadamente", como reconoce Sigfredo Figueroa, director ejecutivo del programa ePaís, que lleva a cabo la Secretaría Técnica de la Presidencia de la República.
Esta dependencia, con el apoyo de la Comisión Nacional para la Sociedad de la Información y consultores nacionales e internacionales, ha elaborado una “Estrategia Nacional”, para que el país desarrolle y aproveche sus potenciales informáticos.

"Se definieron tres grandes líneas de trabajo: cómo se regulaba la comunicación y firma electrónica, la protección de datos y comercio electrónico. De todo eso, quizá lo más importante en este momento es el Anteproyecto de Ley de Comunicación y Firma Electrónica, porque eso le va a dar una legalidad a todas las operaciones electrónicas (...)

Esa es la ley madre para que exista validez legal de todas las operaciones", destacó Figueroa.

6. ACELERAR LA FORMACIÓN DE PROFESIONALES DE SEGURIDAD INFORMATICA ESPECIALIZADOS EN INFORMATICA FORENSE EN EL SALVADOR

Los delitos informáticos tales como: el robo de datos, el fraude bancario, la suplantación de identidad, el espionaje industrial, son una preocupación global que abarca desde usuarios finales hasta grandes empresa. Esta larga cadena de acciones la puede ejecutar cualquier individuo al momento de hacer una transacción final por Internet.

Ahora en día existen nuevas formas de ataques informáticos, obtención de documentación digital, atraco de identidad fraude y hasta desgraciadamente terrorismo. Es por eso que surge la necesidad de determinar ¿Qué fue lo que paso?, ¿Cuándo paso?, ¿Por dónde entro?, ¿De dónde provino el ataque?, y principalmente, ¿Dónde está?.

Del origen de estas preguntas nace de la pérdida o un acto consumado entonces es ahí cuando necesitamos de un forense informático, el cual debe poseer los conocimientos, metodologías, pericia y técnicas adecuadas para tratar las evidencias y ofrecer respuestas a las preguntas planteadas por los usuarios de los sistemas informáticos.

Estos delitos conllevan a la necesidad de poder contar con profesionales del mundo de la informática y derecho que apliquen de forma práctica a la pericia, que sepan cómo realizar valoraciones, dictámenes y peritaciones, con el fin de colaborar en la resolución de litigios por medio de la extracción de la evidencia digital y presentarlas ante el juez.

CONCLUSION

Este trabajo de investigación, nos demuestra que las empresas deben tener cierta preeminencia sobre el manejo correcto de los intercambios de negociación, desde que comienza toda la secuencia de pasos, hasta finalizarlo eficientemente y seguro. Para lograr que esto se cumpla, debemos acoplar todos aquellos componentes que estén relacionados con un buen diseño de políticas de seguridad, elementos propios de la empresa, métodos de protección y determinados requisitos; ya que si lo hacemos por sí solo y no lo tomamos en cuenta, no tendremos la habilidad de romper barreras que se interpongan al momento de ejecutar la tan esperada acción para los clientes.

Es menester, que las organizaciones detecten donde están localizadas las deficiencias en los sistemas que utilizan, porque de lo contrario, no se podrá asegurar perfectamente la información, ya que se podría encontrar grandes riesgos que solo pueden ser resueltos con la verificación constante, de que estos cuenten con características de ser más confidenciales, íntegros, autenticados, con eficacia, no repudiados, entre otros, diariamente. Esto se necesita con el propósito, de estar bien preparados para responder con rapidez y positivamente contra los ataques que cada vez son más constantes hacia las instituciones públicas o privadas tanto dentro como fuera del país.

En resumen, se espera que el análisis de esta investigación pueda abrir paso a nuevas ideas, que nos enriquezca aún más de conocimientos y de esta manera se pueda lograr combatir de raíz las graves amenazas a las que se exponen las empresas hoy en día puesto que la tecnología avanza a gran velocidad y los usuarios que la emplean no deben estar vulnerables ante tal problemática, sino más bien, vuelvan todos sus esfuerzos en contar con un amplio y mejorado sistema de seguridad, para que pueda existir un incremento en las ganancias de la organizaciones y colocarlas en un ambiente dinámico y competitivo.

RECOMENDACIONES

Una vez finalizado este trabajo de Investigación, se considera significativamente que se analicen y se pongan en práctica, los siguientes detalles que se sugieren a continuación:

- Usar medidas de seguridad informática a nivel empresarial, donde cada departamento debe estar conocedor de cómo se maneja la información dentro de la red para prevenir cualquier desestabilización en sus operaciones y no se generen altas pérdidas en el centro de costos de las mismas.

- Evaluar el impacto de pérdida y los riesgos que causa el empleo de la información digital, para identificar que tan protegida se encuentra y con anticipación se puedan corregir los errores, creando de este modo nuevas oportunidades de mejora.

- Implementar sistemas de aplicación integral, para impedir que los firewalls se vean afectados por los ataques masivos que destruyen y hacen que se pierda totalmente la fidelidad de todos los procesos que se hacen con los datos, en las diversas organizaciones que se benefician de este recurso tan necesario para su crecimiento.

- Crear dentro de las empresas un área dentro del departamento de informática, que se dedique solamente al monitoreo y control de todos los intercambios que se realizan de los datos en la red ya que de no ser así, no se podrían descubrir cuáles son las vulnerabilidades que perjudican el buen desarrollo de las transacciones en los sistemas de seguridad.

- Instalar y actualizar un antivirus periódicamente, ayuda a reducir amenazas peligrosas en los dispositivos que se utilizan de almacenamiento de datos o archivos descargados de Internet.

- Instalar un Firewall, servirá para interrumpir las entradas sin permiso previo en la web.

- Aplicar contraseñas seguras y modificarlas con frecuencia, permitirá que se dificulte el acceso no autorizado en los equipos, logrando así impedir el robo de información sumamente confidencial.

- Verificar si las páginas web en las que se navega, contienen el certificado o sello para obviar que no se están realizando procedimientos sin confiabilidad o excelencia.

- Estudiar a profundidad acerca de nuevas técnicas de protección en los equipos informáticos, nos dará la certeza de caminar hacia la resolución más efectiva a estos problemas de inseguridad que cada vez más producen bajo crecimiento económico en las empresas.

REFERENCIAS

[1] CISSP All-in-One Exam Guide, 6th Edition, Shon Harris, Feb 1, 2013.

[2] Seguridad de la Información: Expectativas Riesgos y Técnicas de Protección, Vicente Aceituno Canal, Febrero 28, 2006.

[3] CompTIA Security+ Certification Study Guide, Third Edition: Exam SY0-201 3E Paperback, August 11, 2009.

[4] IPsec Virtual Private Network Fundamentals by James Henry Carmouche, July 19, 2006.

[5] IPSec VPN Design By Vijay Bollapragada, Mohamed Khalid, Scott Wainner, April 07, 2005.

[6] Data and Computer Communications (8th Edition) Williams Stallings, August 12, 2006.

[7] Operating Systems: Internals and Design Principles (7th Edition), Williams Stallings, March 10, 2011.

[8] LEY DE SIMPLIFICACIÓN ADUANERA, Asamblea Legislativa de El Salvador, Disponible en línea: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-simplificacion-aduanera-teledespacho/ Verificado el 25 de diciembre de 2014.

[9] Tipos de certificados SSL, Disponible en línea: https://www.globalsign.es/centro-informacion-ssl/tipos-de-certificado-ssl.html. Verificado el 25 de diciembre de 2014.

[10] Computer Security -- ESORICS 2013: 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013, Proceedings (Lecture Notes in Computer Science / Security and Cryptology) by Jason Crampton (Editor), Sushil Jajodia (Editor), Dr. Keith Mayes University of London (Editor), August 6, 2013.

[11] Cryptography and Network Security Principles and Practice, 5th Edition, Williams Stallings, January 14, 2010.

[12] PCI Security Standards Council, Disponible en línea: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf. Verificado el 29 de enero de 2015.

[13] Protocols for Secure Electronic Commerce, Second Edition, Mostafa Hashem Sherif, Noviembre 24, 2003.

[14] Network Security with OpenSSL, Pravir Chandra, Matt Messier, John Viega, June 27, 2002.

[15] Certificados digitales SSL y TLS, Disponible en línea: https://www.owasp.org/images/1/1f/6.OWASP_Day_Costa_Rica_Didier.pdf. Verificado el 29 de enero de 2015.

[16] Guía sobre riesgos y buenas prácticas en autenticación online, Disponible en línea: https://www.incibe.es/CERT/guias_estudios/guias//Guia_Autenticacion. Verificado el 29 de enero de 2015.

ANEXOS

Teledespacho, modernización de las aduanas

Desde este 14 de febrero, el uso de Teledespacho es obligatorio para todos los importadores a la hora de declarar sus mercancías en las aduanas del país. Entérese cómo funciona este sistema y las empresas que brindan soporte técnico.

Rhina Ventura
El Diario de Hoy
suplementos@elsalvador.com

Como parte de la modernización de la Dirección General de Aduanas (DGRA), cobró vigencia el sistema de Teledespacho por Internet. San Bartolo y la Delegación de Aduanas de la Tres Torres fueron las primeras en dar este servicio desde el 28 de enero; para el 14 de febrero la medida es obligatoria.

Por el momento no entrarán en Teledespacho por Internet, las operaciones realizadas a través del Formulario Aduanero Único Centroamericano (FAUCA) y las exportaciones. Se espera que la declaración de ambas se realicen vía Internet en la primera semana de marzo.

El fin concreto del cambio es implementar un sistema de declaración virtual donde importadores y exportadores realicen sus declaraciones desde su casa y de cualquier parte del mundo utilizando su firma digital.

Esta disposición establece que los oficiales aduaneros ya no tendrán que digitalizar la información requerida en el formulario de la Declaración de Mercancías, sino más bien verificar los datos requeridos.

¿Ventajas? Se sintezan en ahorro de tiempo y de recursos tanto para los usuarios como para la DGRA. Significa una disminución de al menos 30 minutos por cada cliente al llenar el formulario que contiene alrededor de 60 casillas. Lo mejor radica en la posibilidad de declarar las 24 horas los 365 días del año.

Un sistema seguro

El Teledespacho es un sistema integrado de información entre clientes, bancos, aduanas e instituciones relacionadas, que permite establecer conexiones a través de una red privada VPN (Virtual Private Network). Significa que los clientes se conectan con Aduanas sin que otros usuarios de internet tengan acceso al paquete de datos.

Los requerimientos tecnológicos para realizar los trámites aduanales con el Teledespacho son una Computadora Pentium 2 ó 3 o equivalente, tarjeta modem, IP pública (tipo de conexión con Aduanas), computadora con CD-ROM y 64 memoria RAM.

Actualmente existen diez empresas que brindan soporte técnico a los usuarios de Teledespacho, va desde la instalación del software de comunicación y digitalización hasta la configuración del hardware para que puedan conectarse con las Aduanas.

Según David Rodríguez, gerente de servicio al cliente de DIESCO, estas firmas son útiles, ya que los usuarios del Teledespacho con frecuencia tienen problemas de conexión de internet o muchas dudas para llenar los formularios.

LEY DE SIMPLIFICACIÓN ADUANERA, Asamblea Legislativa de El Salvador

DECRETO Nº 529.-

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I.- Que el crecimiento del tráfico internacional de mercancías y la profusión de negociaciones comerciales en que se encuentra inmerso el país imponen la necesidad de adecuar los servicios aduaneros a los estándares mundiales de calidad y eficiencia en términos de facilitación del comercio internacional, control de la recaudación fiscal y protección de la sociedad.

II.- Que en este mismo contexto, los países del área también han realizado esfuerzos para adecuar la legislación regional a las exigencias de simplificación y facilitación de los procedimientos aduaneros, habiéndose autorizado en tal sentido la modalidad de despacho conocida como autodeterminación o autoliquidación, regulada por el Art. 75 del Código Aduanero Uniforme Centroamericano, la cual debe ser desarrollada para su implementación en la legislación interna de cada país.

III.- Que la adecuación de los servicios aduaneros a las exigencias antes planteadas requiere de la implementación de un marco legal moderno y flexible que permita el desarrollo de nuevas modalidades de despacho que por su agilidad otorguen ventajas competitivas a los productores nacionales, en una relación de equilibrio con el control aduanero.

POR TANTO,

en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Hacienda,

DECRETA, la siguiente:

LEY DE SIMPLIFICACION ADUANERA

Art. 1.- La presente Ley tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de las operaciones aduaneras, a través del uso de sistemas automáticos de intercambio de información.

Cuando en el texto de esta ley, se mencione Dirección General deberá entenderse que se refiere a la Dirección General de la Renta de Aduanas.

