

Cargo Security

PUBLICACIÓN ESPECIALIZADA EN SEGURIDAD DE LA CADENA DE SUMINISTRO INTERNACIONAL

AÑO IV / 2011 - 9

Un nuevo frente de prevención: **LA CIBER SEGURIDAD**

- ▶ **Evitar un 11-S digital vía ataques cibernéticos** (Pág. 3)
AVOIDING A DIGITAL 11-S VIA CYBER ATTACKS
- ▶ **Las actuales amenazas en el ciber espacio** (Pág. 5)
CURRENT THREATS IN CYBER SPACE
- ▶ **Estrategias nuevas para nuevas guerras** (Pág. 9)
NEW STRATEGIES FOR NEW WARS

Los Programas de Operador Económico Autorizado (OEA) en Asia (Pág. 13).

El programa OEA en la Unión Europea: Un vistazo general (Pág. 21).

Promueven implementación del programa OEA en el Perú (Pág. 27).

Especialistas en Soluciones Transaccionales para Comercio Exterior y Operaciones Logísticas

TCI [®] **19** Años de
Excelencia
en el Servicio
Soluciones de Tecnología de Información



CHECK POINT
Software Technologies Ltd.



We Secure the Internet.



- B2B - Teledespacho Aduanero & EDI
- Soluciones para Agentes de de Carga
- Soluciones para Agentes Marítimos
- Soluciones de Factura Electrónica
- Soluciones de seguridad, monitoreo y control
- Consultoría TI y Desarrollo de Software
- Hosting / Housing & Servicios de Internet



www.tci.net.pe



Contenido / Content



3

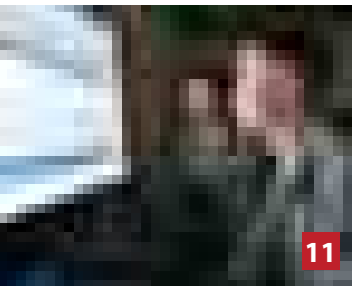
2 EDITORIAL / EDITORIAL

Un nuevo frente de prevención: La ciber seguridad / *A new prevention resource: cyber security.*

3 PORTADA / COVER

La Ciber seguridad: Nueva capa de seguridad contra el crimen organizado / *Cyber security: New layer of security against organized crime*

- Evitar un 11-S digital vía ataques cibernéticos / *To avoid a digital 11-S digital via cyber attacks*
- Las actuales amenazas en el ciber espacio / *The current threats in cyberspace*
- Configuración del nuevo escenario de guerra / *Configuration of the new war scenario*
- Estrategias nuevas para nuevas guerras / *New strategies for new wars*
- Los riesgos por zonas (incluye Sudamérica) / *Risks by areas (including South America)*
- Lo último: Ciber guerra con reglas de comportamiento / *The latest: Cyber war with rules of behavior*



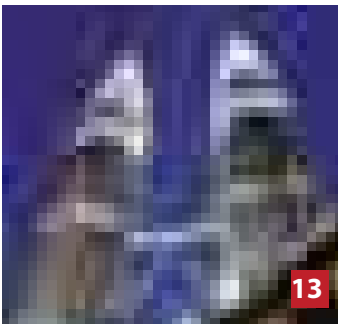
11

13 ENFOQUE / APPROACH

Los Programas de Operador Económico Autorizado (OEA) en países asiáticos / *Authorized Economic Operator (AEO) programs in Asian countries*

21 AL DÍA / UP TO DATE

El programa OEA en la Unión Europea: Un vistazo general / *The AEO program in the European Union: An overview*



13

24 ENTREVISTAS / INTERVIEWS

Daniel Linares, Intendente de Análisis de la Unidad de Inteligencia Financiera (UIF) de la SBS (Plan Nacional de Lucha Contra el Lavado de Activos y Financiamiento del Terrorismo) / *Mayor of Analysis of the Financial Intelligence Unit (FIU) of the SBS (National Plan to Combat Money-Laundering and Financing of Terrorist)*

Fermín Cuza, Presidente Internacional de la Organización Mundial BASC (Acceso más rápido a los mercados extranjeros y tomar ventaja de los acuerdos comerciales) / *International president of the World BASC Organization (Faster access to foreign markets and take advantage of trade agreements)*

30 ACTUALIDAD / PRESENT TIME

- Respuesta coordinada para la seguridad del transporte de carga / *Coordinated response to the security of cargo transportation*
- C-TPAT y OEA, lo mismo pero diferentes / *C-TPAT and AEO, the same but different*
- China y Estados Unidos colaboran con la seguridad del comercio / *China and the United States cooperate with trade security*
- Inician programa europeo de vigilancia marítima PERSEUS / *They begin PERSEUS, an European maritime surveillance program*

35 MUNDO BASC / WORLD BASC

Noticias y actividades de BASC / *BASC News and activities*

37 NOTICIAS Y EVENTOS / NEWS AND EVENTS

Sucesos del mundo del Supply Chain Security / *Events in the world of Supply Chain Security.*



24



Un nuevo frente de prevención: la ciber seguridad

A new prevention resource: cyber security

En esta edición estamos cubriendo un tema que viene imponiéndose paulatinamente a nivel mundial entre las preocupaciones actuales de seguridad. Se trata de la ciber seguridad. Efectivamente, en un mundo donde los sistemas de redes informáticas dirigen la vida cotidiana de las personas, empresas y organizaciones privadas y públicas (que incluye gobiernos), han surgido nuevos riesgos, desde los más elementales (ej.: contaminación de virus en una computadora personal) hasta la seguridad nacional (ej.: incursión no autorizada al sistema informático de una central nuclear), pasando por la agresión de tipo empresarial (ej.: espionaje industrial).

A la luz de los acontecimientos, de ser solo una posibilidad de amenaza hace algunos años atrás, este tema se ha convertido a la fecha en una preocupante realidad. La ciber seguridad ahora ocupa un lugar en la agenda de los gobiernos de países desarrollados. Es más, ya existen en esos países proyectos específicos en marcha destinados a convertirse en el centro de operaciones para prevenir y contrarrestar las amenazas en este campo.

¿Y las empresas? Aunque no existe mucha información respecto a los ataques directos a organizaciones empresariales, sus efectos y las reacciones, es de dominio público que reconocidas compañías, especialmente transnacionales, no han estado exentas de estas amenazas. En este sentido debemos ser prevenidos, pues no es descabellado pensar que la delincuencia organizada ya está fijando su mirada hacia este segmento organizacional. Nosotros, aplicando la prevención, le ofrecemos material actualizado para que se informe sobre los aspectos en este tipo de amenazas.

De hecho, este tema ya forma parte de nuestra preocupación institucional, por lo que brindaremos también eventos especializados para desarrollarlo con la participación de los expertos y de ustedes, quienes siempre serán la motivación principal para encontrar soluciones a los problemas de seguridad informática, antes que se conviertan en algo difícil de contrarrestar.

In this edition we are covering a topic that is gradually imposing itself worldwide among today's security concerns. This is cyber security. Indeed, in a world where computer network systems run the daily lives of individuals, businesses and public and private organizations (including governments), there are new risks from the most basic ones (e.g.: Contamination of virus in a personal computer) to national security (e.g.: unauthorized incursion into the computer system of a nuclear plant), to enterprise-class aggression (e.g.: industrial espionage).

In light of events, from just being a possibility of a threat a few years ago, this issue has become a disturbing reality so far. Cyber security now occupies a place on the governments' agenda of developed countries. Moreover, there are already specific projects afoot in those countries intended to become the operation center to prevent and counter the threats in this field.

What about the companies? Although there is little information regarding direct attacks on business organizations, their effects and reactions, it is common knowledge that recognized companies, especially multinationals, have not been exempt from these threats. In this sense we should be prevented, it is not unreasonable to think that organized crime is now setting its eyes to this organizational segment. We implement prevention, we offer updated material for reporting on the issues in this type of threat.

In fact, this issue is already part of our institutional concern, so we will also provide special events to develop it with the participation of experts and you who will always be the main motivation for finding solutions to security problems before they become difficult to counter.

Atentamente / Best regards

María del Carmen Masías
Presidente / President
BASC PERÚ

Comité Editorial / Editorial Board

María del Carmen Masías
Patricia Siles Álvarez
Raúl Saldías Haettenschweiler
César Venegas Núñez

Director / Director
César Venegas Núñez

Edición / Redacción / Editor / Writer
Unices Montes Espinoza

Coordinación / Coordinator
Giovanna Dloses Morel

Suscripciones y Publicidad / Subscription & Advertising
imagen@bascp Peru.org

Diagramación e Impresión / Design and Press
Comunica 2



BUSINESS ALLIANCE FOR SECURE COMMERCE

Alianza Empresarial para un Comercio Seguro
(Capítulo BASC PERÚ)
Av. Javier Prado Este 897, edif. Limatambo
8vo piso of. 84, San Isidro Lima- Perú
Teléf.: (511) 612-8300
www.bascp Peru.org

Consejo Directivo / Directors Board

Presidente del Directorio
Asociación Marítima del Perú - ASMARPE
María del Carmen Masías

Vicepresidente
Asociación Peruana de Operadores Portuarios - ASPPOR
Lorenzo L. Morandi Cadei

Director Secretario
Asociación de Exportadores - ADEX
José Letts Romero

Director Tesorero
Sociedad Nacional de Industrias - SNI
Mateo Balarin Benavides

Director Vocal
Sociedad de Comercio Exterior - COMEX
Patricia Siles Álvarez

Director Vocal
Cámara de Comercio Americana del Perú - AMCHAM
Aldo Defilippi Traverso

Directores
Cámara de Comercio de Lima - CCL
Juan A. Morales Bermúdez

Consejo Nacional de Usuarios de Distribución Física Internacional de Mercancías - CONUDFI
Armando Grados Mogrojevo

Asociación Peruana de Agentes Marítimos - APAM
Eduardo Amorrturo Velayos

Instituto Peruano de Espárragos y Hortalizas - IPEH
Leylha Rebaza García

Asociación de Servicios Aeroportuarios Privados - ASAEPI
Fernando Raventos Marcos

Asociación de Agentes de Aduana del Perú - AAAP
Arias Schreiber Ponce

Past President
BASC PERÚ
Raúl Saldías Haettenschweiler

Gerente General
César Venegas Núñez

Cargo Security® es una publicación bimestral promovida por los gremios que conforman la Alianza Empresarial para un Comercio Seguro (BASC por sus siglas en inglés), asociación civil sin fines de lucro adscrita a la Organización Mundial BASC.

Las opiniones vertidas en los artículos firmados son de exclusiva responsabilidad de sus autores.

Derechos reservados. Se permite la difusión del material contenido en esta revista siempre que se cite la fuente.

REGISTRO DE MARCA: Certificado N° 00153963
(Resolución N° 010346-2009/DSD-INDECOPI)



Seguridad cibernética internacional en marcha / *International cyber security in motion*

Evitar un 11-S digital vía ataques cibernéticos

AVOIDING A DIGITAL 11-S VIA CYBER ATTACKS

No es un término reciente, ya se habla de él desde años atrás como un riesgo potencial. Lo nuevo es que la seguridad cibernética ya es una realidad. Los promotores, como es de esperar, son los países desarrollados, pero el escenario de una potencial guerra cibernética es literalmente global. Además, paralelo al campo de seguridad nacional, este riesgo avanza también en el campo empresarial mundial conllevando potenciales pérdidas incalculables.

It is not a recent term. It has been discussed for years as a potential risk. What is new is that cyber security is a reality. The promoters, as expected, are the developed countries, but the scenario of a potential cyberwar is literally global. In addition, parallel to the field of national security, this risk also grows in the global business field implying potential incalculable losses.

El más reciente suceso que refleja plenamente la preocupación por un inminente ataque cibernético es el anuncio de la construcción en el Estado de Utah, Estados Unidos de América, de uno de los mayores complejos tecnológicos diseñados para dedicarse exclusivamente a prevenir esta amenaza. Se trata del

Utah Data Center, proyecto cuya construcción fue anunciado a finales del año pasado por la Agencia de Seguridad Nacional estadounidense (National Security Agency) con un presupuesto de US\$ 1.200 millones de dólares, en un extenso terreno al sur de Salt Lake City, capital de dicho Estado, ubicación donde los trabajos de construcción y desarrollo deman-

The most recent event that fully reflects the concern about an impending cyber attack is the announcement of the construction of one of the most complex technology in the State of Utah, United States of America designed to devote itself exclusively to prevent this threat. It is the Utah Data Center of which construction project was announced late last year by the U.S. National Security Agency with a budget of U.S. \$ 1,200 million in an extensive ground to the south of Salt Lake City, capital of the state, location where the construction and development will demand between 5 and 10 thousand jobs until October 2013 when completed.

According to reports in the American press, Utah was chosen to build the first "Spy Center" of this kind between more than other 37 potential sites in the country. Its weight and dimensions are such that this center of cyber security is considered "the largest military construction project in recent history."

For the selection of Utah, the authorities of this State promoted the important factors for the respective

darán entre 5 y 10 mil empleos hasta octubre de 2013 cuando sea culminado.

Según trascendió en la prensa estadounidense, Utah fue elegido para construir el primer "Spy Center" de este tipo de entre más de 37 otros lugares potenciales en el país. Su importancia y dimensión son tales que este centro de seguridad cibernética es considerado como "el más grande proyecto de construcción militar en la historia reciente".

Para la selección de Utah, las autoridades de este Estado promovieron factores importantes para que la licitación respectiva les sea favorable, tales como costos favorables de la energía, infraestructura de Internet, una próspera industria del software y la proximidad al aeropuerto internacional de Salt Lake City.

La infraestructura del complejo prevé ocupar 100 mil pies cuadrados (9,300 mts² aproximadamente) para el centro de datos (núcleo) y 900 mil pies cuadrados (84,000 mts² aproximadamente) de espacio para apoyo técnico y administrativo. En el núcleo las agencias de inteligencia del país recopilarán datos para ser utilizados por las agencias de seguridad nacional para proteger las redes de seguridad nacional y emitir advertencias sobre amenazas a la seguridad cibernética.

El centro está diseñado para ser capaz de producir su propia energía a través de una subestación eléctrica, así como sus propios almacenes de combustible y agua. Además, contará con servicios de apoyo que incluyen un edificio de inspección de vehículos, un centro de control de visitantes, una planta enfriadora, entre otros.

Resultado de una política nacional

El *Utah Data Center* se enmarca en el programa Comprehensive National Cybersecurity Initiative (Iniciativa Integral de Ciberseguridad Nacional) establecido por el presidente George Bush en enero de 2008 con la participación de varias agencias, entre ellas el Department of Homeland Security y la National Security Agency. Este programa tuvo inicialmente el carácter de material clasificado hasta que en marzo de 2010, la administración Obama ordenó se le retire dicha clasificación.

Entre los objetivos de la iniciativa se incluyen: establecer una línea de defensa contra la intrusión a las redes tecnológicas defendiendo EE.UU. contra todo el espectro de amenazas a través de contrainteligencia y el fortalecimiento del futuro de la

ciber seguridad a través de la educación, coordinación e investigación. Así mismo, el plan contempla doce iniciativas que conforman el cuerpo de acción, las cuales deben servir para enfocar el desarrollo del proceso respectivo. Estas son:

Iniciativa 1	Administrar la Red Federal como una red empresarial simple con conexiones de Internet confiables.
Iniciativa 2	Implementar un sistema de detección de intrusiones mediante sensores en toda la Red Federal.
Iniciativa 3	Continuar la implementación de sistemas de prevención de intrusiones a través de la Red Federal.
Iniciativa 4	Coordinar y redirigir los esfuerzos de investigación y desarrollo (I + D).
Iniciativa 5	Conectar los actuales "cyber ops centers" (centros de operaciones cibernéticas claves federales) para tener mayor conocimiento de la situación.
Iniciativa 6	Desarrollar e implementar una contrainteligencia cibernética (CI) en todo el gobierno.
Iniciativa 7	Aumentar la seguridad de nuestras redes clasificadas.
Iniciativa 8	Ampliar la educación cibernética.
Iniciativa 9	Definir y desarrollar tecnologías estrategias y programas "un salto adelante" duraderas.
Iniciativa 10	Definir y desarrollar estrategias y programas de disuasión permanente.
Iniciativa 11	Desarrollar un enfoque de frente múltiple para el manejo de riesgos de la cadena de suministro global.
Iniciativa 12	Definir el papel Federal para extender la seguridad cibernética en dominios de infraestructuras críticas.

Fuente: Prensa Utah / White House

bidding to be favorable such as favorable energy costs, Internet infrastructure, a thriving software industry and proximity to the airport in Salt Lake City.

The infrastructure of the complex expects to occupy 100 thousand square feet (9,300 m² approximately) for the data center (heart) and 900 thousand square feet (84,000 m² approximately) of space for administrative and technical support. At the heart the country's intelligence agencies will collect data to be used by national security agencies to protect national security networks and issue warnings about threats to cyber security.

The center is designed to be able to produce its own energy through an electrical substation, as well as their own fuel and water stores. It will also include support services that include a vehicle inspection building, a visitor control center, a cooler plant, among others.

Results of a national policy

The Utah Data Center is part of the Comprehensive National Cybersecurity Initiative established by President George Bush in January 2008 with the participation of several agencies including the Department of Homeland Security and the National Security Agency. This program initially had the character of classified material until the Obama administration ordered the withdrawal of such classification in March 2010.