Art. 1-A.- LA DIRECCIÓN GENERAL REQUERIRÁ DE LOS AUXILIOS DE LA FUNCIÓN PÚBLICA ADUANERA Y DE LOS DEMÁS USUARIOS, LA TRANSMISIÓN ELECTRÓNICA DESDE LAS TERMINALES REMOTAS UBICADAS EN SUS PROPIAS OFICINAS O DESDE EL PROPIO RECINTO FISCAL, ACCESANDO EN LÍNEA AL SERVIDOR CENTRAL DE LA DIRECCIÓN GENERAL, O POR OTROS MEDIOS, DE LA INFORMACIÓN RELATIVA A LOS ACTOS, OPERACIONES Y REGÍMENES ADUANEROS EN QUE PARTICIPEN. (1)

LOS SUJETOS PASIVOS Y DEMÁS USUARIOS DEL SERVICIO ADUANERO, PODRÁN TRANSMITIR POR LA VÍA ELECTRÓNICA, ENTRE OTROS DOCUMENTOS, DECLARACIONES DE MERCANCÍAS, CERTIFICADOS O CERTIFICACIONES DE ORIGEN, MANIFIESTOS DE CARGA, CONOCIMIENTOS DE EMBARQUE Y CUALQUIER OTRO DOCUMENTO REQUERIDO PARA REALIZAR OPERACIONES DE COMERCIO EXTERIOR, CONFORME A LOS REQUISITOS Y FORMALIDADES ESTABLECIDOS EN LA LEGISLACIÓN ADUANERA O DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL EMITIDAS POR LA DIRECCIÓN GENERAL. (3)

Art. 2.- PREVIO AL ARRIBO DE LAS MERCANCÍAS AL TERRITORIO ADUANERO NACIONAL, LOS TRANSPORTISTAS YA SEAN TERRESTRES, MARÍTIMOS O AÉREOS, O LOS AGENTES DE TRANSPORTE EN SU CASO, ESTÁN OBLIGADOS A PROPORCIONAR A LA ADUANA DE INGRESO, MEDIANTE TRANSMISIÓN ELECTRÓNICA U OTROS MEDIOS AUTORIZADOS POR LA DIRECCIÓN GENERAL, LA INFORMACIÓN CONTENIDA EN EL MANIFIESTO GENERAL DE CARGA. (1)

EN LOS CASOS EN LOS QUE EL IMPORTADOR, NO PUEDA ACREDITAR EL VALOR DE LA PRIMA DE SEGURO POR NO HABER EFECTUADO LA CONTRATACIÓN DE UNA PÓLIZA PARA EL TRANSPORTE DE CARGA, EL SERVICIO DE ADUANAS, PODRÁ ESTABLECER COMO PRIMA DE SEGURO, LOS PORCENTAJES QUE A CONTINUACIÓN SE DETALLAN: (3)

a) TRANSPORTE REGIONAL TERRESTRE DE CARGA: 1.25% SOBRE EL VALOR FOB DE LAS MERCANCÍAS; Y

b) TRANSPORTE INTERNACIONAL DE CARGA, SIN CONSIDERACIÓN DE LA MODALIDAD DE TRANSPORTE: 1.50% SOBRE EL VALOR FOB DE LAS MERCANCÍAS.

PARA LA DETERMINACIÓN DEL VALOR DE FLETE, EL SERVICIO DE ADUANAS, PODRÁ ESTABLECER DE MANERA PERIÓDICA VALORES DE REFERENCIA, EN CONSULTA CON LAS GREMIALES DE TRANSPORTE O EMPRESAS DEL RUBRO, LOS CUALES SERÁN PUBLICADOS PARA CONOCIMIENTO DE LOS IMPORTADORES Y AUXILIARES DE LA FUNCIÓN PÚBLICA ADUANERA. (3)

EN LOS CASOS EN LOS CUALES NO SE PUEDA ACREDITAR UN VALOR DE FLETE, POR PARTE DEL IMPORTADOR, EL SERVICIO DE ADUANAS, ESTABLECERÁ EL 10% SOBRE EL VALOR FOB DE LAS MERCANCÍAS. (3)

EN CUANTO A LA INFORMACIÓN RELATIVA A LAS MERCANCÍAS, DEBERÁ CONSIGNARSE EL PESO BRUTO EN KILOGRAMOS, LA CLASE Y CANTIDAD DE BULTOS, ASÍ COMO LA CLASE O TIPO GENÉRICO DE LAS MERCANCÍAS, DETALLANDO PRIMERO Y EN ORDEN DESCENDENTE LAS DE MAYOR VALOR COMERCIAL. (1)

LOS GASTOS DE TRANSPORTE DE LAS MECÁNICAS IMPORTADAS HASTA EL PUERTO O LUGAR DE IMPORTACIÓN, ASÍ COMO LOS GASTOS DE CARGA, DESCARGA Y MANIPULACIÓN OCASIONADOS POR EL TRANSPORTE DE LAS MERCANCÍAS IMPORTADAS HASTA EL PUERTO DE IMPORTACIÓN Y EL COSTO DEL SEGURO, ESTARÁN INCLUIDOS EN EL VALOR EN ADUANA DE LAS MERCANCÍAS, PARA LOS EFECTOS DEL NÚMERO 2 DEL ART. 8 DEL ACUERDO A LA APLICACIÓN DEL ARTÍCULO VII DEL ACUERDO GENERAL SOBRE ARANCELES ADUANEROS Y COMERCIO DE 1994. (1)

PARA EFECTOS DEL INCISO PRIMERO DE ESTE ARTÍCULO, SE CONSIDERA AGENTE DE TRANSPORTE, LA PERSONA NATURAL O JURÍDICA REGISTRADA ANTE LA DIRECCIÓN GENERAL, QUE REPRESENTAN EN EL PAÍS, A LAS COMPAÑÍAS QUE SE DEDICAN AL TRANSPORTE INTERNACIONAL DE MERCANCÍAS. (1)

EL TRANSPORTISTA QUE EJECUTA UNA OPERACIÓN DE TRÁNSITO ADUANERO Y EL AGENTE DE TRANSPORTE, SERÁN RESPONSABLES ANTE EL FISCO POR LA ENTREGA DE LAS MERCANCÍAS A LA ADUANA DE DESTINO, EN CONSECUENCIA, SIN PERJUICIO DE LAS RESPONSABILIDADES CIVILES, ADMINISTRATIVAS Y PENALES EN QUE PUEDAN INCURRIR EN EL EJERCICIO DE SUS FUNCIONES, RESPONDERÁN SOLIDARIAMENTE POR EL PAGO DE LOS DERECHOS E IMPUESTOS A LA IMPORTACIÓN SI LAS MISMAS NO ARRIBAN EN SU TOTALIDAD A DICHA ADUANA. A LOS EFECTOS DE CUBRIR ESTA RESPONSABILIDAD, TANTO EL TRANSPORTISTA COMO EL AGENTE DE TRANSPORTE, COMO CONDICIÓN PARA EJECUTAR O HACER EJECUTAR EL TRÁNSITO ADUANERO DE MERCANCÍAS, DEBERÁN RENDIR A FAVOR DEL FISCO, UNA GARANTÍA GLOBAL QUE SERÁ FIJADA POR LA DIRECCIÓN GENERAL, DE CONFORMIDAD A LOS CONVENIOS INTERNACIONALES QUE REGULAN LA MATERIA DEL TRANSPORTE INTERNACIONAL DE MERCANCÍAS, SUSCRITOS Y RATIFICADOS POR EL SALVADOR. (1)

Art. 3.- EN EL SISTEMA DE AUTODETERMINACIÓN O AUTOLIQUIDACIÓN, CORRESPONDE AL DECLARANTE LA DETERMINACIÓN DE LA OBLIGACIÓN TRIBUTARIA ADUANERA Y EL CUMPLIMIENTO DE LAS DEMÁS REGULACIONES ESTABLECIDAS EN LAS LEYES RESPECTIVAS, Y ADEMÁS, LA PRESENTACIÓN DE LA DECLARACIÓN DE MERCANCÍAS Y EL PAGO DE LOS TRIBUTOS QUE SE CAUSEN. (3)

Excepcionalmente, la autoridad aduanera efectuará la determinación de la obligación tributaria aduanera sobre la base de la información entregada por el declarante y el reconocimiento de las mercancías. Tales casos de excepción, serán determinados por la Dirección General a través de normas administrativas de aplicación general.

CUANDO EN EL EJERCICIO DE SUS FACULTADES DE VERIFICACIÓN INMEDIATA O FISCALIZACIÓN A POSTERIORI, ESTABLECIDAS EN LA LEY, LA AUTORIDAD ADUANERA COMPETENTE DETERMINE EL INCUMPLIMIENTO DE LA OBLIGACIÓN TRIBUTARIA ADUANERA, PROCEDERÁ A LA LIQUIDACIÓN OFICIOSA DE LOS TRIBUTOS A LA IMPORTACIÓN DEJADOS DE PAGAR Y A IMPONER LAS SANCIONES RESPECTIVAS. (3)

Art. 4.- Para efectos de la autodeterminación de las obligaciones aduaneras, el declarante o su representante tendrá derecho a efectuar, de acuerdo al procedimiento que establezca al efecto la Dirección General, el examen previo de las mercancías, que consiste en el reconocimiento físico de las mismas, previo a su despacho, para determinar sus características generales y los elementos determinantes de las obligaciones tributarias aduaneras y demás requisitos que se requieren para la autorización del régimen u operación aduanera a que serán destinadas.

ASIMISMO, EL DECLARANTE DEBERÁ EFECTUAR EL PAGO DE SUS OBLIGACIONES TRIBUTARIAS ADUANERAS EN LOS BANCOS DEL SISTEMA FINANCIERO, MEDIANTE TRANSFERENCIA ELECTRÓNICA DE FONDOS DE LA CUENTA BANCARIA DEL DECLARANTE, AGENTE DE ADUANAS O DE TERCEROS EN SU CASO, A LA CUENTA CORRIENTE DE LA DIRECCIÓN GENERAL DE TESORERÍA, O A TRAVÉS DE CUALQUIER OTRO MEDIO QUE AL EFECTO SE AUTORICE. EN ESTE CASO, EL BANCO QUE PERCIBA EL PAGO DE TRIBUTOS, ESTARÁ OBLIGADO A TRANSMITIR INMEDIATAMENTE A LA DIRECCIÓN GENERAL

DE TESORERÍA Y A LA DIRECCIÓN GENERAL, TODA LA INFORMACIÓN REFERIDA A DICHO PAGO.

LOS BANCOS QUE TRANSMITAN A LA DIRECCIÓN GENERAL, INFORMACIÓN ERRÓNEA, INCOMPLETA O FALSA SOBRE EL PAGO DE OBLIGACIONES TRIBUTARIAS ADUANERAS, EN VIRTUD DE LO CUAL LA AUTORIDAD ADUANERA AUTORICE LA ENTREGA DE MERCANCÍAS QUE SE ENCUENTREN EN DEPÓSITO TEMPORAL O ALMACENADAS EN CUALQUIER OTRO RECINTO FISCAL, TENDRÁN POR ESTE HECHO, RESPONSABILIDAD SUBSIDIARIA FRENTE AL FISCO, POR EL PAGO DE LOS RESPECTIVOS DERECHOS E IMPUESTOS QUE TOTAL O PARCIALMENTE NO HUBIERAN SIDO EFECTIVAMENTE PERCIBIDOS. A ESTOS EFECTOS, LOS BANCOS TENDRÁN RESPONSABILIDAD PATRIMONIAL POR LAS ACTUACIONES DE SUS DEPENDIENTES.(1)

Art. 5.- CUALQUIER PERSONA CON UN INTERÉS LEGÍTIMO PODRÁ EFECTUAR CONSULTAS A LAS AUTORIDADES ADUANERAS, COMO ACTO PREVIO A LA PRESENTACIÓN DE LA DECLARACIÓN, RELACIONADAS CON LA APLICACIÓN DE LAS DISPOSICIONES LEGALES, REGLAMENTARIAS O ADMINISTRATIVAS QUE REGULAN LOS PROCEDIMIENTOS ADUANEROS, LA CLASIFICACIÓN ARANCELARIA, LA VALORACIÓN ADUANERA, LOS TRIBUTOS QUE SE CAUSAN CON MOTIVO DE LAS OPERACIONES ADUANERAS O SOBRE CUALQUIER OTRO ASUNTO QUE TENGA RELEVANCIA TRIBUTARIA ADUANERA; PARA TALES EFECTOS EL SUJETO PASIVO, SU REPRESENTANTE O APODERADO DEBIDAMENTE ACREDITADO, DEBERÁ PRESENTAR ESCRITO, EN EL QUE DETALLE EL CRITERIO RAZONADO QUE SOBRE EL ASUNTO CONSULTADO TENGA; ADEMÁS, DE PROPORCIONAR TODOS LOS ELEMENTOS Y DOCUMENTOS NECESARIOS, Y DE SER POSIBLE LA MUESTRA CORRESPONDIENTE. DICHAS CONSULTAS SERÁN EVACUADAS POR LA AUTORIDAD ADUANERA A MÁS TARDAR DENTRO DE LOS QUINCE DÍAS HÁBILES SIGUIENTES A SU RECEPCIÓN, Y SÓLO SURTIRÁN EFECTO EN EL CASO CONCRETO ESPECÍFICAMENTE CONSULTADO; DICHO PLAZO PODRÁ SER AMPLIADO DE OFICIO POR UN PERÍODO IGUAL POR LA AUTORIDAD ADUANERA, CUANDO POR LA NATURALEZA DE LA CONSULTA SEA NECESARIO EFECTUAR INVESTIGACIONES Y ANÁLISIS QUE REQUIERAN UN MAYOR TIEMPO QUE EL SEÑALADO.

SI LA EVACUACIÓN DE CONSULTAS REQUIERE NECESARIAMENTE DE UN ANÁLISIS DE LABORATORIO, EL INTERESADO PODRÁ REQUERIR LOS SERVICIOS DEL DEPARTAMENTO DE LABORATORIO DE LA DIRECCIÓN GENERAL, O PRESENTAR DICTÁMENES EMITIDOS POR CUALQUIER LABORATORIO PÚBLICO O PRIVADO DEBIDAMENTE AUTORIZADO POR LA AUTORIDAD GUBERNAMENTAL COMPETENTE Y CERTIFICADO POR EL CONSEJO NACIONAL DE CIENCIA Y TECNOLOGÍA.

LA PRESENTACIÓN DE LA CONSULTA NO SUSPENDE EL CUMPLIMIENTO DE LAS OBLIGACIONES TRIBUTARIAS Y NO TRIBUTARIAS ADUANERAS. LA RESPUESTA QUE HAYA SIDO EMITIDA POR ESCRITO POR LA AUTORIDAD ADUANERA Y QUE SE HAGA DEL CONOCIMIENTO AL INTERESADO, NO TIENE CARÁCTER DE RESOLUCIÓN Y NO ES SUSCEPTIBLE DE IMPUGNACIÓN O RECURSO ALGUNO. (3)

Art. 5-A. EN EL CASO DE SOLICITUDES RELACIONADAS CON CRITERIOS O RESOLUCIONES ANTICIPADAS, PRESENTADAS ANTE LA DIRECCIÓN GENERAL, EN EL MARCO DE LOS ACUERDOS, CONVENIOS, TRATADOS Y OTROS INSTRUMENTOS EN MATERIA COMERCIAL, ÉSTAS DEBERÁN SER RESUELTAS DENTRO DE LOS PLAZOS ESTABLECIDOS EN DICHOS INSTRUMENTOS LEGALES, MEDIANTE RESOLUCIÓN RAZONADA. DE LA RESOLUCIÓN EMITIDA PROCEDERÁ EL RECURSO DE APELACIÓN ANTE EL TRIBUNAL DE APELACIONES DE LOS IMPUESTOS INTERNOS Y DE ADUANAS, CONFORME AL PROCEDIMIENTO, FORMALIDADES Y PLAZOS ESTABLECIDOS EN SU LEY DE ORGANIZACIÓN Y FUNCIONAMIENTO.

LAS SOLICITUDES DE CRITERIOS O RESOLUCIONES ANTICIPADAS ÚNICAMENTE PROCEDERÁN EN LOS CASOS PREVISTOS EN LOS ACUERDOS, CONVENIOS, TRATADOS Y OTROS INSTRUMENTOS EN MATERIA COMERCIAL, Y DEBERÁN CUMPLIR CON LOS REQUISITOS DE TIEMPO Y FORMA ESTABLECIDOS EN LOS MISMOS, DEBIENDO LA DIRECCIÓN GENERAL, TRAMITARLA CONFORME AL PROCEDIMIENTO REGULADO EN DICHAS DISPOSICIONES LEGALES.

LOS CRITERIOS O RESOLUCIONES ANTICIPADAS, SE ACEPTARÁN CUANDO SE PRESENTEN ANTES QUE SE REALICE LA IMPORTACIÓN DE LA MERCANCÍA EN CUESTIÓN, LOS CUALES CONSERVARÁN SU VALIDEZ POR TRES AÑOS, SIEMPRE Y CUANDO NO HAYAN CAMBIADO LAS CONDICIONES QUE FUNDAMENTARON SU EMISIÓN; LO ANTERIOR, SIN PERJUICIO DE LAS FACULTADES DE FISCALIZACIÓN DE QUE DISPONE LA DIRECCIÓN GENERAL. (3)

Art. 6.- LA DECLARACIÓN PARA DESTINAR ADUANERAMENTE LAS MERCANCÍAS, DEBERÁ EFECTUARSE MEDIANTE TRANSMISIÓN ELECTRÓNICA DE LA INFORMACIÓN, CONFORME LOS LINEAMIENTOS Y FORMATOS FÍSICOS Y ELECTRÓNICOS ESTABLECIDOS POR LA DIRECCIÓN GENERAL, A TRAVÉS DEL SISTEMA CONOCIDO COMO TELEDESPACHO, EL CUAL, PARA ASEGURAR LA INTEGRIDAD DE LOS FLUJOS DE INFORMACIÓN, DEBERÁ ESTAR ESTRUCTURADO POR PROCEDIMIENTOS QUE ASEGUREN LA AUTENTICIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y NO REPUDIACIÓN DE LA INFORMACIÓN TRANSMITIDA. EXCEPCIONALMENTE, LA DECLARACIÓN PODRÁ EFECTUARSE POR OTROS MEDIOS LEGALMENTE AUTORIZADOS O POR DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL DICTADAS POR LA DIRECCIÓN GENERAL. (1)

PARA EFECTOS DE ESTA LEY, TELEDESPACHO CONSTITUYE EL CONJUNTO SISTEMATIZADO DE ELEMENTOS TECNOLÓGICOS DE CARÁCTER INFORMÁTICO Y DE COMUNICACIONES QUE PERMITEN, DENTRO DE UN MARCO DE MUTUAS RESPONSABILIDADES Y MEDIANTE LOS PROCEDIMIENTOS AUTORIZADOS, EL INTERCAMBIO POR VÍA ELECTRÓNICA DE INFORMACIÓN DE TRASCENDENCIA TRIBUTARIA ENTRE LA DIRECCIÓN GENERAL Y LOS USUARIOS Y AUXILIARES DEL SERVICIO ADUANERO, BANCOS Y EN GENERAL, LOS OPERADORES E INSTITUCIONES CONTRALORAS DEL COMERCIO EXTERIOR. (1)

LOS DOCUMENTOS CONTENIDOS EN UN SOPORTE MAGNÉTICO, DIGITAL O ELECTRÓNICO PRODUCIRÁN LOS MISMOS EFECTOS JURÍDICOS QUE LOS ESCRITOS EN UN SOPORTE DE PAPEL; EN CONSECUENCIA, LO DISPUESTO EN EL PÁRRAFO ANTERIOR, SERÁ APLICABLE A LA DECLARACIÓN DEL VALOR EN ADUANA Y A CUALQUIER OTRO DOCUMENTO EN FORMATO ELECTRÓNICO QUE CONFORME LA LEGISLACIÓN REQUIERA ADJUNTARSE A LA DECLARACIÓN DE MERCANCÍAS. CUANDO LA LEY REQUIERA QUE LA INFORMACIÓN CONSTE O QUE LA MISMA SE A PRESENTADA Y CONSERVADA O ARCHIVADA EN SU FORMA ORIGINAL, ESE REQUISITO QUEDARÁ SATISFECHO CON UN MENSAJE DE DATOS, SIEMPRE QUE LA INFORMACIÓN CONTENIDA EN ÉSTE SEA ACCESIBLE PARA SU ULTERIOR CONSULTA. (1)

EN AQUELLOS CASOS EN LOS QUE LA DIRECCIÓN GENERAL DE ADUANAS TENGA LA OBLIGACIÓN DE CREAR Y POSEER UN REGISTRO, PODRÁ ADMINISTRARLO Y CONSERVARLO DE MANERA ELECTRÓNICA; ASIMISMO, POTENCIARÁ LA NOTIFICACIÓN DE LOS ACTOS ADMINISTRATIVOS POR MEDIO DE MENSAJE DE DATOS ELECTRÓNICOS. (4)

EN TODO TRÁMITE LEGAL, NO SE DARÁ APLICACIÓN A DISPOSICIÓN ALGUNA QUE SEA ÓBICE PARA LA ADMISIÓN COMO PRUEBA DE UN MENSAJE DE DATOS. (1)

SE PROHÍBE A LOS AUXILIARES DE LA FUNCIÓN PÚBLICA ADUANERA, REVELAR O PERMITIR EL USO A TERCEROS DE SU CLAVE DE ACCESO O FIRMA DIGITAL, INCLUSIVE REVELARLA O PERMITIR EL USO DE LA MISMA A SUS ASISTENTES AUTORIZADOS. (3)

Art. 7.- EL USO DE MEDIOS INFORMÁTICOS Y DE LA VÍA ELECTRÓNICA PARA EL INTERCAMBIO DE INFORMACIÓN, GOZARÁ DE PLENA VALIDEZ PARA LA FORMULACIÓN, TRANSMISIÓN, REGISTRO Y ARCHIVO DE LA DECLARACIÓN DE MERCANCÍAS, DE LA INFORMACIÓN RELACIONADA CON LA MISMA Y DE LOS DOCUMENTOS QUE A ÉSTA DEBAN ADJUNTARSE, ASÍ COMO PARA CERTIFICAR EL PAGO DEL ADEUDO, Y SU UTILIZACIÓN PRODUCIRÁ LOS MISMOS EFECTOS JURÍDICOS QUE PRODUCIRÍA LA ENTREGA DE ESA MISMA INFORMACIÓN EN SOPORTES FÍSICOS.

EN CASO QUE SE DETECTARE UNA DISCONFORMIDAD DE DATOS DE UN MISMO DOCUMENTO, REGISTRADOS EN LOS ARCHIVOS DE LOS BANCOS, USUARIOS O AUXILIARES DEL SERVICIO ADUANERO EN RELACIÓN CON LOS REGISTRADOS Y ARCHIVADOS POR LA ADUANA, SE CONSIDERARÁ COMO CORRECTOS LOS DATOS SOBRE LOS CUALES LA ENTIDAD CERTIFICADORA HUBIERA OTORGADO FÉ PÚBLICA, O EN SU DEFECTO, LOS QUE CONSTEN EN EL DOCUMENTO FÍSICO CUYA INFORMACIÓN SE TRANSMITIÓ, SIEMPRE QUE EL MISMO NO TENGA BORRONES, TACHADURAS O ALTERACIONES. (1)

Art. 8.- A EFECTOS DE GARANTIZAR LA AUTENTICIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN Y DE IMPEDIR SU POSTERIOR REPUDIACIÓN, SE ESTABLECEN SISTEMAS DE CERTIFICACIÓN DE LA INFORMACIÓN TRANSMITIDA, PARA LO CUAL, SE AUTORIZARÁ LA INTERMEDIACIÓN DE EMPRESAS QUE PROVEAN SERVICIOS DE CERTIFICACIÓN DE DICHA INFORMACIÓN, LLAMADAS EN ADELANTE ENTIDADES CERTIFICADORAS. LA AUTORIZACIÓN PARA OPERAR, LA FISCALIZACIÓN Y LA FACULTAD SANCIONATORIA RELACIONADAS CON LAS ENTIDADES CERTIFICADORAS, SERÁ EJERCIDA POR EL MINISTERIO DE HACIENDA, EN TANTO NO SE DICTE UNA LEY QUE REGULE DE MANERA GENERAL TODOS LOS ASPECTOS RELACIONADOS CON EL COMERCIO ELECTRÓNICO, EN CUYO CASO, DICHA POTESTAD CORRESPONDERÁ A LA AUTORIDAD ACREDITANTE O LICENCIANTE DE ENTIDADES CERTIFICADORAS QUE EN LA MISMA SE ESTABLEZCA. A ESTOS EFECTOS, EL MINISTERIO DE HACIENDA TENDRÁ, OTRAS, LAS FACULTADES SIGUIENTES:

a) AUTORIZAR LA OPERACIÓN DE LAS ENTIDADES CERTIFICADORAS EN EL TERRITORIO NACIONAL;

b) VELAR POR EL FUNCIONAMIENTO Y LA EFICIENTE PRESTACIÓN DEL SERVICIO POR PARTE DE LAS ENTIDADES CERTIFICADORAS;

c) REALIZAR VISITAS DE AUDITORÍA A LAS ENTIDADES CERTIFICADORAS;

d) REVOCAR O SUSPENDER LA AUTORIZACIÓN PARA OPERAR COMO ENTIDAD CERTIFICADORA;

e) SOLICITAR LA INFORMACIÓN PERTINENTE PARA EL EJERCICIO DE SUS FUNCIONES DE CONTROL;

f) IMPONER SANCIONES A LAS ENTIDADES CERTIFICADORAS, CUANDO DE CONFORMIDAD CON LA LEY CORRESPONDA;

g) ORDENAR LA REVOCACIÓN DE CERTIFICADOS CUANDO LA ENTIDAD CERTIFICADORA LOS EMITA SIN EL CUMPLIMIENTO DE LAS FORMALIDADES LEGALES;

h) EMITIR CERTIFICADOS EN RELACIÓN CON LAS FIRMAS DIGITALES DE LAS ENTIDADES CERTIFICADORAS; E

i) IMPARTIR INSTRUCCIONES A TRAVÉS DE DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL, SOBRE EL ADECUADO CUMPLIMIENTO DE LAS NORMAS A LAS CUALES DEBEN SUJETARSE LAS ENTIDADES CERTIFICADORAS Y LOS SUSCRIPTORES DE ÉSTAS.

LAS ENTIDADES CERTIFICADORAS, DEBERÁN SER PERSONAS JURÍDICAS QUE ADEMÁS DE ESTAR CAPACITADAS TECNOLÓGICAMENTE PARA PRESTAR SERVICIOS DE GENERACIÓN Y CERTIFICACIÓN DE FIRMA DIGITAL, DEBERÁN CUMPLIR PARA SU AUTORIZACIÓN CON LOS REQUISITOS LEGALES Y REGLAMENTARIOS, QUE AL EFECTO SE ESTABLEZCAN. UNA VEZ AUTORIZADAS PARA OPERAR, DICHAS ENTIDADES ESTARÁN DOTADAS DE LA POTESTAD DE OTORGAR FÉ PÚBLICA RESPECTO A QUE EN UNA FECHA Y HORA ESPECÍFICAS, PERSONAS PERFECTAMENTE INDIVIDUALIZADAS REALIZARON UNA TRANSMISIÓN ELECTRÓNICA DE DATOS EN DETERMINADOS TÉRMINOS. LA INFORMACIÓN ASÍ CERTIFICADA, NO PODRÁ SER NEGADA O REPUDIADA POSTERIORMENTE.

PARA LA EJECUCIÓN DE LAS DISTINTAS ACTUACIONES QUE CONFORMAN EL SISTEMA DE TELEDESPACHO Y PARA EL INTERCAMBIO DE LA INFORMACIÓN EN GENERAL, CADA USUARIO AUTORIZADO, CONTARÁ CON UNA PAREJA DE CLAVES O LLAVES ÚNICAS Y CORRESPONDIENTES ENTRE SÍ, UNA PÚBLICA Y OTRA PRIVADA, DE MANERA TAL QUE AMBAS SE CORRESPONDAN DE MANERA EXCLUSIVA Y EXCLUYENTE, DEBIENDO ADEMÁS LA ENTIDAD CERTIFICADORA, ADMINISTRAR UN SISTEMA DE PUBLICIDAD DE LAS LLAVES PÚBLICAS. LA VINCULACIÓN DE AMBAS LLAVES O CLASES CONSTITUYE LA FIRMA DIGITAL O ELECTRÓNICA, QUE PARA TODOS LOS EFECTOS LEGALES SE CONSTITUYE EN EL SUSTITUTO DIGITAL DE LA FIRMA MANUSCRITA QUE EN EL MARCO DEL INTERCAMBIO ELECTRÓNICO DE DATOS PERMITE AL RECEPTOR DE UN MENSAJE ELECTRÓNICO VERIFICAR CON CERTEZA LA IDENTIDAD PROCLAMADA POR EL TRANSMISOR, IMPIDIENDO A ESTE ÚLTIMO DESCONOCER EN FORMA POSTERIOR LA AUTORÍA DEL MENSAJE. LOS USUARIOS DEL SISTEMA, CONOCIDOS ADEMÁS COMO SUSCRIPTORES, TENDRÁN LA OBLIGACIÓN DE GUARDAR SECRETO ACERCA DE LAS LLAVES PRIVADAS QUE LES HAYAN SIDO ASIGNADAS Y RESPONDERÁN POR LAS CONSECUENCIAS LEGALES QUE SE DERIVEN DE UN USO INDEBIDO DE TALES LLAVES, YA SEA POR PARTE DE ÉL MISMO O DE TERCERAS PERSONAS NO AUTORIZADAS.