The objectives of the initiative include: establishing a line of defense against intrusion to technological networks defending U.S. against the full spectrum of threats through counterintelligence and strengthening the future of cyber security through education, coordination and research. The plan also includes twelve initiatives to make up the body for action and these initiatives should serve to focus the development of the respective process. These are:

Las actuales amenazas en el ciber espacio

CURRENT THREATS IN CYBER SPACE

De acuerdo a William Jackson de Government Computer News, publicación estadounidense especializada en seguridad cibernética, respecto a las amenazas en el ciber espacio, podemos esperar que lo sucedido durante el 2010 podría repetirse en 2011. En general, las tendencias principales se basan en la consideración de que el "malware" es cada vez más sofisticado y los criminales más profesionales. Actualmente, en tanto que los profesionales de seguridad se encuentran trabajando para que la funcionalidad de las herramientas tecnológicas no supere a la seguridad, la aplicación de la ley podría ser cada vez mejor un instrumento para disipar la nube gris de la inseguridad. Para Jackson, los siguientes temas prevalecerán durante el 2011.

1) Supply Chain Security

Un estudio reciente de Enterprise Strategy Group, consultora de Massachusetts, Estados Unidos, encargado por Microsoft y Hewlett-Packard, encontró que muchas organizaciones en los sectores de infraestructuras críticas no estaban preparados para garantizar que las cadenas de suministro que dependen de recursos de las tecnologías de información sean dignas de crédito. El estudio concluyó que la seguridad de la cadena de suministro debe ser una alta prioridad para el futuro cercano.

Las vulnerabilidades introducidas a través de la cadena de suministro pueden ser particularmente peligrosas porque pueden ser especialmente diseñadas para atacar un objetivo específico evitando ser

detectados por los escáneres de códigos utilizados para detectar vulnerabilidades. Esto no es tan difícil, pues los escáneres se construyen generalmente en busca de errores no intencionales y no de cosas que intencionalmente se han ocultado.

2) Consumo de Tecnologías de la Información (IT por sus siglas en inglés)

Las computadoras ahora son productos básicos de consumo de tal modo que la línea de separación entre la casa (o cafetería) y el centro de trabajo está desapa-

reciendo, con la consecuencia de que las puertas de la empresa se abren más a las amenazas por la tendencia a llevar más y más dispositivos no administrados a la red. Es el caso, por ejemplo, de los conectores USB. Según especialistas, podría verse un aumento de los ataques dirigidos contra los dispositivos de consumo, mediante su acceso a los recursos corporativos.

3) Dispositivos móviles

El consumismo por los dispositivos informáticos está ligado estrechamente al factor movilidad,

According to William Jackson of Government Computer News, a publication that specializes in cyber security, we can expect that what happened with threats in cyberspace in 2010 could be repeated in 2011. In general, major trends are based on the consideration that "malware" is becoming more sophisticated and criminals more professional. Today, while security professionals are working for the functionality of the technological tools does not exceed the safety, law enforcement could be getting better, a tool to dispel the dark cloud of uncertainty. For Jackson, the following issues will prevail in 2011.

1) Supply Chain Security

A recent study by Enterprise Strategy Group, a consultant from Massachusetts, USA, commissioned by Microsoft and Hewlett-Packard found that many organizations in the critical infrastructure sectors were not prepared to en-

sure that supply chains that depend on technology resources of information be credible. The study concluded that the security of the supply chain should be a high priority for the near future.

The vulnerabilities introduced through the supply chain can be particularly dangerous because they can be specially designed to attack a specific target while avoiding detection by code scanners used to detect vulnerabilities. This is not that difficult since scanners are generally constructed looking for non-intentional errors and not things that have been intentionally hidden.

2) Consumption of Information Technology (IT)

Computers now are consumer basic consumption products so the line between the house (or cafeteria) and the workplace is disappearing with the result that the doors of the company are more open to threats by the tendency to take more and more unmanaged

y son aquellos dispositivos móviles que entran en contacto con el lugar de trabajo. Ejemplo: los teléfonos inteligentes. El temor es al “malware” de telefonía celular, riesgo que cada vez crece debido al veloz incremento de la cantidad de éstos teléfonos, así como del desarrollo de su funcionalidad.

4) Los objetivos políticos como blancos

Según especialistas se apreciará más espionaje cibernético y, potencialmente, el sabotaje cibernético. El ciber espionaje no es nuevo, en el 2010 hubo dos ejemplos de ataques ultra sofisticados, específicamente con el Google hack sucedido en diciembre de 2009 y el descubrimiento de Stuxnet, seis meses después.

En el primer caso, Google detectó un ataque a su infraestructura corporativa procedente de China y que había sido víctima de robo de propiedad intelectual. Similar


ataque se detectaron en otras 150 corporaciones en el mundo. Según McAfee, los ataques se habrían generado después de que algunos empleados de las empresas perjudicadas aplicaran un enlace que los direccionaba a una página web especial, desde la que se descargaba de forma secreta un software malicioso. Los hackers bautizaron dicha campaña como “Operación Aurora”.

El segundo caso se trata de un gusano informático que puede hacer el mismo daño que una bomba que destruye una planta industrial o una instalación militar porque actúa como un espía y reprograma los sistemas industriales. Se cree que el Stuxnet fue utilizado para atacar las instalaciones nucleares de Irán. Sus repercusiones son considerables, pues cualquier empresa que use sistemas de control industrial puede ser atacada por el gusano causando un daño comparado al de una explosión física.

El Google hack tiene como ob-

jetivo obtener información sensible de alto valor, en tanto que el Stuxnet al parecer obedece a perjudicar sistemas de control industrial. Estos ataques se distinguen por su compleja elaboración y dificultad en descartarlos. Representan a una clase emergente de los denominados Advanced Persistent Threats –APT (Amenazas Persistentes Avanzadas).

5) Guerra cibernética

Con el tema de los ataques por motivos políticos viene la cuestión de la guerra cibernética. Estados Unidos ha reconocido el ciber espacio como un nuevo teatro virtual de guerra, junto con la tierra, el agua, el aire y el espacio. En esta situación se hace difícil saber quién lo está atacando o que exactamente está siendo atacado, lo que complica responder de manera oportuna sin herir a sus amigos en lugar de sus enemigos. Fuente: GCN Government Computer News. 

devices to the network. This applies, for example, for the USB connectors. According to experts, there could be an increase in attacks targeting consumer devices through access to corporate resources.

3) Mobile Devices

Consumerism for computing devices is closely linked to mobility factor, and mobile devices are those that come into contact with the workplace. Example: smartphones. The fear is of “malware” cell phone, an increasingly risk due to the rapid increase in the number of these phones, as well as the development of its functionality.

4) Political objectives as targets

According to specialists more cyber espionage will be appreciated, and potentially, cyber-sabotage. Cyber espionage is not new. There were two examples of ultra-sophisticated attacks in 2010, specifically

the Google hack that happened in December 2009 and the discovery of Stuxnet six months later.


In the first case, Google detected an attack on their corporate infrastructure from China and had been the victim of theft of intellectual property. Similar attacks were detected in 150 other corporations in the world. According to McAfee, the attacks would have been generated after some employees of affected companies clicked a link that directed them to a special website that secretly downloaded malicious software. Hackers referred the campaign as “Operation Dawn”.

The second case is a computer worm that can do the same damage as a bomb that destroys an industrial plant or military installation because it acts as a spy and reprograms industrial systems. It is believed that Stuxnet was used to attack Iran’s nuclear facilities. Its impact is significant because any company that uses industrial con-

trol systems can be attacked by the worm causing damage in comparison to that of a physical explosion.

The hack Google aims to obtain sensitive information of high value, while apparently Stuxnet obeys to damage industrial control systems. These attacks are characterized by their complex design and difficulty in discarding them. They represent an emerging class of so-called Advanced Persistent Threats - APT.

5) Cyber war

The issue of cyber warfare comes up with the issue of politically motivated attacks. United States has recognized the cyberspace as a new virtual theater of war along with land, water, air and space. In this situation it is difficult to know who is attacking or what exactly is being attacked, making it difficult to respond in a timely manner without hurting their friends instead of enemies. Source: GCN Government Computer News. 

Configuración del nuevo escenario de guerra

CONFIGURING THE NEW WAR SCENARIO

En los últimos años la ciencia ficción nunca ha estado más cerca de la realidad. Se sabe que en una computadora pueden entrar virus y cookies espía con los consiguientes perjuicios para el propietario de esa herramienta. Pero esto también sucede en organismos oficiales, instituciones básicas de los Gobiernos, o puede, en el sector privado, darse con la anulación de las comunicaciones en aeropuertos, puertos y sistemas de trenes. Esto simplemente significa caos y devastación pero en

condiciones físicas intactas. La pólvora y las sustancias químicas pierden importancia en la era de Internet. En este contexto, los conocedores ya no se preguntan si ocurrirá, sino cuándo ocurrirá la ciber guerra.

Entre tanto, los Gobiernos europeos y el norteamericano han denunciado en varias ocasiones operaciones parecidas de espionaje, con origen en un país asiático. A finales de 2009, la Comisión de Revisión de Economía y Seguridad entre Estados Unidos y China confirmaba en su informe la participación cada vez

In recent years science fiction has never been closer to reality. It is known that a computer can get viruses and spyware cookies with consequent damage to the owner of that tool. But this is also the case in government agencies, basic institutions of governments, or could be also possible in the private sector with consequences such as the cancellation of communications at airports, ports and rail systems. This simply means chaos and devastation but in physically intact conditions. The gunpowder and chemicals become less important in the Internet age. In this context, the connoisseurs no longer wonder if it will happen, but rather when the cyberwarfare will happen.