LAS ENTIDADES CERTIFICADORAS QUE SEAN AUTORIZADAS PARA OPERAR, EMITIRÁN LOS RESPECTIVOS CERTIFICADOS QUE PERMITAN A LOS USUARIOS DEL SISTEMA UNA INTERACCIÓN SEGURA EN LA RED INFORMÁTICA HABILITADA PARA EL INTERCAMBIO ELECTRÓNICO DE DATOS. EL CERTIFICADO EMITIDO POR UNA ENTIDAD CERTIFICADORA DEBERÁ SER RECONOCIDO POR LAS DEMÁS ENTIDADES CERTIFICADORAS AUTORIZADAS. (1)

SE PROHÍBE A LOS AUXILIARES DE LA FUNCIÓN PÚBLICA ADUANERA, REVELAR O PERMITIR EL USO A TERCEROS DE SU CLAVE DE ACCESO O FIRMA DIGITAL, INCLUSIVE REVELARLA O PERMITIR EL USO DE LA MISMA A SUS ASISTENTES AUTORIZADOS. (3)

Art. 8-A.- LAS ENTIDADES CERTIFICADORAS AUTORIZADAS TENDRÁN LAS FUNCIONES

SIGUIENTES:

a) EJERCER LA POTESTAD JURÍDICA DE OTORGAR FÉ PÚBLICA EN EL MARCO DEL INTERCAMBIO ELECTRÓNICO DE DATOS, RESPECTO DE LA PERTENENCIA DE LAS FIRMAS DIGITALES A PERSONAS NATURALES O JURÍDICAS Y DE LOS TÉRMINOS EN QUE SE HA GENERADO Y TRANSMITIDO UN MENSAJE DE DATOS;

b) GENERAR EL PAR DE LLAVES PRIVADA Y PÚBLICA, A SOLICITUD EXPRESA, VIRTUALMENTE O POR ESCRITO, DE UNA PERSONA NATURAL O JURÍDICA;

c) ASIGNAR LAS LLAVES PÚBLICAS A LOS SUSCRITOS O A LAS PERSONAS NATURALES O JURÍDICAS QUE ASÍ LO SOLICITEN, VERIFICANDO EL CUMPLIMIENTO DE LOS REQUISITOS QUE AL EFECTO SE ESTABLEZCAN Y DETERMINANDO FEHACIENTEMENTE LA IDENTIDAD Y LA CAPACIDAD DE OBRAR DE LAS PERSONAS NATURALES Y LA PERSONERÍA JURÍDICA DE LOS REPRESENTANTES LEGALES DE LAS PERSONAS JURÍDICAS;

d) EXPEDIR O EMITIR LOS CERTIFICADOS RESPECTIVOS, ESTO ES, LOS DOCUMENTOS ELECTRÓNICOS QUE, AÑADIDOS A LA LLAVE PÚBLICA COMO DATOS E INFORMACIÓN CARACTERÍSTICAS DEL FIRMANTE, ACREDITAN O RESPALDAN LA VIGENCIA Y LA CORRESPONDENCIA ENTRE UNA CLAVE PÚBLICA Y LA PERSONA QUE ES TITULAR DE DICHA LLAVE, UTILIZANDO SISTEMAS QUE GARANTICEN LA SEGURIDAD TÉCNICA Y CRIPTOGRÁFICA DE LOS PROCESOS DE CERTIFICACIÓN. PARA ESTOS EFECTOS, LA ENTIDAD CERTIFICADORA PODRÁ PUBLICAR EL CERTIFICADO EN SU SITIO WEB DE INTERNET, OTORGARLO DIRECTAMENTE O ENVIARLO A LOS SISTEMAS DEL SUSCRIPTOR DE LA LLAVE PÚBLICA, O ENTREGARLO SIN COSTO A CUALQUIERA QUE LO SOLICITE;

e) LLEVAR UN REGISTRO MAGNÉTICO O DIRECTORIO PÚBLICO EN LÍNEA, TANTO DE LAS LLAVES PÚBLICAS COMO DE LOS CERTIFICADOS O DOCUMENTOS ELECTRÓNICOS QUE ACREDITEN O RESPALDEN LA CORRESPONDENCIA ENTRE DICHA CLAVE PÚBLICA Y LA PERSONA QUE SEA SU TITULAR;

f) TOMAR MEDIDAS TÉCNICAS Y ADMINISTRATIVAS TENDIENTES A EVITAR LA FALSIFICACIÓN DE LLAVES PÚBLICAS Y CERTIFICADOS; Y,

g) LAS DEMÁS QUE OTRAS DISPOSICIONES LEGALES O REGLAMENTARIAS LES OTORGUEN.

EN TODO CASO, LAS ENTIDADES CERTIFICADORAS DEBERÁN PREVIAMENTE A LA ASIGNACIÓN DE LLAVES A LOS USUARIOS DE LOS SERVICIOS ADUANEROS, CORROBORAR QUE LOS MISMOS HAN SIDO AUTORIZADOS POR LA DIRECCIÓN GENERAL PARA ACTUAR POR SI MISMOS ANTE EL SERVICIO DE ADUANAS DE LA REPÚBLICA, EN TÉRMINOS PREVISTOS POR EL Art. 9 DE ESTA LEY. (1)

Art. 8-B.- SE ESTABLECE LA OBLIGACIÓN DE SECRETO Y RESERVA RESPECTO A LOS DATOS PERSONALES O NOMINATIVOS DE QUIENES FIRMEN Y SEAN CERTIFICADOS DIGITALMENTE, QUE ARCHIVEN O ALMACENEN LAS ENTIDADES CERTIFICADORAS EN BASES DE DATOS QUE PARA TODOS LOS EFECTOS LEGALES SERÁN CONSIDERADAS DE ACCESO PRIVADO, CON EL OBJETO DE ASEGURAR LA CONFIDENCIALIDAD DE LA INFORMACIÓN Y EL RESPETO Y LA PROTECCIÓN DE LA PRIVACIDAD DE

LAS PERSONAS, SALVO QUE LA FISCALÍA GENERAL DE LA REPÚBLICA O UN TRIBUNAL COMPETENTE REQUIERA EL CONOCIMIENTO DE DICHOS ANTECEDENTES POR MOTIVOS FUNDADOS. EN NINGÚN CASO, DICHOS DATOS PERSONALES PODRÁN SER CRUZADOS, PERFILADOS O UTILIZADOS PARA OTROS FINES QUE LOS REGULADOS POR ESTA LEY, SALVO QUE EL TITULAR DE LOS DATOS CONSIENTA EXPRESAMENTE Y POR ESCRITO EN SU USO PARA UNA FINALIDAD DISTINTA DE AQUELLA CON LA CUAL FUERON RECOLECTADOS, PROCESADOS Y REGISTRADOS O ALMACENADOS. (1)

NO OBSTANTE LO ANTERIOR, LA DIRECCIÓN GENERAL PODRÁ PUBLICAR POR CUALQUIER MEDIO QUE ESTIME CONVENIENTE, LAS DECLARACIONES Y ESTADÍSTICAS DE IMPORTACIÓN O EXPORTACIÓN, RESERVÁNDOSE ÚNICAMENTE EL NOMBRE Y DEMÁS DATOS PERSONALES DEL DECLARANTE. (1)

LA DIRECCIÓN GENERAL DEBERÁ PUBLICAR POR LOS MEDIOS QUE ESTIME CONVENIENTES LA LISTA DE LOS AUXILIARES DE LA FUNCIÓN PÚBLICA ADUANERA AUTORIZADOS, SUSPENDIDOS O INHABILITADOS, ASÍ COMO LAS DIRECCIONES, TELÉFONOS, CORREOS ELECTRÓNICOS U OTROS DATOS DEL LUGAR EN EL QUE EJERZAN SUS NEGOCIOS, A EFECTO DE PERMITIRLES A LOS USUARIOS CONTACTARLOS. ASIMISMO, LA AUTORIDAD ADUANERA PODRÁ INFORMAR POR CUALQUIER MEDIO, EL LISTADO DE LOS AUXILIARES DE LA FUNCIÓN PÚBLICA ADUANERA, CALIFICADOS DE ACUERDO AL HISTORIAL DE OPERACIONES EN LAS QUE HUBIERAN PARTICIPADO Y EL NIVEL DE RIESGO QUE POSEAN EN EL SISTEMA. (4)

Art. 8-C.- LAS ENTIDADES CERTIFICADORAS TENDRÁN ADEMÁS, ENTRE OTROS, LOS SIGUIENTES DEBERES:

a) EMITIR CERTIFICADOS CONFORME A LO SOLICITADO O ACORDADO CON EL SUSCRIPTOR;

b) IMPLEMENTAR LOS SISTEMAS DE SEGURIDAD PARA GARANTIZAR LA EMISIÓN Y CREACIÓN DE FIRMAS DIGITALES, LA CONSERVACIÓN Y ARCHIVO DE CERTIFICADOS Y DOCUMENTOS EN SOPORTE DE MENSAJE DE DATOS;

c) GARANTIZAR LA PROTECCIÓN, CONFIDENCIALIDAD Y DEBIDO USO DE LA INFORMACIÓN SUMINISTRADA POR EL SUSCRIPTOR;

d) RENDIR A FAVOR DEL FISCO UNA GARANTÍA GLOBAL, BANCARIA O DE COMPAÑÍA DE SEGUROS, POR EL MONTO QUE SE LE FIJE POR EL MINISTERIO DE HACIENDA;

e) GARANTIZAR LA PRESTACIÓN PERMANENTE DEL SERVICIO DE ENTIDAD DE CERTIFICACIÓN;

f) ATENDER OPORTUNAMENTE LAS SOLICITUDES Y RECLAMACIONES HECHAS POR LOS SUSCRIPTORES;

g) EFECTUAR LOS AVISOS Y PUBLICACIONES CONFORME A LO DISPUESTO POR ESTA LEY;

h) SUMINISTRAR LA INFORMACIÓN QUE LE REQUIERAN LAS ENTIDADES ADMINISTRATIVAS O JUDICIALES COMPETENTES EN RELACIÓN CON LAS FIRMAS DIGITALES Y CERTIFICADOS EMITIDOS Y EN GENERAL SOBRE CUALQUIER MENSAJE DE DATOS QUE SE ENCUENTRE BAJO SU CUSTODIA Y ADMINISTRACIÓN;

i) PERMITIR Y FACILITAR LA REALIZACIÓN DE LAS AUDITORÍAS POR PARTE DEL MINISTERIO DE HACIENDA O DE LA ENTIDAD A QUIEN CORRESPONDA DICHA FUNCIÓN DE ACUERDO CON LAS NORMAS QUE A FUTURO REGULEN EL COMERCIO ELECTRÓNICO;

j) ELABORAR LOS REGLAMENTOS QUE DEFINAN SUS RELACIONES CON EL SUSCRIPTOR Y LA FORMA DE PRESTACIÓN DEL SERVICIO; Y,

k) LLEVAR UN REGISTRO DE LOS CERTIFICADOS EMITIDOS.

Art. 8-D.- SON DEBERES DE LOS SUSCRIPTORES:

a) GENERAR LA FIRMA ELECTRÓNICA ASIGNADA POR LA EMPRESA CERTIFICADORA, UTILIZANDO UN MÉTODO AUTORIZADO POR ÉSTA;

b) SUMINISTRAR LA INFORMACIÓN QUE REQUIERA LA ENTIDAD CERTIFICADORA;

c) MANTENER EL CONTROL DE LA FIRMA DIGITAL, ESPECIALMENTE DE SU CLAVE O LLAVE PRIVADA;

d) SOLICITAR OPORTUNAMENTE LA REVOCACIÓN DE LOS CERTIFICADOS; Y,

e) LOS DEMÁS QUE LES IMPONGAN LAS LEYES O REGLAMENTOS DE LA REPÚBLICA.