Meanwhile, the European and U.S. governments have repeatedly denounced similar espionage operations originating from an Asian country. In late 2009, the Committee of Review of Economics and Security between the U.S. and China

más agresiva del Estado Chino en ataques de ciber espionaje contra el Departamento de Defensa de EE.UU.: casi 44.000 sólo en la primera mitad de 2009.

Otra característica es que para hacer la ciber guerra no se necesitan ejércitos, sólo un buen informático puede ser suficiente. Ya en 2002 fue detenido en Inglaterra Gary McKinnon, acusado de haber entrado ilegalmente en 97 computadores del Gobierno de EE.UU., incluidos algunos del Pentágono, la Marina, el Ejército y la NASA. Otro protagonista es Rusia, presunto autor de los fuertes ciber bombardeos contra Estonia, en 2007, y Georgia, en 2008. A veces, el ataque es para colapsar redes, en otros casos para robar secretos, como fue el caso reciente, al parecer, de Corea del Norte.


Así mismo, a finales de 2008, debido a la campaña militar israelí en Gaza, se detectó una gran cantidad de ataques procedentes de países árabes contra páginas

simpatizantes de Israel. En el otro bando, hackers israelíes lanzaban ataques DDoS (bombardeos de denegación de servicio) contra webs de noticias palestinas.

A la fecha, estos sucesos pueden llamarse escaramuzas de ciber guerra, pero al parecer cada vez más estados vienen poniendo a punto sus armadas cibernéticas. Según el estudio de McAfee titulado "Economías desprotegidas: cómo proteger la información vital", elaborado a finales de 2009 a partir de encuestas a más de 800 CEO en el mundo, Israel, Rusia, Estados Unidos, China y Francia encabezan esta nueva carrera armamentística calificado como "ciber guerra fría".

La preocupación mundial por la ciber defensa nació en verano de 2007, cuando Estonia sufrió un fuerte ciber bombardeo supuestamente orquestado por Rusia. Sin embargo, el concepto había nacido muchos años antes, en Estados Unidos, cuando la revista Time se

refirió a ella en una de sus portadas en 1996. Luego de lo sucedido en Estonia en 2007 la OTAN creó, en la capital de dicho país, su Centro de Excelencia Cooperativa para la Ciber Defensa.

Posteriormente, en 2008, Estados Unidos ponía en marcha la Iniciativa Integral de Ciber seguridad Nacional (Comprehensive National Cybersecurity Initiative) que la actual gestión de Obama ha mejorado con la creación de una Ciber comandancia y el nombramiento de un coordinador nacional de ciber seguridad. Ya en 2007, en medio de la lucha contrainsurgente en Irak, EE.UU. ejecutó un ciber ataque autorizado por el presidente Bush contra teléfonos móviles y ordenadores de líderes de Irak, que los usaban para planear atentados con bomba y colgar los videos en Internet. La operación permitió espiar a los iraquíes, despistarles con información falsa y hacerles caer en emboscadas. 

confirmed in its report the participation of increasingly aggressive cyber espionage attacks from the Chinese State against the U.S. Department of Defense, almost only 44,000 in the first half of 2009.

Another characteristic is that armies are not necessary to make the cyber war, just a good computer may be sufficient. In 2002 Gary McKinnon was arrested in England, he was accused of trespassing in 97 U.S. government computers, including some in the Pentagon, Navy, Army and NASA. Another protagonist is Russia suspected of cyber bombing Estonia in 2007 and Georgia in 2008. Sometimes the attack is to collapse networks, in other cases to steal secrets as was the case apparently of North Korea in recent time.


Also, in late 2008 due to the Israeli military campaign in Gaza, a lot of

attacks from Arab countries against Israel supporter pages were detected. On the other side, Israeli hackers launched DDoS attacks (distributed denial of service attack) against Palestinian news sites.

To date, these events can be called cyber skirmishes, but it seems that more and more States are developing their cyber armies. According to McAfee's study entitled "Unprotected economies: how to protect vital information," produced in late 2009 from surveys of more than 800 CEOs in the world, Israel, Russia, USA, China and France are leading this new arms race described as "cyber cold war."

The global concern for cyber defense was born in the summer of 2007, when Estonia suffered a severe cyber bombing supposedly orchestrated by Russia. However, the concept was born many years ago in the United States when Time magazine commented

about it in one of their covers in 1996. After what happened in Estonia in 2007, NATO created in the capital of that country the Centre of Cooperative Excellence for Cyber Defence.

Later, in 2008, the U.S. launched the Comprehensive National Cybersecurity Initiative that Obama's current administration has improved with the creation of a Cyber Command and the appointment of a national cyber security coordinator. In 2007, amid the counterinsurgency in Iraq, the U.S. carried out a cyber attack authorized by President Bush against mobile phones and computers of Iraqi leaders who used them to plan bombings and post videos on the Internet. The operation made possible to spy the Iraqis, confuse them with false information and make them fall into ambushes. 


Estrategias nuevas para nuevas guerras

NEW STRATEGIES FOR NEW WARS

En la ciber guerra ya no es cuestión de contar quién tiene más misiles o más soldados. Los militares saben que en este escenario no sirven las estrategias de siempre. El anonimato difumina al enemigo y la complejidad de las redes hace imposible controlar el alcance y el lugar de una acción ofensiva.

De la experiencia reciente se ha visto que los ataques no vienen de un solo sitio sino de decenas, incluidos los países víctimas. Eran computadoras personales secuestradas por virus. Si los países víctimas quieren defenderse a la vieja usanza, deberían atacar estos ordenadores, que en realidad son víctimas. Es más, al estar muchos en países amigos o en el propio país atacado, éste tendría que dispararse a sí mismo. ¿Qué lógica militar se pondría en práctica?

La vieja táctica de desarmar no aplica en la ciber guerra. Es muy difícil desarmar a otra nación de su capacidad de usar a hackers, ni tampoco puedes desarmar a esos

hackers. Hasta ahora, la eficacia de la ciber guerra no ha sido suficientemente probada. ¿Qué pasaría si, al atacar sistemas de Irán, por la complejidad de las redes se acaba destruyendo sistemas informáticos de empresas extranjeras? Estratégicamente, si se decide inutilizar los suministros de energía, financieros y de telecomunicaciones de un país, no se podría saber certeramente qué se ha hecho y será muy difícil predecir los daños colaterales. 

The cyber war is no longer a matter of counting who has more missiles or more soldiers. The military knows that in this scenario strategies do not always serve. Anonymity fades the enemy and the complexity of networks makes impossible to control the extent and location of offensive action.

from recent experience it was possible to see that the attacks do not come from a single site, but dozens, including those victimized countries. Personal computers

were hijacked by viruses. If countries want to defend victims in the old fashioned way, they should attack these computers which are in fact victims. Moreover, being in many friendly countries or in the attacked country, this would have to shoot itself. What military logic would be implemented?

The old disarming tactic does not apply to cyber warfare either. It is quite difficult to disarm another nation of its ability to use hackers, nor can you disarm these hackers. So far, the effectiveness of cyber war has not been sufficiently tested. What if by attacking Iran's systems, because of the complexity of the networks computer systems of foreign companies were destroyed? Strategically, if you choose to disable the power, financial and telecommunications supplies in a country, you could not know accurately what has been done and it will be very difficult to predict collateral damage.

Los riesgos por zonas / THE RISKS AREAS

En el segundo trimestre de 2010 CISCO, el líder en redes para Internet, difundió un estudio de seguridad que analizó la actividad de las amenazas web estableciendo una distribución del riesgo por países. En sus conclusiones establece que el Este de Europa, Sudamérica y China son las regiones del planeta con mayor actividad de malware.

Al respecto, un 33% del malware generado durante el segundo trimestre de 2010 se localizaba en Europa del Este, mientras Sudamérica representaba el 14% y China concentraba un 11% del total de amenazas. La región Nórdica es la menos expuesta a los ataques basados en la web, con un 4%. Por su parte, el porcentaje de riesgo en Europa, Asia Pacífico y África alcanzaba el 9%, y dentro de Europa los países con mayor concentración de malware basado en la web fueron Reino Unido (21%), España (19%) y Francia (11%).


El estudio de CISCO señaló que "la seguridad es una cuestión que debemos plantearnos a escala global, ya que los ataques se producen normalmente desde países lejanos donde resulta muy difícil su persecución". Es así como el clásico perímetro de seguridad se ha desdibujado: teniendo en cuenta que los trabajadores usan cada vez más las herramientas web 2.0 y que el número de dispositivos móviles conectados a la Red alcanzará los 1.300 millones en tres años, ya "no basta con el clásico firewall y las políticas de seguridad internas para proteger a las empresas, sino que se debe apostar por una seguridad global con arquitecturas que protejan mediante protocolos de encriptación desde el momento en que arranca la conexión".