LOS SUSCRIPTORES SERÁN RESPONSABLES POR LA FALSEDAD, ERROR U OMISIÓN EN LA INFORMACIÓN SUMINISTRADA A LA ENTIDAD CERTIFICADORA Y POR EL INCUMPLIMIENTO DE SUS DEBERES COMO SUSCRIPTOR, ASÍ COMO DEL MAL USO, ABUSO O DAÑO QUE EN CUALQUIER FORMA CAUSEN A LOS SISTEMAS INFORMÁTICOS UTILIZADOS POR LA DIRECCIÓN GENERAL EN EL MARCO DEL INTERCAMBIO ELECTRÓNICO DE INFORMACIÓN. (1)

Art. 8-E.- EL MINISTERIO DE HACIENDA, DE ACUERDO CON EL DEBIDO PROCESO Y EL DERECHO DE DEFENSA, PODRÁ IMPONER SEGÚN LA NATURALEZA Y LA GRAVEDAD DE LA FALTA, LAS SIGUIENTES SANCIONES A LAS ENTIDADES CERTIFICADORAS:

a) AMONESTACIÓN;

b) SUSPENDER LA AUTORIZACIÓN PARA OPERAR DE LA ENTIDAD CERTIFICADORA INFRACTORA, HASTA POR EL PLAZO DE SEIS MESES, CUANDO SE COMPRUEBE QUE HA AUTORIZADO, EJECUTADO O TOLERADO CONDUCTAS VIOLATORIAS DE LA LEY, QUE PUDIEREN PROVOCAR UN PERJUICIO FISCAL O DAÑO A LOS SISTEMAS INFORMÁTICOS DE LA DIRECCIÓN GENERAL, SIN PERJUICIO DE LA RESPONSABILIDAD PENAL QUE PUEDA CORRESPONDER A LAS PERSONAS NATURALES QUE HUBIERAN ACORDADO, AUTORIZADO, PERMITIDO O EJECUTADO TALES ACTOS;

c) REVOCAR DEFINITIVAMENTE LA AUTORIZACIÓN PARA OPERAR, CUANDO LA ENTIDAD CERTIFICADORA SE HUBIERA HECHO ACREEDORA A UNA SEGUNDA SUSPENSIÓN EN

EL LAPSO DE UN MISMO AÑO, CONTADO DESDE LA FECHA DE LA COMISIÓN DE LOS HECHOS QUE MOTIVARON LA PRIMERA SUSPENSIÓN.

PARA LA APLICACIÓN DE LAS SANCIONES ESTABLECIDAS EN LOS LITERALES b) Y c), DEL INCISO ANTERIOR, SE UTILIZARÁ EL PROCEDIMIENTO ESTABLECIDO POR EL ART. 17 DE LA PRESENTE LEY. (1)

Art. 9.- Los datos y registros recibidos y archivados en el sistema informático constituirán plena prueba de que el usuario del servicio aduanero realizó los actos que le corresponden y que el contenido de esos actos y registros fue suministrado por éste, haciendo uso de su clave de acceso confidencial.

Los empleados, funcionarios o autoridades que intervengan en la operación del sistema, serán responsables civil, administrativa y penalmente de sus actos y de los datos que suministren.

Cualquier información transmitida electrónicamente por medio de un sistema informático autorizado por la Dirección General será admisible en los procedimientos administrativos o judiciales como evidencia de la transmisión y del contenido de esa información.

PARA GARANTIZAR EL ACCESO GENERALIZADO AL TELEDESPACHO, LA PARTICIPACIÓN DE LOS AGENTES DE ADUANA O AGENTES ADUANEROS EN LA GESTIÓN DE LOS TRÁMITES ADUANEROS QUE TENGAN POR OBJETO MERCANCÍAS DESTINADAS A SU PROCESAMIENTO O COMERCIALIZACIÓN, SERÁ OPTATIVA PARA EL USUARIO, SIEMPRE QUE ÉSTE SEA UNA PERSONA JURÍDICA, QUIEN PODRÁ OBTENER UNA AUTORIZACIÓN DE LA DIRECCIÓN GENERAL PARA EFECTUAR POR SÍ MISMA SUS DECLARACIONES ADUANERAS, PARA LO CUAL DEBERÁ OTORGAR PODER DE REPRESENTACIÓN EN ESCRITURA PÚBLICA A FAVOR DE CUALQUIERA DE SUS EMPLEADOS QUE LA REPRESENTARÁ EN CALIDAD DE APODERADO ESPECIAL ADUANERO ANTE LAS ADUANAS DE LA REPÚBLICA, QUIENES SERÁN SOMETIDOS A UN EXAMEN DE SUFICIENCIA QUE VERSARÁ SOBRE MATERIAS ADUANERAS Y QUE PODRÁ COMPRENDER ADEMÁS PRUEBAS PSICOTÉCNICAS, DEBIENDO CUMPLIR CON LOS REQUISITOS QUE LA NORMATIVA ADUANERA O LA DIRECCIÓN GENERAL ESTABLEZCAN A TRAVÉS DE DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL, QUE DEBERÁN SER DEBIDAMENTE PUBLICADAS EN EL DIARIO OFICIAL.

UNA VEZ AUTORIZADO EL APODERADO ESPECIAL ADUANERO, LA PERSONA JURÍDICA PODERDANTE DEBERÁ RENDIR UNA FIANZA QUE SERÁ FIJADA POR LA DIRECCIÓN GENERAL, LA CUAL SERVIRÁ PARA RESPONDER POR LOS DERECHOS E IMPUESTOS, MULTAS Y DEMÁS RECARGOS QUE PUEDAN GENERARSE EN EL MARCO DE SUS ACTUACIONES ANTE LAS AUTORIDADES ADUANERAS.

EL APODERADO ESPECIAL ADUANERO QUEDARÁ SUJETO, EN VIRTUD DE SU INTERVENCIÓN, A LAS MISMAS DISPOSICIONES LEGALES QUE REGULAN LO RELATIVO A LA SUSPENSIÓN Y REVOCATORIA DE LA AUTORIZACIÓN PARA OPERAR DE LOS AGENTES DE ADUANA. (1)

Art. 10.- Las instituciones públicas y entidades privadas relacionadas con el servicio de aduanas, deberán transmitir electrónicamente a las autoridades aduaneras competentes los permisos, certificados, licencias, autorizaciones y demás información inherente al tráfico de mercancías o a la comprobación del pago de las obligaciones tributarias aduaneras, de conformidad a los procedimientos acordados entre tales entidades y la Dirección General.

Por su parte, la autoridad aduanera deberá proporcionar a estas instituciones o entidades la

información atinente a su competencia sobre las operaciones aduaneras de acuerdo a los procedimientos que al efecto se hubieran convenido.

Art. 11.- TODA MERCANCÍA PARA SER DESTINADA A UN RÉGIMEN ADUANERO, DEBERÁ ESTAR AMPARADA EN UNA DECLARACIÓN. LA DECLARACIÓN DE MERCANCÍAS SE CONSIDERARÁ ACEPTADA CUANDO SE REGISTRE EN EL SISTEMA INFORMÁTICO AUTORIZADO POR LA DIRECCIÓN GENERAL. LA REALIZACIÓN DE DICHO ACTO NO IMPLICA AVALAR EL CONTENIDO DE LA DECLARACIÓN, NI LIMITA LAS FACULTADES DE COMPROBACIÓN, FISCALIZACIÓN Y LIQUIDACIÓN A POSTERIORI DE LA AUTORIDAD ADUANERA.

EN EL CASO DE TRANSFERENCIA O VENTA DE MERCANCÍAS IMPORTADAS BAJO LOS REGÍMENES ADUANEROS SUSPENSIVOS Y LIBERATORIOS, LA DECLARACIÓN DE IMPORTACIÓN DEFINITIVA MEDIANTE LA CUAL SE CANCELA EL RÉGIMEN, DEBERÁ PRESENTARSE Y PAGARSE PREVIO A LA TRANSFERENCIA O VENTA REALIZADA. EN EL CASO DE LAS SANCIONES Y LIQUIDACIONES DE OFICIO PRACTICADAS POR LA AUTORIDAD ADUANERA COMPETENTE, EL PAGO DE LOS TRIBUTOS Y MULTAS DEBERÁ EFECTUARSE DENTRO DEL PLAZO DE LOS OCHO DÍAS HÁBILES SIGUIENTES A LA NOTIFICACIÓN DE LA RESOLUCIÓN DEFINITIVA.

LAS DECLARACIONES QUE HAYAN SIDO TELEDESPACHADAS Y SE ENCUENTREN REGISTRADAS EN EL SISTEMA INFORMÁTICO DE LA DIRECCIÓN GENERAL Y QUE NO SE PRESENTEN DENTRO DEL PLAZO DE DIEZ DÍAS, SERÁN ANULADAS DE OFICIO DEL SISTEMA POR LA AUTORIDAD ADUANERA COMPETENTE; EN EL CASO DE LAS DECLARACIONES DE MERCANCÍAS QUE SE ENCUENTREN EN LA MISMA CONDICIÓN ANTERIOR, Y QUE HAYAN SIDO PAGADOS LOS TRIBUTOS, SERÁN ANULADAS DEL SISTEMA DE ADUANAS DENTRO DEL PLAZO DE SESENTA DÍAS SIGUIENTES A SU REGISTRO, EN ESTE ÚLTIMO CASO EL INTERESADO PODRÁ PRESENTAR LA SOLICITUD DE DEVOLUCIÓN DE IMPUESTOS ANTE LA AUTORIDAD ADUANERA CORRESPONDIENTE. (3)

Art. 11-A.- SE ENTENDERÁ POR PROCEDIMIENTO SIMPLIFICADO PARA EL RETIRO DE MERCANCÍAS, EL RETIRO DE ÉSTAS DE LOS RECINTOS ADUANEROS, SIN LA DETERMINACIÓN FINAL DE LOS ARANCELES ADUANEROS, IMPUESTOS Y CARGOS APLICABLES A LA IMPORTACIÓN, DENTRO DE LAS CUARENTA Y OCHO HORAS POSTERIORES A LA LLEGADA DE LA MERCANCÍA. DICHO PROCEDIMIENTO SERÁ AUTORIZADO MEDIANTE RESOLUCIÓN RAZONADA, POR UN PLAZO DE UN AÑO, PRORROGABLE A CRITERIO DE LA DIRECCIÓN GENERAL, SIN PERJUICIO DE LAS FACULTADES DE FISCALIZACIÓN QUE ÉSTA DISPONE DE CONFORMIDAD A LA LEY. EL PROCEDIMIENTO SIMPLIFICADO SERÁ APLICABLE EN AQUELLOS CASOS ESTABLECIDOS EN ACUERDOS, CONVENIOS, TRATADOS Y OTROS INSTRUMENTOS EN MATERIA COMERCIAL. EL PROCEDIMIENTO SIMPLIFICADO TAMBIÉN PODRÁ SER APLICADO CUANDO ASÍ SE ACUERDE EN UN CONVENIO SUSCRITO ENTRE LA DIRECCIÓN GENERAL Y UN OPERADOR DE ENVÍOS DE ENTREGA RÁPIDA O COURIER. LA DIRECCIÓN GENERAL ESTABLECERÁ LOS REQUISITOS PARA CALIFICAR A UN OPERADOR DE ENVÍOS DE ENTREGA RÁPIDA O COURIER.

EN EL CASO DEL PROCEDIMIENTO SIMPLIFICADO, EL PAGO DE LOS TRIBUTOS DETERMINADOS EN LA DECLARACIÓN DE MERCANCÍAS DE IMPORTACIÓN DEBERÁ EFECTUARSE DENTRO DEL PLAZO DE OCHO DÍAS HÁBILES SIGUIENTES A LA PRESENTACIÓN DE LA MISMA ANTE LA AUTORIDAD ADUANERA COMPETENTE, DEBIENDO CUMPLIR CON LOS REQUISITOS SIGUIENTES :

a) PRESENTAR ANTE LA DIRECCIÓN GENERAL, UNA SOLICITUD DE AUTORIZACIÓN PARA EL PROCEDIMIENTO SIMPLIFICADO PARA EL RETIRO DE MERCANCÍAS, LA CUAL DEBERÁ

CONTENER ENTRE OTROS, LA INFORMACIÓN GENERAL DEL SOLICITANTE, UBICACIÓN DE LA EMPRESA, CAPACIDAD DE ALMACENAJE, ESTIMACIÓN DEL MONTO Y TIPO DE LAS MERCANCÍAS QUE INGRESARÁN ANUALMENTE;

b) EN EL CASO DE LAS PERSONAS JURÍDICAS, DEBERÁN PRESENTAR LOS DATOS RELATIVOS A SU PERSONERÍA JURÍDICA;

c) JUSTIFICACIÓN DE LA OPERACIÓN, DE CONFORMIDAD A LOS VOLÚMENES EN NÚMERO Y RECAUDACIÓN TRIBUTARIA, ASÍ COMO A LA CLASE DE MERCANCÍAS, RÉGIMEN ADUANERO Y DEMÁS ELEMENTOS; PARA TALES EFECTOS DEBERÁ LLENAR LOS FORMULARIOS QUE ESTABLEZCA LA DIRECCIÓN GENERAL;

d) QUE NO TENGA DEUDAS PENDIENTES CON EL FISCO;

e) QUE NO HAYA SIDO SANCIONADO EN FORMA REINCIDENTE, EN LOS ÚLTIMOS SEIS MESES POR INFRACCIONES ADUANERAS;

f) CONTAR CON LAS INSTALACIONES ADECUADAS PARA LA RECEPCIÓN, MANEJO Y ALMACENAMIENTO DE LAS MERCANCÍAS;

g) RENDIR ANTE EL FISCO UNA GARANTÍA SUFICIENTE EN FORMA DE DEPÓSITO O FIANZA, POR EL MONTO ESTIMADO DE SUS OPERACIONES QUE CUBRA EL PAGO DEFINITIVO DE LOS DERECHOS ADUANEROS, IMPUESTOS Y CARGOS RELACIONADOS CON LA IMPORTACIÓN, LA CUAL SERÁ AUTORIZADA POR LA DIRECCIÓN GENERAL, POR UN PLAZO DE UN AÑO, Y PODRÁ SER MEDIANTE FIANZA O DEPÓSITO EN CUENTA CORRIENTE A FAVOR DE LA DIRECCIÓN GENERAL DE TESORERÍA;

h) PRESENTAR LAS RESPECTIVAS SOLVENCIAS DE PAGO DEL INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL Y DE LAS DIFERENTES ADMINISTRADORAS DE FONDOS DE PENSIONES, DE LAS COTIZACIONES CORRESPONDIENTES A LOS TREINTA DÍAS ANTERIORES, A AQUEL EN EL QUE SE PRESENTE LA SOLICITUD;

i) CUMPLIR CON LOS DEMÁS REQUISITOS Y OBLIGACIONES NO TRIBUTARIAS ESTABLECIDAS EN LA LEY;

j) CUMPLIR CON OTROS REQUISITOS QUE LA DIRECCIÓN GENERAL DETERMINE MEDIANTE DISPOSICIONES ADMINISTRATIVAS.