El peligro de las redes sociales

Por otra parte, aunque el acceso a aplicaciones de redes sociales desde el lugar de trabajo y la conexión de dispositivos personales a la red corporativa pueden mejorar la productividad de los trabajadores, esto

está poniendo en riesgo la seguridad de las empresas. Según un estudio de la consultora estadounidense InsightExpress encargado por CISCO y elaborado mediante encuestas a 500 responsables de seguridad T.I., más de la mitad de los consultados admiten que los empleados utilizan aplicaciones no permitidas, en la mayoría de los casos de redes sociales (68%).

Además, el 41% reconoce que los trabajadores han estado conectando a la red corporativa dispositivos personales no permitidos, y, por esta razón, más de un tercio se han encontrado con fallos de seguridad o pérdida de datos.

A pesar de esta creciente tendencia, más de la mitad (53%) de los responsables de seguridad T.I. afirman que permitirán la conexión de dispositivos personales a la red corporativa (7% ya lo permite), "por lo que hace falta plantearse nuevos mecanismos de seguridad en el acceso e incidir en la educación de los usuarios hacia un uso responsable y seguro", señalaron voceros del estudio. Fuente: Cisco. 

In the second quarter of 2010 CISCO, the leader in networking for the Internet released a study that analyzed the web security threat activity by establishing a distribution of the risk by countries. In its conclusions they state that Eastern Europe, South America and China are the world's regions with most active malware.

In this regard, 33% of malware created during the second quarter of 2010 was located in Eastern Europe, while South America represented 14% and China concentrated 11% of total threats. The Nordic region is less exposed to the web-based attacks with 4%. Meanwhile, the percentage of risk in Europe, Asia Pacific and Africa was estimated to be 9%, and within Europe the countries with the largest concentration of web-based malware


were UK (21%), Spain (19%) and France (11%).

The study of CISCO said that "security is an issue that must be considered globally as attacks usually occur from distant countries where its persecution is very difficult." This is how the traditional security perimeter has become vague, taking into account that workers are increasingly using web 2.0 tools and the number of mobile devices connected to the network will reach 1,300 million in three years, "the classic firewall and security policies to protect domestic companies are no longer enough, we have to opt for a global security with architectures that provide protect by encryption protocols from the moment that the connection starts.

The danger of social networks

Furthermore, although access to social networking applications from the workplace and the connection of personal devices to the corporate network can improve the productivity of workers, this is putting the security of companies at risk. According to the study of a U.S. consulting firm InsightExpress commissioned by Cisco and developed through surveys to 500 IT security managers, more than half of respondents agree that employees use applications that are not allowed, in most cases social networks applications (68%).

In addition, 41% recognize that workers have been connecting not allowed personal devices to the corporate network, and for this reason, more than one third have encountered with security breaches or data loss.

Despite this growing trend, more than half (53%) of those IT security managers state that they will allow connection of personal devices to the corporate network (7% already allows it), "so we need to consider new security mechanisms in the access and influence in educating users for a safe and responsible use" declared spokesmen of the study. Source: Cisco. 



Lo último: Ciber guerra con reglas de comportamiento

TOPIC: CYBER WAR WITH RULES OF BEHAVIOR

La 47ª Conferencia de Seguridad de Munich, celebrada entre el 04 y el 06 de febrero de 2011, si bien estuvo dominada por el tema de las revoluciones en Túnez y, sobre todo, en Egipto, también tocó el tema de la ciber seguridad. En la reunión, en la que asistieron líderes políticos de primer nivel del mundo, el profesor de Harvard Joseph Nye, resumió los desafíos a la seguridad que plantea el ciber espacio en tres materias: ciber crimen, espionaje industrial y terrorismo. Según Nye, la amenaza es real, pero los gobiernos sólo acaban de empezar a lidiar con ella. Para el académico, la situación actual se asemeja a la proliferación de las armas nucleares en los años cincuenta: has-

ta el momento, nuevas armas ofensivas han sido introducidas en Internet, pero los gobiernos nacionales no tienen ni idea de cómo utilizarlas.

Previo a esta reunión, el influyente Instituto EastWest de Nueva York había dado a conocer su propuesta de "traducir las convenciones de Ginebra y La Haya al ciber espacio", lo cual sería desarrollada en la Conferencia, según anunció la BBC de Londres. El mundo necesita "reglas de compromiso" para la ciber guerra que permitan arreglárselas frente al efecto potencialmente devastador de las ciber armas, aseguraron expertos de EEUU y Rusia en la propuesta preparada para dicho evento mundial.

La lógica detrás de la propuesta es que en el entremezclado mundo

The 47th Munich Security Conference, held between February 4 and 6, 2011, though it was dominated by the theme of revolutions in Tunisia and especially in Egypt, it also raised the subject of cyber safety. In the meeting, attended by top level political leaders of the world, Harvard professor Joseph Nye, summarized the challenges to security posed by cyberspace in three areas: cyber crime, industrial espionage and terrorism. According to Nye, the threat is real, but governments are only just beginning to deal with it. For the academician, the current situation resembles the proliferation of nuclear weapons in the fifties, so far, new offensive weapons have been introduced on the Internet, but national governments have no idea how to use them.

Prior to this meeting, the influential New York EastWest Institute had announced its proposal to "translate the Geneva Conventions and the Hague to cyberspace," which would be developed at the Conference, as announced by the BBC of London. The world needs "rules of engagement" for cyber war that allows struggling against the po-


del ciber espacio, se necesita proteger zonas que operan instalaciones como hospitales o escuelas. El borrador del documento también pedía una nueva definición de "Estado nación", con nuevos "territorios" y jugadores en el ciber espacio detrás de los gobiernos, como las corporaciones multinacionales, las organizaciones no gubernamentales o los ciudadanos. La propuesta también incluía que la ambigüedad sobre qué constituye un ciber conflicto está retrasando las políticas internacionales para lidiar con el tema, y que quizá las ideas de "guerra" o "paz" son demasiado simples para la era de Internet cuando el mundo puede encontrarse en una tercera versión no de una guerra sino de "algo diferente".


Otros, sin embargo, creen que hablar de ciber guerra es una exageración, que puede resultar útil para las empresas de defensa que buscan nuevas maneras de hacer dinero. De acuerdo con el estudio "Reduciendo los riesgos sistémicos de la ciber seguridad" elaborado por Peter Sommer, de la London School of Economics, y Ian Brown, del Instituto de

Internet de la Universidad de Oxford, "es improbable que en algún momento se dé una ciber guerra". Ello porque la mayoría de los sistemas de computación están protegidos contra amenazas conocidas, por lo que quienes decidan lanzar ataques

tentially devastating impact of cyber weapons claimed U.S. and Russia experts in the proposal prepared for this global event.

The logic behind the proposal is that in the interspersed world of cyber space you need to protect areas that operate facilities such as hospitals or schools. The draft document also ask for a new definition of "nation state", with new "territories" and players in cyber space behind the governments, such as multinational corporations, NGOs and citizens. The proposal also included that the ambiguity about what constitutes a cyber conflict is delaying international policies to deal with the issue, and perhaps the ideas of "war" or "peace" are too simple for the Internet age when the world can be in a third version not of a war, but "something different".

tendrían que ubicar flancos débiles en los sistemas. El reporte asegura que tras las filtraciones de WikiLeaks y los ataques de hacktivistas se ha exagerado el alcance de sus ofensivas. Fuente: BBC London / Política Exterior.com y otras. 

Others, however, believe that talking about cyber war is an exaggeration, that it can be useful for defense companies seeking new ways to make money. According to the study "Reducing the systemic risks of cyber security" prepared by Peter Sommer of London School of Economics and Ian Brown of Internet Institute at Oxford University, "the appearance of a cyber war is unlikely". This is because most computer systems are protected against known threats so people who decide to launch attacks would have to locate weak points in the systems. The report says that after the leak by Wikileaks and hacktivists attacks the extent of their offensive was exaggerated. Source: BBC London / Política Exterior.com among others. 

¿Y qué es Anonymous? / What is Anonymous?

El fenómeno de Internet Anonymous, es un movimiento internacional de ciber activistas, formado por un número indeterminado de personas que actúan sin identificarse. Declaran luchar contra la censura en Internet y en favor de la transparencia política. El movimiento utiliza la imagen popularizada por el comic "V de Vendetta" (adaptada al cine con el mismo título) como símbolo de identidad. Así mismo, dicen no tener líderes y ser todos iguales, así como se declaran no pertenecer a ningún partido político. La careta representa la figura de Guy Fawkes, conspirador católico inglés del siglo XVII, quien trató de poner una bomba en los cimientos del Parlamento Británico para asesinar al rey Jacobo I en 1605.

Su surgimiento se inicia luego del caso Wikileaks. Se declararon enemigos de los enemigos de Wikileaks y atentaron contra todos los que negaron su apoyo a Julian Assange, el responsable de dicho caso. Sus ataques se basan en denegación de servicios distribuidos (Ddos), el cual consiste en lanzar numerosas peticiones a un servidor que aloja una página web, hasta que el servicio de hosting no puede soportar la sobre carga de peticiones y queda suspendido el servicio.