AL MOMENTO DEL INGRESO DE LAS MERCANCÍAS AL TERRITORIO ADUANERO NACIONAL, AMPARADAS BAJO LA MODALIDAD DEL PROCEDIMIENTO SIMPLIFICADO, EL SUJETO PASIVO DEBERÁ CUMPLIR CON LOS REQUISITOS SIGUIENTES:

a) TRANSMISIÓN Y PRESENTACIÓN DEL MANIFIESTO DE CARGA; Y

b) TRANSMITIR ELECTRÓNICAMENTE LA DECLARACIÓN DE MERCANCÍAS Y PRESENTARLA JUNTO CON LA DOCUMENTACIÓN DE RESPALDO ANTE LA AUTORIDAD ADUANERA

COMPETENTE AL MOMENTO DEL INGRESO DE LAS MERCANCÍAS, DEBIENDO EFECTUARSE EL PAGO DE LOS TRIBUTOS Y DEMÁS CARGOS APLICABLES A LA IMPORTACIÓN, DENTRO DE LOS OCHO DÍAS HÁBILES SIGUIENTES A DICHO ACTO.

LA DIRECCIÓN GENERAL PODRÁ REVOCAR LA AUTORIZACIÓN CORRESPONDIENTE, ANTE EL INCUMPLIMIENTO POR PARTE DEL SUJETO PASIVO DE LAS CONDICIONES Y REQUISITOS ESTABLECIDOS EN LA RESOLUCIÓN DE AUTORIZACIÓN O EN EL CONVENIO CORRESPONDIENTE, LO CUAL DARÁ LUGAR A QUE SE HAGA EFECTIVA LA GARANTÍA O FIANZA RENDIDA A FAVOR DEL FISCO Y DARÁ LUGAR A LA SUSPENSIÓN DE SUS OPERACIONES ADUANERAS HASTA QUE SE VERIFIQUE EL PAGO CORRESPONDIENTE.

TRATÁNDOSE DE UN CONVENIO ENTRE LA DIRECCIÓN GENERAL Y UN OPERADOR DE ENVÍOS DE ENTREGA RÁPIDA O COURIER, LAS CONDICIONES Y EL PLAZO DE VIGENCIA SERÁN LOS ESTABLECIDOS EN EL CONVENIO Y TOMARÁN EN CUENTA LAS DIRECTRICES PARA EL LEVANTE INMEDIATO DE LOS ENVÍOS POR PARTE DE LA ADUANA, ESTABLECIDAS POR LA ORGANIZACIÓN MUNDIAL DE ADUANAS. ESTOS CONVENIOS DEBERÁN INCLUIR:

a) RENDIR ANTE EL FISCO UNA GARANTÍA SUFICIENTE EN FORMA DE DEPÓSITO O FIANZA, POR EL MONTO ESTIMADO DE SUS OPERACIONES QUE CUBRA EL PAGO DEFINITIVO DE LOS DERECHOS ADUANEROS, IMPUESTOS Y CARGOS RELACIONADOS CON LA IMPORTACIÓN, LA CUAL SERÁ AUTORIZADA POR LA DIRECCIÓN GENERAL, POR UN PLAZO DE UN AÑO, Y PODRÁ SER MEDIANTE FIANZA O DEPÓSITO EN CUENTA CORRIENTE A FAVOR DE LA DIRECCIÓN GENERAL DE TESORERÍA;

b) PARA ENVÍOS CUYO VALOR FOB SEA INFERIOR A DOSCIENTOS DÓLARES (US$ 200.00), EL RETIRO DE LAS MERCANCÍAS DE LOS RECINTOS FISCALES SE AUTORIZARÁ CON LA PRESENTACIÓN DE LA GUÍA AÉREA Y LA FACTURA RESPECTIVA, PRESENTADO POR EL OPERADOR DE ENVÍOS DE ENTREGA RÁPIDA O COURIER; EN CASO DE NO TENER FACTURA SERÁ SOMETIDO A LOS VALORES DE REFERENCIA EMITIDOS POR EL DEPARTAMENTO DE VALORACIÓN DE LA DIRECCIÓN GENERAL;

c) PARA ENVÍOS CUYO VALOR FOB SEA SUPERIOR A DOSCIENTOS DÓLARES (US$ 200.00) Y NO MAYOR A TRES MIL DÓLARES (US$ 3,000.00), EL RETIRO DE LAS MERCANCÍAS DE LOS RECINTOS FISCALES SE AUTORIZARÁ CON LA PRESENTACIÓN DE LA DECLARACIÓN DE MERCANCÍAS. LA DECLARACIÓN DE MERCANCÍAS PODRÁ SER CONSOLIDADA SIEMPRE QUE EL TOTAL DE LA SUMA DEL VALOR FOB DE CADA UNA DE LAS MERCANCÍAS NO SUPERE LOS TRES MIL DÓLARES (US$ 3,000.00) POR EL OPERADOR DE ENVÍOS DE ENTREGA RÁPIDA O COURIER. (3)

Art. 12.- La declaración de mercancías autoliquidada será sometida a un proceso selectivo y aleatorio que determine si corresponde efectuar la verificación inmediata de lo declarado. Dicha verificación no limita las facultades de fiscalización posterior de la autoridad aduanera.

LOS SERVICIOS ADUANEROS PODRÁN UTILIZAR EQUIPOS DE INSPECCIÓN NO INTRUSIVA O INVASIVA QUE LES PERMITA REALIZAR INSPECCIONES CUANDO SEA NECESARIO Y DE CONFORMIDAD CON LOS RESULTADOS DEL ANÁLISIS DE RIESGO, EN BASE A LOS PARÁMETROS ESTABLECIDOS POR LA DIRECCIÓN GENERAL DE ADUANAS O A PETICIÓN DE LAS ENTIDADES ENCARGADAS DE EJERCER

CONTROLES, CON EL FIN DE FACILITAR LA INSPECCIÓN DE LA CARGA, DE LOS CONTENEDORES U OTROS MEDIOS DE TRANSPORTE, SIN INTERRUMPIR EL FLUJO DEL COMERCIO LEGÍTIMO. (4)

LA PRESTACIÓN DE SERVICIOS DE INSPECCIÓN NO INTRUSIVA A CARGO DE LA AUTORIDAD ADUANERA, CON INFRAESTRUCTURA TECNOLÓGICA PROPIA O DE TERCEROS AUTORIZADOS, SE CONSIDERARÁ INICIADA DESDE EL ANÁLISIS DE RIESGO A QUE SON SOMETIDAS LAS OPERACIONES Y CONSISTIRÁ, ENTRE OTROS ASPECTOS, EN VERIFICACIONES SOBRE LA NATURALEZA, ESTADO, PESO, CANTIDAD Y DEMÁS CARACTERÍSTICAS DE LAS MERCANCÍAS QUE SE COLOQUEN A SU DISPOSICIÓN, DE ACUERDO AL ANÁLISIS DE RIESGO PREVIAMENTE REALIZADO. DE ESTABLECERSE INDICIOS DE MERCANCÍAS NO DECLARADAS O DE CUALQUIER OTRO INCUMPLIMIENTO DE DISPOSICIONES LEGALES, SE PROCEDERÁ A LA INSPECCIÓN FÍSICA POR PARTE DE LA AUTORIDAD ADUANERA, LA QUE A SU VEZ, PODRÁ AUXILIARSE Y COORDINARSE CON OTRAS AUTORIDADES QUE TENGAN COMPETENCIA EN EL CONTROL DE LAS MERCANCÍAS. (4)

LA VERIFICACIÓN POR SISTEMAS NO INTRUSIVOS, NO LIMITA LAS FACULTADES DE VERIFICACIÓN INMEDIATA O DE FISCALIZACIÓN A POSTERIORI QUE PUEDA REALIZAR LA AUTORIDAD ADUANERA CORRESPONDIENTE, COMO RESULTADO DE LOS ANÁLISIS DE GESTIÓN DE RIESGO Y EL EJERCICIO DE LA POTESTAD ADUANERA. (4)

EL SERVICIO ADUANERO ESTABLECERÁ LOS LUGARES EN LOS QUE PODRÁ PRACTICARSE LA INSPECCIÓN NO INTRUSIVA, PUDIENDO REALIZARSE FUERA DE LOS RECINTOS ADUANEROS EN PUNTOS ESTRATÉGICOS PARA LA VERIFICACIÓN DE CUMPLIMIENTOS DE RUTAS O COMPROBACIÓN DE LA INTEGRIDAD DE LAS MERCANCÍAS QUE SE ENCUENTREN SOMETIDAS A OPERACIONES DE COMERCIO EXTERIOR, ENTENDIÉNDOSE COMO TALES, IMPORTACIONES, EXPORTACIONES, TRÁNSITOS, ENTRE OTRAS. LAS OPERACIONES REALIZADAS FUERA DE LOS RECINTOS ADUANEROS PODRÁN SER COORDINADAS CON LA POLICÍA NACIONAL CIVIL Y OTRAS INSTITUCIONES ENCARGADAS DEL CONTROL DE LAS OPERACIONES DE COMERCIO EXTERIOR. (4)

Art. 12-A.- EN AQUELLOS PROCESOS DE INSPECCIÓN NO INTRUSIVA QUE PUEDA ADVERTIRSE QUE EXISTE EL COMETIMIENTO DE UN ILÍCITO, SE DEBERÁN CERTIFICAR LAS IMÁGENES QUE REPRODUZCA EL SISTEMA Y REMITIRSE A LAS AUTORIDADES COMPETENTES.

LAS REFERIDAS CERTIFICACIONES HARÁN PLENA PRUEBA EN EL PROCESO PENAL CORRESPONDIENTE; EN TODO CASO, LAS AUTORIDADES QUE CONOZCAN DEL CITADO PROCESO PENAL PODRÁN REQUERIR, EN CASO DE CONSIDERARLO NECESARIO, UN DICTAMEN ACLARATORIO SOBRE LA LECTURA DE LOS RESULTADOS, SIN PERJUICIO DE LAS RESPONSABILIDADES TRIBUTARIAS Y ADUANERAS QUE DEBERÁN SER DETERMINADAS POR LA AUTORIDAD ADUANERA COMPETENTE.

EL MISMO VALOR PROBATORIO TENDRÁN LAS IMÁGENES REPRODUCIDAS DEL SISTEMA DE INSPECCIÓN NO INTRUSIVA EN LOS PROCESOS ADMINISTRATIVOS CORRESPONDIENTES.

LA DECLARATORIA DE SOBRESEIMIENTO DEFINITIVO O CONDENA EN EL PROCESO PENAL, NO INHIBIRÁN A LA AUTORIDAD ADUANERA PARA DETERMINAR LA RESPONSABILIDAD ADMINISTRATIVA O TRIBUTARIA A QUE DIERAN LUGAR LAS ACCIONES U OMISIONES COMETIDAS CONFORME AL PRESENTE ARTÍCULO.

EN EL CASO QUE DURANTE EL PROCEDIMIENTO DE VERIFICACIÓN NO INTRUSIVA O EN

CUALQUIER MOMENTO PREVIO AL LEVANTE DE LA MERCANCÍA SE DETERMINARE LA EXISTENCIA DE MERCANCÍA QUE DEBA SER DESTRUIDA POR CUALQUIER CIRCUNSTANCIA, LOS GASTOS DE DICHO PROCESO DEBERÁN SER ASUMIDOS POR EL DECLARANTE O SU REPRESENTANTE, PUDIENDO LA AUTORIDAD ADUANERA HACER EFECTIVA LA GARANTÍA DE OPERACIÓN, EN EL CASO DE HABERSE OTORGADO. EN EL CASO QUE NO SE HUBIERE OTORGADO GARANTÍA, LA MISMA NO SE PUDIERA HACER EFECTIVA O NO ALCANCE PARA CUBRIR EL MONTO DETERMINADO, SE PROCEDERÁ A INHABILITARLOS DE LOS SISTEMAS INFORMÁTICOS, HASTA QUE CANCELEN LOS COSTOS DE LA DESTRUCCIÓN EN QUE HUBIERE DE INCURRIR LA ADMINISTRACIÓN.

PARA CUMPLIR CON LO DISPUESTO EN EL INCISO ANTERIOR, EL SERVICIO ADUANERO DEBERÁ ESTABLECER EL MONTO DEL COSTO DE LA DESTRUCCIÓN EN LA RESOLUCIÓN QUE PONE FIN AL PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR O DE LIQUIDACIÓN OFICIOSA DE IMPUESTOS. EN CASO QUE NO SE HUBIERE INICIADO PROCEDIMIENTO ADMINISTRATIVO, DEBERÁ EMITIR UNA RESOLUCIÓN EN LA QUE DETALLE LOS COSTOS DE LA DESTRUCCIÓN, DEBIENDO NOTIFICARLA AL OBLIGADO PARA SU PAGO, CONFORME A LAS REGLAS ESTABLECIDAS EN EL ARTÍCULO 16 DE LA PRESENTE LEY.

LO ANTERIOR SIN PERJUICIO DE LAS RESPONSABILIDADES PENALES QUE PUDIERAN RESULTAR DE TALES CONDUCTAS. (4)

Art. 12-B.- CRÉASE UNA TASA QUE SE COBRARÁ POR LA PRESTACIÓN DE SERVICIOS DE INSPECCIÓN NO INTRUSIVA.

LA TASA EN REFERENCIA SERÁ DE UN MONTO DE DIECIOCHO DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA, LA CUAL INCLUYE EL PAGO DEL IMPUESTO A LA TRANSFERENCIA DE BIENES MUEBLES Y A LA PRESTACIÓN DE SERVICIOS. EL SERVICIO ADUANERO NO PODRÁ AUTORIZAR EL DESPACHO SIN EL PAGO DE LA MISMA.