Anonymous, the Internet phenomenon is an international movement of Internet activists, formed by an indeterminate number of persons acting without identifying themselves. They declare to fight against Internet censorship and in favor of political transparency. The movement uses the popularized image by the comic "V for Vendetta" (made into film with the same title) as a symbol of identity. Also say they have no leaders and be all equal and declare that they do not belong to any political party. The mask represents the figure of Guy Fawkes, English Catholic conspirator of the seventeenth century who tried to place a bomb in the foundations of the British Parliament to assassinate King James I in 1605.

Its emergence began after Wikileaks case. They declared themselves enemies of the enemies of Wikileaks and attacked against every person who refused their support to Julian Assange, the head of that case. Their attacks are based on DDoS which consists of launching numerous requests to a server hosted by a website until the hosting service can not handle the overload of requests and the service is suspended.

Its emergence began after Wikileaks case. They declared themselves enemies of the enemies of Wikileaks and attacked against every person who refused their support to Julian Assange, the head of that case. Their attacks are based on DDoS which consists of launching numerous requests to a server hosted by a website until the hosting service can not handle the overload of requests and the service is suspended.

Its emergence began after Wikileaks case. They declared themselves enemies of the enemies of Wikileaks and attacked against every person who refused their support to Julian Assange, the head of that case. Their attacks are based on DDoS which consists of launching numerous requests to a server hosted by a website until the hosting service can not handle the overload of requests and the service is suspended.



Los Programas de Operador Económico Autorizado (OEA) en Asia

AUTHORIZED ECONOMIC OPERATOR (AEO) PROGRAMS IN ASIA

De los 176 países miembros de la Organización Mundial de Aduanas – OMA, hasta marzo del presente año, 164 de ellos han firmado una declaración de intención con dicha entidad comprometiéndose a poner en aplicación el Marco Normativo SAFE para asegurar y facilitar el comercio mundial. Hasta mayo de 2010 existían 30 programas distintos en 56 países (la diferencia se debe a que 27 Estados Miembros de la UE tienen un programa único y uniforme). También hay otros países que ya han establecido o prevén establecer sus programas.

En general, según la OMA todos los programas se dividen en tres tipos: programas OEA operativos; programas OEA previstos para iniciar en un futuro próximo y programas de observancia aduanera. Si bien estos últimos no constituyen programas OEA desde el punto de vista técnico, se les pueden considerar como un paso inicial hacia el establecimiento de uno. A partir de esta edición se hará entrega de información básica sobre los programas OEA y los programas de observancia aduanera, con una recopilación que incluye también una breve descripción de los procedimientos de autorización

From 176 member countries of the World Customs Organisation - WCO, 164 of them have signed a statement of intent with this entity until March of this year committing to give effect to the SAFE Framework of Standards to Secure and facilitate global trade. Until May 2010 there were 30 different programs in 56 countries (the difference is that 27 EU Member States have a unique program and uniform). There are other countries that have established or plan to establish their programs.

In general, according to the OMA all programs are divided into three types: AEO operational programs, AEO programs intended to start in the near future and customs compliance programs. Although the latter do not constitute AEO programs from the technical point of view, they can be considered as an initial step toward establishing one. From this edition basic information about the AEO program and customs compliance programs with a collection that also includes a brief description of the procedures

de los OEA y de las ventajas que ofrece. Iniciaremos con países del Asia.

Hasta el 2010 la región de Asia Pacífico ha puesto en marcha seis programas OEA (China, Japón, Corea, Malasia, Nueva Zelanda, y Singapur). Estos países, como todo aquel interesado en implementar este programa, estudian el Marco Normativo SAFE de la OMA y aprenden de la experiencia de otros países que ya lo establecieron, así como diversos países prestan asistencia en materia de fortalecimiento de capacidades a escala regional y bilateral.

Así mismo, no hay que perder de vista el reconocimiento mutuo del programa OEA, un objetivo importante para las Administraciones de Aduanas con miras a asegurar y facilitar en mayor medida el comercio mundial. Como se recuerda, esto implica que el gobierno de un país reconozca formalmente el programa OEA del gobierno de otro país, y consecuentemente otorgue ventajas a las empresas OEA de dicho país. En un principio, el reconoci-

miento mutuo de los programas de OEA es bilateral, sin embargo cabe esperar que se amplíe para abarcar el nivel sub-regional y regional.

El reconocimiento mutuo en el marco del OEA es de suma importancia para las empresas, pues lograr la compatibilidad y el reconocimiento mutuo de los programas OEA supone fundamentalmente la armonización y simplificación de los procedimientos aduaneros que contribuirán a conseguir el objetivo de la facilitación del comercio y la seguridad de la cadena logística.

Corea

En Corea el nombre del programa es OEA (es de observancia aduanera) y fue iniciado en abril de 2009 para atender los campos de exportación e importación. Trabaja con exportadores, importadores, agentes aduaneros, agentes de carga, transportistas (transportistas de depósito aduanero), transportistas marítimos/aéreos, manipuladores de carga terrestre, almacenistas (operadores de depósitos aduaneros

incluyendo, terminal portuario). Hasta mayo de 2010 había 41 certificados de 26 empresas.

En legislación existe la revisión de la legislación aduanera hecha en enero de 2008, el Decreto de aplicación de la legislación aduanera correspondiente a febrero de 2009 y la Norma de aplicación de los OEA en abril de 2009. Se sabe que entre los planes previstos figura ampliar continuamente las ventajas para los OEA mediante la investigación y las consultas con el sector privado. Hasta diciembre pasado existían 242 solicitantes para OEA.

Entre los requisitos generales para ingresar al programa están: Observancia jurídica; Control Interno; Solvencia financiera; Gestión de la seguridad. Para la acreditación se necesita la presentación de la solicitud (autoevaluación, evaluación de riesgos, declaración sobre gestión de OEA, responsable interno de la condición de OEA); Auditoría (documental; validación en el sitio); Distribución del Certificado OEA, teniendo en cuenta la observan-

for authorization of the AEO and the benefits it offers will be given. We will begin with countries in Asia.

By 2010 the Asia Pacific region has launched six AEO programs (China, Japan, Korea, Malaysia, New Zealand, and Singapore). These countries, as anyone interested in implementing this program, study the SAFE Framework of the WCO and learn from the experience of other countries that already established it, and various countries provide assistance regarding strengthening of capacities at regional and bilateral levels.

Also, we must not lose sight of the mutual recognition of AEO program, an important goal for Customs administrations with a view to ensure and further facilitate global trade. As was mentioned, this implies that the government of a country formally recognizes the AEO program of the government of another country, and consequently gives benefits to AEO companies of that country. At first, the mutual recognition of AEO programs is bilateral, but is expected to be ex-

tended to cover the sub-regional and regional levels.

Mutual recognition in the AEO framework is of utmost importance for companies because to achieve compatibility and mutual recognition of AEO programs essentially involves the harmonization and simplification of customs procedures which contribute to achieving the goal of trade facilitation and logistical chain security.

Korea

In Korea the name of the program is AEO (customs compliance) and was initiated in April 2009 to address the areas of export and import. It works with exporters, importers, customs brokers, freight forwarders, carriers (customs warehousing carriers), ocean / air carriers, ground freight handlers, warehouse worker (including customs warehouse and port terminal operators). From 26 companies there were 41 certified until May 2010.

There is a revision of customs legislation in legislation made in January 2008, the Enforcement Decree of the

customs legislation relating to February 2009 and the application norm of AEO in April 2009. It is known that among the set out plans the constant expansion of the advantages for the AEO through research and consultations with the private sector appears. Until last December there were 242 applicants for AEO.

Among the general requirements for entering the program we have: Legal Compliance, Internal Control, financial solvency, management of security. For accreditation the submission of the application is necessary (self-assessment, risk assessment, statement about AEO management, internal responsible for AEO), Auditing (documentary, validation on the site); Distribution of AEO certificate taking into account the compliance: Class AA (90% or more), Class A (85% or more), or request for improvement measures; Granting of the AEO certificate (valid for 03 years, 06 months before maturity renewal) and designation of a coordinator for the user, self-management / a posteriori monitoring; assessment

cia: clase AA (90% o más); clase A (85% o más), o solicitud de medidas de mejora; Concesión del certificado OEA (válido para 03 años, renovación 06 meses antes de su vencimiento) y designación de un coordinador para el usuario; Autogestión/seguimiento a posteriori; Evaluación de la observancia (mediante solicitud o selección): ajuste de la clase (A, AA o AAA en el caso de más del 95% de observancia; o solicitud de medidas de mejora); Autogestión/seguimiento a posteriori.

Las ventajas generales comprenden: inspección simplificada y menos inspecciones físicas, procedimientos aduaneros simplificados, menor carga financiera, etc. según el tipo de operador (importador, exportador, etc.). Las ventajas acordadas al mismo tipo de operadores se diferencian igualmente según el nivel de OEA (A, AA, AAA) de una empresa.

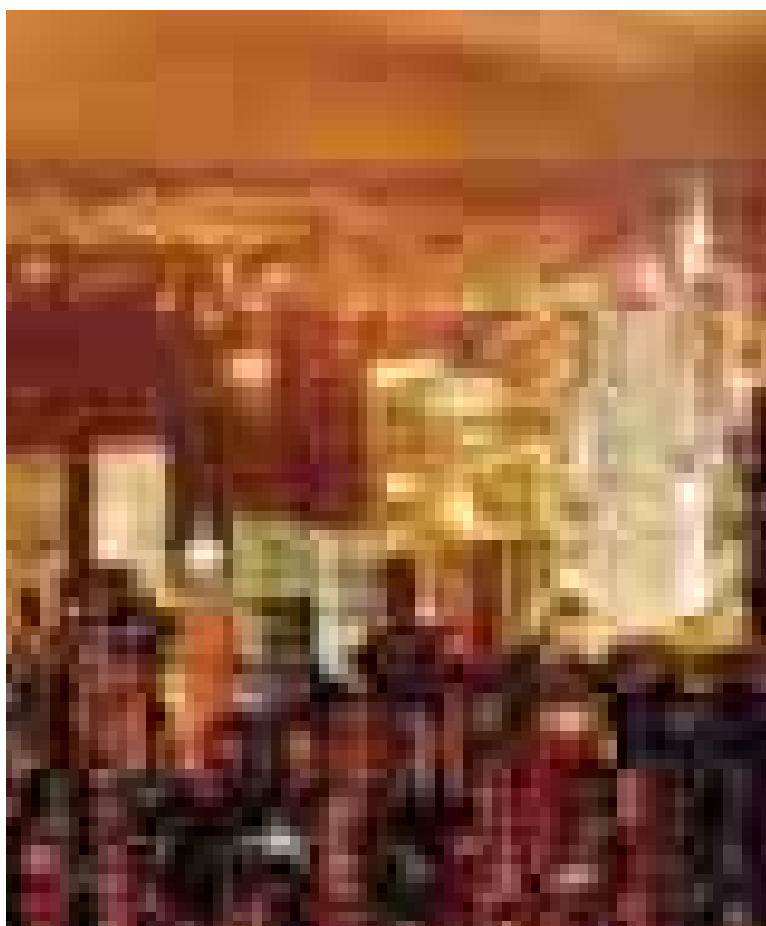
Menos inspecciones físicas en el proceso de expo/impo.; inspección en el lugar elegido por el importador; menos requisitos en cuanto a la presentación de documentos suplementarios tras la declaración electrónica; exención de la auditoría fiscal previa a la aceptación de la declaración de importación así como del control a posteriori; facilidades para el despacho aduanero, etc. en puertos (aeropuertos) internacionales a conveniencia del representante de un OEA; autogestión a posteriori de las importaciones que se supone deben estar bajo control aduanero de conformidad con la ley aduanera para la aplicación de un derecho arancelario determinado, la reducción o de la exención de los derechos aduaneros o del pago a plazos de los derechos.

Existe también carga financiera menor por la exención de la obligación de prestar una garantía a efectos del despacho; el pago mensual de derechos e impuestos aduaneros, así como reducción de las sanciones en caso de infracción de las disposiciones en materia aduanera.

Malasia

El nombre del programa en Malasia es OEA expresamente y empezó en enero del 2010. Se aplica para exportaciones e importaciones. Hasta marzo del 2010 tenía procesando 39 solicitudes y en el campo legislativo tiene instrucciones y directivas administrativas. Entre sus planes tenía previsto el reconocimiento mutuo con Japón.

Los requisitos para la acreditación incluyen: tener un historial de 03 años de operaciones en el país; historial de observancia de los requisitos legales y normativos de la Aduana; ausencia de retrasos en los pagos de impuestos a la Aduana; permiso de seguridad previo de la inteligencia aduanera y otros organismos públicos como la Policía, Inmigración, y otros, que se ocupan de los procedimientos relacionados con el despacho aduanero; control interno adecuado (seguimiento de auditoría) de todas las importaciones, exportaciones y movimientos



of compliance (by request or selection): adjustment of the class (A, AA or AAA in the case of more than 95% of compliance, or application of improvement measures) , Self-management / a posteriori monitoring.

The overall benefits include: simplified inspection and less physical inspections, simplified customs procedures, less financial burden, and so on according to the type of operator (importer, exporter, etc.). The advantages granted to the same type of operators are also differentiated by the level of AEO (A, AA, AAA) of a company.

Fewer physical inspections in the process of exportation / importation; inspection at the place chosen by the importer, less requirements on the submission of additional documents after the electronic declaration; exemption from the tax audit prior to the acceptance of the import declaration and a posteriori control, facilities for customs clearance, etc. in international ports (airports) for the convenience of an AEO representative, a posteriori self-management imports that are supposed under the Customs control in accordance to Customs Act to implement a determined customs tariff, the reduction or exemption of customs duties or installments payment of duties.

There is also a minor financial burden exemption for the obligation to provide security for the purposes of the office, the monthly payment of customs duties and taxes as well as reducing the penalties for violations of customs provisions.

de mercancías; programa interno de observancia de la seguridad y aspectos sobre seguridad; efectuar el pago de derechos mediante transferencia de fondos electrónica; el personal relacionado a las operaciones aduaneras y sus agentes aduaneros, precisan formación obligatoria en materia de procedimientos aduaneros y la aprobación de la Aduana; las empresas consideradas de nivel alto de riesgo deben comunicarse con la Aduana para ver su caso.

Las empresas finalmente cuentan como ventaja con: despacho aduanero con un mínimo de datos y procedimientos simplificados; despacho rápido y eficaz; reclamaciones de drawback simplificadas fundamentadas en principios de auto contabilidad y; pagos aplazados de derechos.

Nueva Zelanda

El programa de observancia aduanera en este país se denomina "Régimen de colaboración para la seguridad de las exportaciones

(SES)" y está vigente desde el 2004 solamente para el sector exportador. El programa opera desde el punto de embalaje hasta el punto de carga. Como parte del esquema, los exportadores son también responsables de sus operadores terceros y su logística incluyendo a transportistas y agentes. El número de operadores inscritos hasta marzo del 2010 era de 122 miembros. En el plano legal se adaptó la legislación para asegurar las mercancías desde el punto de embalaje hasta el punto de carga para su exportación. Entre los planes del gobierno figura el examen en curso del planteamiento respecto a los OEA y el examen de las ventajas de ampliar los ARM (Acuerdos de Reconocimiento Mutuo) a otros socios.

Entre las condiciones de acreditación figuran: el esquema tiene un proceso de validación anterior y posterior que realizan grupos independientes y distintos dentro de la Administración de Aduanas del país; los exportadores son responsables de todos los subcontratistas

conforme con los términos de su acuerdo; se prevé que la Aduana intervenga o inspeccione las mercancías exportadas en el marco del SES a partir de la fijación del precinto aduanero en el contenedor, en cualquier punto de la cadena logística nacional, independientemente de si las mercancías se encuentran o no en una zona controlada por la Aduana; si no existe una autorización de exportación (Customs Export Delivery Order), los operadores portuarios no tienen permiso para cargar el contenedor y; notificación electrónica de las declaraciones de exportación obligatoria.

Como ventajas el sistema ofrece: seguridad de la cadena de suministro desde el punto de embalaje hasta el puerto de carga para su exportación; mejora de la previsibilidad de la cadena de suministro con el fin de reducir la intervención de las autoridades públicas, de forma que existan menos interrupciones y se disminuyan los gastos relacionados con la observancia; observancia de las normas de seguridad en cuanto a los contratos

Malaysia

The name of the program in Malaysia is expressly AEO and started in January 2010. It applies to exports and imports. Until March 2010 it had 39 applications processing and in the legislative field it has instructions and administrative policies. There was the mutual recognition with Japan among its plans.

The accreditation requirements include: having a history of 03 years of operations in the country, record of compliance with legal and regulatory requirements of Customs, absence of delayed tax payments to Customs, security clearance prior to the customs and other intelligence agencies such as Police, Immigration, and others that deal with procedures related to customs clearance, adequate internal control (audit trail) of all imports, exports and movement of goods, internal compliance program of security and security aspects, make the payment of fees by electronic funds transfer, personnel related to customs

operations and customs agents require compulsory training of customs procedures and the approval of the Customs, and the companies considered high level of risk should contact Customs to see your case.

The companies finally have the advantage of: customs clearance with minimum data and simplified procedures, rapid clearance and effective and implied drawback claims based on principles of self accounting and, deferred payment of duties.

New Zealand

The customs enforcement program in this country is called "collaborative program for the safety of exports (SES)" and is in force since 2004 only for the export sector. The program operates from the point of packing up the loading point. As part of the scheme, exporters are also responsible for their third party and logistics operators including carriers and agents. The number of registered operators until March 2010

was 122 members. In legal terms the law was adapted to ensure the goods from the point of packaging to the point of loading for its export. Among the government's plans there is the ongoing review of approaches regarding the AEO and the review of the benefits of extending the MRA (Mutual Recognition Agreements) to other members.