LA OBLIGACIÓN DEL PAGO SE GENERARÁ SIEMPRE Y CUANDO LAS OPERACIONES ANTES INDICADAS SE PRODUZCAN POR EL INGRESO O SALIDA DE MERCANCÍAS O MEDIOS DE TRANSPORTE DEL TERRITORIO ADUANERO NACIONAL POR CUALQUIER VÍA.

EL PAGO DEBERÁ EFECTUARSE AL MOMENTO DE LA TRANSMISIÓN ELECTRÓNICA DEL MANIFIESTO, DECLARACIÓN DE MERCANCÍAS A CUALQUIERA DE LOS REGÍMENES ADUANEROS, FORMULARIO ADUANERO ÚNICO CENTROAMERICANO, TRÁNSITOS INTERNOS O INTERNACIONALES U OTRAS DECLARACIONES O FORMULARIOS QUE AMPAREN EL TRANSPORTE, TRASLADO O MOVIMIENTO DE MERCANCÍAS DESDE Y HACIA EL TERRITORIO ADUANERO NACIONAL, UTILIZANDO CUALQUIERA DE LAS PLATAFORMAS AUTORIZADAS POR EL SERVICIO ADUANERO QUE PERMITAN LA CAPTURA DE DICHOS DOCUMENTOS.

A LOS EFECTOS DE LO ESTABLECIDO EN LA PRESENTE DISPOSICIÓN, SON SUJETOS RESPONSABLES Y COMO CONSECUENCIA ESTÁN OBLIGADOS AL PAGO DE LA TASA EN REFERENCIA, LOS DECLARANTES O EL REPRESENTANTE DE ÉSTOS, QUE DE ACUERDO A LO ESTABLECIDO EN LA PRESENTE LEY, DEBAN HACER USO DEL SERVICIO DE INSPECCIÓN NO INTRUSIVA.

CORRESPONDERÁ A LA DIRECCIÓN GENERAL DE ADUANAS EJERCER LAS FACULTADES ADMINISTRATIVAS NECESARIAS QUE GARANTICEN LA OPORTUNA VERIFICACIÓN Y COMPROBACIÓN

DEL PAGO DE LA TASA POR LA PRESTACIÓN DEL SERVICIO DE INSPECCIÓN NO INTRUSIVO.

PARA LOS EFECTOS ANTERIORES, FACÚLTASE AL MINISTERIO DE HACIENDA, A TRAVÉS DE LA DIRECCIÓN GENERAL DE ADUANAS Y LA DIRECCIÓN GENERAL DE TESORERÍA, PARA EMITIR LAS REGULACIONES DE ORDEN ADMINISTRATIVO Y DE CARÁCTER GENERAL QUE GARANTICEN EL COBRO DE LA TASA.

EL INCUMPLIMIENTO AL PAGO DE LA TASA SERÁ SANCIONADO DE CONFORMIDAD A LO ESTABLECIDO EN LA LEY ESPECIAL PARA SANCIONAR INFRACCIONES ADUANERAS. (4)

Art. 12-C.- FACÚLTASE AL MINISTERIO DE HACIENDA, PARA QUE MEDIANTE LA EMISIÓN DEL ACUERDO EJECUTIVO CORRESPONDIENTE, QUE DEBERÁ SER RAZONADO, MOTIVADO Y JUSTIFICADO, HAGA LOS AJUSTES A LA TASA YA DETERMINADA.

LA TASA PODRÁ SER REVISADA Y AJUSTADA CADA DOS AÑOS POR EL MINISTERIO DE HACIENDA, HASTA UN MÁXIMO DE 10 POR CIENTO, SOBRE EL VALOR DE LA TASA ESTABLECIDA EN EL ARTÍCULO ANTERIOR, CONSIDERANDO ENTRE OTROS ASPECTOS: EL ÍNDICE DE INFLACIÓN ACUMULADA, EL AUMENTO O DISMINUCIÓN DE LAS OPERACIONES, ASÍ COMO CUALQUIER VARIACIÓN DE LOS COSTOS SIGUIENTES:

a) EL COSTO DE MANTENIMIENTO RUTINARIO, ENTENDIDO COMO TAL, LA SUMA DE LOS COSTOS NECESARIOS PARA MANTENER EL SISTEMA NO INTRUSIVO EN LAS MEJORES CONDICIONES DE OPERATIVIDAD;

b) EL COSTO DE MANTENIMIENTO PREVENTIVO, RELACIONADO A LA INVERSIÓN NECESARIA PARA PREVENIR EL DETERIORO DEL SISTEMA NO INTRUSIVO;

c) EL COSTO DEL MANTENIMIENTO CORRECTIVO, ENTENDIDO COMO LA PROYECCIÓN QUE SE REALICE DE LOS COSTOS EN QUE PUEDA INCURRIRSE PARA LA REPARACIÓN O SUSTITUCIÓN DEL SISTEMA DE INSPECCIÓN NO INTRUSIVO;

d) EL COSTO DE LA OPERACIÓN, ENTENDIDO COMO LA SUMA DE LOS COSTOS NECESARIOS PARA CUBRIR LOS GASTOS DIRECTOS E INDIRECTOS QUE GARANTICEN LA ADECUADA PRESTACIÓN DEL SERVICIO, TALES COMO LA NÓMINA, IMPUESTOS Y TASAS, ASISTENCIAS TÉCNICAS, CONTRAPRESTACIONES, USO DE LA INFRAESTRUCTURA Y OTROS.

e) EL COSTO DE ACTUALIZACIÓN O MEJORAMIENTO, REFERIDO AL VALOR NECESARIO PARA MEJORAR, AMPLIAR, ADECUAR O ACTUALIZAR LOS EQUIPOS Y SISTEMAS.

SI LA PRESTACIÓN DEL SERVICIO DE INSPECCIÓN NO INTRUSIVA FUERE CONCESIONADO, TAMBIÉN SE DEBERÁN CONSIDERAR, ENTRE OTROS, LOS REQUERIMIENTOS TÉCNICOS DE LA ADMINISTRACIÓN ADUANERA Y LOS RENDIMIENTOS DE LA INFRAESTRUCTURA A UTILIZAR, DETERMINANDO LA CAPACIDAD DE LA MISMA; EN ESE CASO, TAMBIÉN DEBERÁN TOMARSE EN CUENTA LOS COSTOS DE INVERSIÓN ASOCIADOS EN LOS QUE EL ESTADO SE VEA OBLIGADO A INCURRIR. (4)

Art. 13.- CUANDO DE CONFORMIDAD CON LOS CRITERIOS SELECTIVOS Y ALEATORIOS,

CORRESPONDA EFECTUAR LA VERIFICACIÓN INMEDIATA DE LO DECLARADO, EL ADMINISTRADOR DE ADUANAS DEBERÁ DISPONER LA PRÁCTICA DE LA MISMA; PARA TALES EFECTOS, DESIGNARÁ UNO O VARIOS CONTADORES VISTA PARA QUE LA REALICEN, QUIENES DEBERÁN PRACTICARLA DENTRO DEL MISMO DÍA EN QUE LAS MERCANCÍAS SE ENCUENTREN A SU DISPOSICIÓN PARA REALIZAR DICHA DILIGENCIA, SALVO QUE LA AUTORIDAD ADUANERA REQUIERA UN PLAZO MAYOR, DE ACUERDO A LAS CARACTERÍSTICAS Y NATURALEZA DE LAS MISMAS.

MIENTRAS LA DIRECCIÓN GENERAL NO POSEA LOS MEDIOS ELECTRÓNICOS PARA LA RECEPCIÓN Y ARCHIVO DE LA DOCUMENTACIÓN QUE SUSTENTEN LAS OPERACIONES DE IMPORTACIÓN Y EXPORTACIÓN, ÉSTA SERÁ ARCHIVADA POR LA AUTORIDAD ADUANERA, SEA QUE HAYA OPERADO VERIFICACIÓN INMEDIATA DE LO DECLARADO O LEVANTE AUTOMÁTICO DE LA MERCANCÍA.

EN LOS CASOS EN QUE EL SUJETO PASIVO, SEA OBJETO DE UN PROCESO DE VERIFICACIÓN DE ORIGEN POR PARTE DE LA AUTORIDAD COMPETENTE DEL PAÍS IMPORTADOR, LA DIRECCIÓN GENERAL, PREVIA SOLICITUD DEL INTERESADO PODRÁ ENTREGAR CERTIFICACIÓN DE LA DOCUMENTACIÓN ORIGINAL RELACIONADA CON LAS EXPORTACIONES REALIZADAS.

LOS SUJETOS PASIVOS QUE DE CONFORMIDAD CON LAS LEYES RESPECTIVAS ESTÉN OBLIGADOS A LLEVAR CONTABILIDAD FORMAL, DEBERÁN TENERLA A DISPOSICIÓN DE LA AUTORIDAD ADUANERA COMPETENTE CUANDO ÉSTA LA REQUIERA EN EL EJERCICIO DE SUS FACULTADES DE CONTROL Y VERIFICACIÓN A POSTERIORI. AQUELLOS SUJETOS PASIVOS QUE NO ESTÉN OBLIGADOS A LLEVAR CONTABILIDAD FORMAL, DEBERÁN LLEVAR REGISTROS ESPECIALES DE CONFORMIDAD CON LAS LEYES, LOS CUALES DEBERÁN TENERSE A DISPOSICIÓN DE LA AUTORIDAD ADUANERA COMPETENTE. EN AMBOS CASOS EL TIEMPO EN QUE SE DEBERÁN TENER A DISPOSICIÓN LOS REGISTROS CONTABLES, REGISTROS ESPECIALES Y LA DOCUMENTACIÓN DE RESPALDO DE LOS MISMOS, SERÁ DE CINCO AÑOS.

LOS EXPORTADORES Y PRODUCTORES DEBERÁN CONSERVAR POR UN MÍNIMO DE CINCO AÑOS, A PARTIR DE LA FECHA DE SU EMISIÓN, LAS CERTIFICACIONES O CERTIFICADOS DE ORIGEN, ASÍ COMO TODOS LOS REGISTROS Y DOCUMENTOS QUE DEMUESTREN QUE UNA MERCANCÍA, PARA LA CUAL EL PRODUCTOR O EL EXPORTADOR PROPORCIONÓ UNA CERTIFICACIÓN DE ORIGEN, DE CONFORMIDAD A LO ESTABLECIDO EN LOS TRATADOS, CONVENIOS, ACUERDOS Y OTROS INSTRUMENTOS EN MATERIA DE COMERCIO SUSCRITOS POR EL PAÍS. (2) (3)

Art. 14.- La Dirección General tendrá amplias facultades de fiscalización, inspección, investigación y control con el fin de asegurar el exacto cumplimiento de las obligaciones tributarias aduaneras y de los demás requisitos no arancelarios que sean necesarios para la autorización del régimen solicitado, incluso respecto de los sujetos que gocen de exenciones, franquicias o incentivos tributarios, tanto en lo relativo a sus declaraciones como al cumplimiento de las condiciones que impone el régimen aduanero declarado o tratamiento tributario especial.

En su función fiscalizadora, la Dirección General podrá:

a) Practicar inspecciones en locales ocupados a cualquier título por los sujetos pasivos de las obligaciones tributarias aduaneras;

b) Exigir a los sujetos pasivos de los derechos e impuestos a la importación, en relación con las operaciones objeto de investigación, la exhibición de sus libros y balances; sistemas,

programas, archivos y registros de contabilidad manual, mecánica o computarizada; documentos, correspondencia comercial, bienes y mercaderías; así como examinar y verificar los mismos y tomar medidas de seguridad para su conservación en el lugar en que se encuentren, aún cuando no correspondan al domicilio del contribuyente, quedando los mismos bajo la responsabilidad de éste;

c) Requerir informaciones y declaraciones a los sujetos pasivos de la obligación tributaria aduanera y auxiliares de la función pública aduanera, relacionadas con hechos que en el ejercicio de sus actividades hayan contribuido a realizar o hayan debido conocer, así como la exhibición de documentación relativa a tales situaciones que se vincule con las obligaciones antes referidas;

d) Exigir a los beneficiarios de franquicias e incentivos tributarios informes sobre el cumplimiento de los requisitos para gozar de tales beneficios;

e) Requerir, cuando no exista prohibición legal, de las personas particulares, de los funcionarios, instituciones o empresas públicas y de las autoridades en general, todos los datos y antecedentes que se estimen necesarios para la fiscalización y control de las obligaciones aduaneras tributarias y no tributarias. Las personas naturales tendrán la obligación de rendir testimonio bajo juramento en calidad de terceros, pudiendo la Dirección General verificar estos testimonios, datos e informes. Se exceptúan de esta norma la Dirección General de Estadística y Censos y las entidades estatales en lo que concierne a informes confidenciales que su respectiva ley de creación o reglamento les prohíban divulgar;

f) Fiscalizar el tránsito aduanero de mercancías por cualquier medio para verificar que se cumpla con los requisitos prescritos en la normativa aduanera;

g) Citar a contribuyentes, responsables o a cualquier tercero para que conteste o informe, verbalmente, por escrito o por cualquier otro medio autorizado por la Dirección General, las preguntas o requerimientos que se estimen necesarios para la verificación del exacto cumplimiento de las obligaciones aduaneras. De esta diligencia deberá levantarse acta, firmada o no por el citado, que servirá de medio de prueba en los procedimientos respectivos;

h) Examinar los hechos que puedan configurar infracciones y hacer del conocimiento de la Fiscalía General de la República sobre las infracciones penales, a efecto de asegurar los medios de prueba e individualizar a los infractores.

La Dirección General deberá potenciar además la fiscalización como un instrumento de orientación a los usuarios de los servicios aduaneros, de modo que se facilite a los mismos el cumplimiento voluntario de sus obligaciones aduaneras.

El plazo para la verificación posterior caducará en cinco años contados desde la fecha de aceptación de la declaración de mercancías correspondientes.

Art. 14-A. PARA EJERCER LAS FACULTADES DE FISCALIZACIÓN A POSTERIORI Y DE VERIFICACIÓN

DE ORIGEN, LA DIRECCIÓN GENERAL CONTARÁ CON UN CUERPO DE AUDITORES Y TÉCNICOS. EN CADA FISCALIZACIÓN O VERIFICACIÓN DE ORIGEN PODRÁN TOMAR PARTE UNO O MÁS AUDITORES O TÉCNICOS QUE LA DIRECCIÓN GENERAL DESIGNE. LOS AUDITORES Y TÉCNICOS TIENEN LAS FACULTADES QUE DE CONFORMIDAD A LA LEGISLACIÓN ADUANERA Y ACUERDOS, CONVENIOS, TRATADOS Y OTROS INSTRUMENTOS EN MATERIA COMERCIAL, LES ASIGNE LA DIRECCIÓN GENERAL EN EL ACTO DE SU DESIGNACIÓN.

LOS AUDITORES O TÉCNICOS AL CONCLUIR SU COMISIÓN, DEBERÁN FORMULAR UN INFORME DIRIGIDO AL DIRECTOR GENERAL DE ADUANAS; DICHO INFORME CUANDO SE TRATE DE FISCALIZACIONES A POSTERIORI SERÁ TRASCRITO ÍNTEGRAMENTE PARA CONOCIMIENTO DEL SUJETO PASIVO.

LOS EMPLEADOS, TÉCNICOS, AUDITORES, PERITOS, COLABORADORES JURÍDICOS, CONTADORES VISTA, OFICIALES ADUANEROS Y FUNCIONARIOS DE LA ADMINISTRACIÓN ADUANERA, NO DEBERÁN LLEVAR POR SI O POR INTERPÓSITA PERSONA, CONTABILIDADES O AUDITORÍAS PARTICULARES Y ASESORÍAS DE CARÁCTER TRIBUTARIO ADUANERO. EL INCUMPLIMIENTO A ESTA DISPOSICIÓN SE SANCIONARÁ DE CONFORMIDAD A LA LEGISLACIÓN APLICABLE. (3)

Art. 15.- CUANDO POR MOTIVO DE LA VERIFICACIÓN INMEDIATA O DE LA FISCALIZACIÓN POSTERIORI, LA AUTORIDAD ADUANERA COMPETENTE, DETERMINE LA EXISTENCIA DE DERECHOS E IMPUESTOS A LA IMPORTACIÓN O CUALQUIER TRIBUTO QUE NO HUBIERE SIDO CANCELADO TOTAL O PARCIALMENTE CON LA DECLARACIÓN DE IMPORTACIÓN RESPECTIVA O ESTABLEZCA EL INCUMPLIMIENTO DE ALGUNA DE LAS REGULACIONES DETERMINADAS EN ACUERDOS, CONVENIOS, TRATADOS Y OTROS INSTRUMENTOS EN MATERIA DE COMERCIO, ABRIRÁ EL PROCESO ADMINISTRATIVO CORRESPONDIENTE. (3)

Art. 16.- Los resultados de la fiscalización deberán ser notificados al declarante o a su agente de aduanas en su caso de acuerdo con las reglas siguientes:

Se notificará al supuesto infractor, a su representante legal, apoderado o mandatario aduanero, curador o heredero, en el lugar señalado para recibir notificaciones o en su domicilio. Tales notificaciones se harán por cualquier Delegado de la Dirección General, por la vía electrónica, telefax o telefacsímil, por correo certificado con constancia de recepción, o por los demás medios que autoricen las leyes.

Si no se encontrare al interesado o a cualquiera de sus representantes en el lugar señalado para recibir notificaciones o en su domicilio, se le notificará por medio de su cónyuge o compañera de vida, hijo mayor de edad, socio, dependiente o sirviente doméstico, o por medio de persona mayor de edad que esté al servicio del representante, apoderado, curador o heredero, o de la empresa, oficina o dependencia establecida en el lugar señalado.

Si no se encontrare ninguna de las personas señaladas en el inciso precedente, en la dirección indicada, o se negaren a recibirla, se fijará en la puerta de la casa u oficina, una esquela en la cual se notificará la resolución en extracto.

Si no se dieren las circunstancias para que la actuación quede legalmente notificada, ésta se hará por edicto, sujetándose a las formalidades siguientes: Se fijará en el tablero de la Dirección General o de la Aduana respectiva, un extracto breve y claro del auto o resolución correspondiente por un término de

setenta y dos horas, pasadas las cuales se tendrá por hecha la notificación. Los interesados estarán obligados a concurrir a la Dirección General si desean conocer íntegramente la providencia que se ha hecho saber en extracto.

Debido a la solidaridad que se establece entre el declarante y su agente de aduanas en lo que respecta a sus obligaciones tributarias aduaneras y al mandato que de acuerdo con la legislación de la materia se establece entre los mismos, la notificación que se haga al agente de aduanas se entenderá extensiva para el declarante.

Art. 17.- El proceso administrativo a que alude el Art. 15 de esta Ley, se desarrollará de la siguiente manera:

a) LA APERTURA DEL PROCESO DEBE NOTIFICARSE AL DECLARANTE O A SU AGENTE DE ADUANAS, APODERADO O REPRESENTANTE, HACIÉNDOLES SABER EL CONTENIDO ÍNTEGRO DEL INFORME DE FISCALIZACIÓN, HOJA DE DISCREPANCIA O INFORME DE INVESTIGACIÓN CORRESPONDIENTE, CONFORME A LAS REGLAS DE NOTIFICACIÓN ESTABLECIDAS EN EL ARTICULO ANTERIOR; (3)

b) El declarante contará con un plazo de quince días hábiles contados desde el siguiente día de la notificación para la presentación de sus alegatos y las pruebas de descargo que estime pertinentes;

c) VENCIDO DICHO PLAZO, LA DIRECCIÓN GENERAL DICTARÁ LA RESOLUCIÓN QUE PROCEDA DENTRO DEL PLAZO DE VEINTE DÍAS HÁBILES. LA NOTIFICACIÓN DE DICHA RESOLUCIÓN SE HARÁ DENTRO DEL PLAZO DE VEINTE DÍAS HÁBILES POSTERIORES A LA FECHA DE SU EMISIÓN, LA CUAL DEBERÁ CONTENER EL TEXTO ÍNTEGRO DE LA MISMA. (2)

CONTRA LA RESOLUCIÓN DE LIQUIDACIÓN OFICIOSA DE IMPUESTOS QUE SE DICTE, SE ADMITIRÁN LOS RECURSOS ADMINISTRATIVOS SEÑALADOS EN LA LEY ESPECIAL PARA SANCIONAR INFRACCIONES ADUANERAS, ANTE LAS AUTORIDADES COMPETENTES Y CONFORME A LOS REQUISITOS, PLAZOS Y PROCEDIMIENTOS ESTABLECIDOS EN LA MISMA. (3)

Art. 18.- Los empleados, funcionarios y usuarios del servicio de aduanas y demás personas autorizadas que utilicen los sistemas informáticos y medios de transmisión electrónica de datos de enlace con la autoridad aduanera, deberán acatar las medidas de seguridad que la Dirección General establezca, incluyendo las relativas al uso de códigos, claves de acceso confidenciales o de seguridad.

Art. 19.- Debido al carácter especial de la presente Ley, las normas de la misma prevalecerán sobre las contenidas en cualquier otra ley, decreto, reglamento o normativa que las contrarie.

Art. 20.- La Dirección General está facultada para emitir las normas administrativas que sean necesarias para el desarrollo de los principios contenidos en esta Ley, principalmente de aquellos que regulan la emisión, transferencia, uso y control de la información relacionada con las operaciones aduaneras.

Art. 21.- El Presidente de la República emitirá el reglamento de la presente ley dentro de los ciento ochenta días subsiguientes a la vigencia de la misma.

Art. 22.- El presente Decreto entrara en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL SALON AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los trece días del mes de enero de mil novecientos noventa y nueve.

JUAN DUCH MARTINEZ
PRESIDENTE

GERSON MARTINEZ
PRIMER VICEPRESIDENTE

CIRO CRUZ ZEPEDA PEÑA
SEGUNDO VICEPRESIDENTE

RONAL UMAÑA
TERCER VICEPRESIDENTE

NORMA FIDELIA GUEVARA DE RAMIRIOS
CUARTA VICEPRESIDENTA

JULIO ANTONIO GAMERO QUINTANILLA
PRIMER SECRETARIO

JOSE RAFAEL MACHUCA ZELAYA
SEGUNDO SECRETARIO

ALFONSO ARISTIDES ALVARENGA
TERCER SECRETARIO

GERARDO ANTONIO SUVILLAGA
CUARTO SECRETARIO

ELVIA VIOLETA MENJIVAR
QUINTA SECRETARIA

JORGE ALBERTO VILLACORTA MUÑOZ
SEXTO SECRETARIO

CASA PRESIDENCIAL: San Salvador, a los veintiún días del mes de enero de mil novecientos noventa y nueve.

PUBLIQUESE,

ARMANDO CALDERON SOL
Presidente de la República

Manuel Enrique Hinds Cabrera,
Ministro de Hacienda.

D. O. N° 23
Tomo N° 342
Fecha: 3 de febrero de 1999.

REFORMAS:

(1) D.L. Nº 523, 30 DE AGOSTO DE 2001;
D.O. Nº 188, T. 353, 5 DE OCTUBRE DE 2001.

(2) D.L. Nº 490, 27 DE OCTUBRE DE 2004;
D.O. Nº 217, T. 365, 22 DE NOVIEMBRE DE 2004.

(3) D.L. Nº 906, 14 DE DICIEMBRE DE 2005;
D.O. Nº 8, T. 370, 12 DE ENERO DE 2006.

(4) D.L. No. 23, 7 DE JUNIO DE 2012;
D.O. No. 123, T. 396, 4 DE JULIO DE 2012.

DISPOSICIONES TRANSITORIAS:

D. L. No. 604, 16 DE ENERO DE 2014;
D. O. No. 9, T. 402, 16 DE ENERO DE 2014. **(Vence 14/07/14)**
PRÓRROGA AL D.L.Nº 604/2014:
D. L. No. 738, 10 DE JULIO DE 2014;
D. O. No. 128, T. 404, 11 DE JULIO DE 2014. **(Vence 11/09/14)**

SUSPÉNDASE POR 60 DÍAS, A PARTIR DEL 9 DE SEPTIEMBRE DE 2014, EL COBRO DE LA TASA POR LA PRESTACIÓN DE SERVICIOS DE INSPECCIÓN NO INTRUSIVA A LAS OPERACIONES DE TRÁNSITO TERRESTRE INTERNACIONAL DE MERCANCÍAS, CONTENIDA EN EL ART. 12-B DE LA LEY DE SIMPLIFICACIÓN ADUANERA.
D.L. No. 801, 11 DE SEPTIEMBRE DE 2014.
D.O. No. 169, T. 404, 12 DE SEPTIEMBRE DE 2014. **(Vence 7/11/14)**

DISPOSICIÓN ESPECIAL:

- **SUSPÉNDESE POR EL PERÍODO DE 6 MESES LA TASA ESTABLECIDA EN EL ART. 12-B DE LA LEY DE SIMPLIFICACIÓN ADUANERA.**
D.L. N° 629, 20 DE FEBRERO DE 2014. **(VETADO)**

SV/mgcl
31/01/06

ROM/mlddb

SV
07/08/12

JQ
21/02/14

GLOSARIO

Ataques cibernéticos
Es un método que una persona realiza para poder cometer un crimen en la red, intentando tomar el control de un computador cuyo fin principal es dañar otro sistema informático.

CA
Por sus siglas en ingles es llamado: certificate authority, pero es mejor conocido como: *"Centro de Certificación"* Y es una entidad la cual emite y revoca certificados digitales.

Cibercriminales
Es una persona que intencionalmente realiza un crimen por medio de internet.

Cifrado de datos simétricos
Es un algoritmo de seguridad que maneja la misma llave para cifrar y descifrar la información de forma segura.

Cifrado de datos asimétricos
Es un protocolo criptográfico que utiliza una llave pública para cifrar el mensaje y una llave privada para descifrarlo o viceversa

DES (estándar de cifrado de datos)
Es un protocolo de seguridad que ocupa una llave de 64 bits de cifrado, con una longitud de 56 bits, lo cual facilita su utilización y el cifrado de datos.

Firewall
Es un software o hardware basado en el control del tráfico saliente o entrante a la redes. Es el que autoriza o deniega todo paquete por medio de una política de seguridad configurada en el dispositivo.

Firma digital
Es un algoritmo que utiliza la criptografía con HASH de 128 bits, para cifrar y descifrar la información no solo del emisor sino también la del receptor y además verifica la autenticación e integridad del documento.

Hacker
Es una persona que obtiene acceso no autorizado a un computador.

Llave pública
Código cifrado que está disponible públicamente a las personas.

Llave privada
Código cifrado que es conocido únicamente por su creador.

Punto a punto (PPP)
Es un protocolo que es manejado a nivel de enlace de datos para establecer conexión entre la LAN y la WAN.

Suplantación de identidad
Es una técnica de crimen informático, donde su finalidad está en falsificar la identidad de un individuo o empresa.

Túnel
Se refiere al encapsulamiento de un protocolo de red sobre otro.

Virus
Es un conjunto de códigos programables que es insertado en un programa para poder ingresar a un host de forma indebida, la cual se distribuye en nuestro ordenador con la finalidad de destruir, robar o compartir información de forma ilegal

VPN
Por sus siglas en inglés significa Virtual Private Network, pero también es mejor conocida como la Red Virtual Privada. Adicional a ello, ocupa el internet público que cifra su comunicación para asegurar que la información que viaja por internet no haya sido alterada en su trayectoria.

Vulnerabilidad
Debilidad en un software o en otro mecanismo que amenaza la confidencialidad, integridad o disponibilidad de un activo.

Zona desmilitarizada
(Demilitarized zone por sus siglas en inglés DMZ) es una red que se ubica entre la red interna de una organización y una red externa.