Among the conditions of accreditation we find: the scheme has a previous and subsequent validation process that distinct and independent groups perform within the Customs Administration of the country. Exporters are responsible for all subcontractors in accordance with the terms of their agreement. It is expected that Customs intervene or inspect the goods exported under the SES from the fixing of customs seals on the container at any point in the national logistical chain, regardless of whether the goods are or not in an area controlled by Customs. If there is an export authorization (Customs Export



de suministro de los importadores establecidos en el extranjero y comprometidos con la seguridad de la cadena de suministro; ventajas en el despacho fronterizo concedidas a aquellas Administraciones con las cuales se ha concertado un Acuerdo de Reconocimiento Mutuo; posibilidad de reducir las interrupciones del comercio durante un suceso relacionado con la seguridad, dado que la seguridad de la cadena de suministro está asegurada; observancia de las normas de la OMA aceptadas a escala mundial; tarifas reducidas para la presentación de todas las declaraciones de exportación; evaluación independiente de los planes y procesos de seguridad de los exportadores; aumento de la concienciación de la empresa en cuestiones de seguridad y mejora de los procesos.

Singapur

El programa de Singapur se llama "Colaboración para la seguridad del comercio (STP)" y empe-

Delivery Order), the port operators are not allowed to load the container and, electronic reporting of export declarations is mandatory.

The system offers as advantages: security of supply chain from the packing point to the port of loading for its export, improve the predictability of the supply chain to reduce the role of public authorities, so that there are fewer interruptions and reduce costs related to compliance, enforcement of safety standards in terms of supply contracts of foreign-based importers and committed to the security of the supply chain; benefits in the border clearance granted to those administrations with which a Mutual Recognition Agreement has been concluded; possibility of reducing the disruption of trade during an incident involving security since security of supply chain is assured; compliance of worldwide accepted standards of the OMA; reduced rates for the presentation of all export declarations,

independent assessment of security plans and processes of exporters, increasing awareness of the company in matters of safety and process improvement.

Singapore

The program in Singapore is called "Cooperation for commerce security (STP)" and began in May 2007 (as STP), while in October 2008 (STP+) was started, which constitute two levels: STP and STP-Plus. This program is commerce security type and its scope covers exports and imports, and is open to all operators in the supply chain located in Singapore. Until April 2010, there were 44 members (20 STP enterprises and STP-Plus 24 enterprises). This group represents more than 9% of the value of exports from Singapore. This scheme has no AEO specific legislation and their plans are to conclude and implement the Mutual Recognition Agreement (MRA) over the next two years.

In accordance with the guideli-

El programa OEA Chino

El programa chino es de observancia aduanera y se denomina "Gestión por categorías de las empresas" (Classified Management of Enterprises / AA Class Enterprises) y se inició en abril de 2008. Su campo de aplicación son las exportaciones e importaciones y está abierta para los exportadores, importadores y agentes de aduana. En general, la aduana china divide a las empresas en 5 categorías: AA, A, B, C y D. Lo hace a través de una evaluación cuyo resultado hace público. Bajo el principio de "cumplimiento por facilitación" la aduana aplica medidas diferenciadas para las empresas según su categoría.

Hasta el 2010 legislativamente había un proceso de revisión por parte de la Aduana china de la Norma sobre la Gestión por categoría de las empresas. Entre los planes previstos se contemplaba desarrollar el concepto de OEA y redactar la legislación para otros participantes de la cadena de suministro, tales como operadores de puertos, agentes de aduana, transportistas, almacenes. Hasta marzo de dicho año China contaba con 1577 empresas AA.

Entre los elementos para la acreditación exigidos por el programa se encuentran como requisitos generales: ser un operador de clase A durante más de un año; en lo que a importadores y exportadores se refiere, el volumen de importación y exportación del año anterior deberá haber sido superior a 30 millones de dólares de EEUU (10 millones para las empresas del sector central y occidental); en calidad de agente, haber presentado el año anterior más de 20.000 (5.000 para las empresas del sector central y occidental) formularios de declaración de importación y exportación o documentos de entrada y salida; respecto a los controles aduaneros de validación y de auditorías deberán probar que se han cumplido los requisitos en cuanto

a gestión aduanera, las operaciones y la dirección de la empresa; y por último presentar el informe de operaciones y gestión así como el de la auditoría correspondiente al año anterior.

La acreditación propiamente consiste en: 1) Autoevaluación; 2) Presentación de la solicitud; 3) Comprobación de la información a nivel interno y externo; 4) Control de validación (visita a los locales); 5) Aprobación por parte de la Oficina central de la Aduana; 6) Emisión de un certificado; 7) Comprobación periódica de los documentos y control de validación a posteriori basado en la evaluación de riesgos.

Entre las ventajas para las empresas se cuenta: la creación de un clima de confianza; designación de funcionarios especiales para ayudar a las empresas a coordinar y resolver cuestiones aduaneras; aplicación de un nivel de control mínimo para las mercancías relacionadas con las importaciones y exportaciones; presentación de declaraciones en el lugar del registro; los procedimientos de inspección y despacho se realizan en los puertos; los trámites de Inspección y despacho se realizan en los locales de la empresa; designación de un equipo especial que realice las inspecciones en los locales; prioridad en la gestión de los trámites urgentes de despacho aduanero fuera del horario laboral y durante las vacaciones; prioridad en la gestión de los trámites comerciales, como la introducción de datos, su modificación y la presentación de informes a efectos de verificación; y prioridad acordada al registro de las declaraciones.

En mayo pasado, Estados Unidos y China firmaron un acuerdo de cooperación para mejorar la seguridad de la cadena de suministro entre ambas economías. El acuerdo cubre la validación conjunta de procedimientos de los programas C-TPAT estadounidense y el OEA chino.

zó en mayo del 2007 (como STP), mientras que en octubre del 2008 inició el (STP+), lo que constituyen dos niveles: STP y STP-Plus. Este programa es de tipo de seguridad de comercio y su campo de acción cubre las exportaciones e importaciones, así como está dirigido a todos los operadores de la cadena de suministro ubicados en Singapur. Hasta abril de 2010, existían 44 miembros (20 empresas de STP y 24 empresas de STP-Plus). Este grupo representa más del 9% del valor de la exportación de Singapur. Este esquema no tiene una legislación específica OEA y entre sus planes

se encuentra concluir y poner en funcionamiento el Acuerdo de Reconocimiento Mutuo (ARM) en los próximos dos años.

De conformidad con las directrices y criterios del STP, las empresas deben: disponer de un sistema de gestión de la seguridad; realizar una evaluación de riesgos de sus operaciones comerciales; aplicar las medidas de seguridad relacionados a los ocho elementos contemplados en el programa STP (elementos compatibles con el Marco Normativo SAFE de la OMA).

Para la acreditación es necesario: presentar el formulario de solicitud,

el perfil de seguridad y los documentos justificativos; visita de validación en todos los locales de la empresa realizada por la Aduana; certificación que garantiza que la empresa cumple los requisitos establecidos en las Directrices STP o los Criterios STP; para la obtención de la condición de STP, la empresa debe cumplir los requisitos establecidos en las Directrices STP; para la obtención de la condición de STP-Plus, la empresa debe cumplir los requisitos mínimos establecidos en los Criterios de STP.

Los beneficios a obtener son: menor posibilidad de inspección de las mercancías; garantía de calidad

The Chinese AEO program

The Chinese program is enforcement of customs and is called "Classified Management of Enterprises / Enterprises Class AA" and began in April 2008. Its scope is exports and imports and is open to exporters, importers and customs brokers. In general, China Customs divides companies into 5 categories: AA, A, B, C and D. It does this through an evaluation which results are published. Under the principle of "compliance by facilitation" customs applies measures for different companies according to their category.

By 2010, there was a review process legislatively by China Customs of the Standard about companies Management by category. Among the envisaged plans it was contemplated to develop the concept of the AEO and drafting legislation to other participants in the supply chain, such as port operators, customs brokers, shippers, warehouses. Until March of this year, China had 1577 AA companies.

Among the elements for accreditation required by the program we can find as general requirements: to be a Class A operator for more than a year regarding importers and exporters, the import and export volume last year must have been more than 30 million U.S. dollars (10 million for companies in the central and western sectors) as agent, the presentation of more than 20,000 (5000 for companies in central and western sectors) import declaration forms and exports and input and output documents last year; regarding customs controls and validation audits they must prove that they have met the requirements for customs management,

operations and management of the company, and finally present the report of operations and management and the audit for the previous year.

The accreditation itself consists of: 1) Self-assessment, 2) Submission of application, 3) Checking of the information internally and externally; 4) Validation Control (visit to the premises), 5) Approval by the Central Bureau of Customs, 6) Issuance of a certificate; 7) Regular checking of documents and a posteriori validation control based on risk assessment.

The benefits for businesses include: creating a climate of trust, appointment of special officers to assist companies to coordinate and resolve customs issues, application of a minimum level of control for goods related to imports and exports; presentation of declarations in the place of registration, the inspection and clearance procedures are done in ports, the inspection and clearance procedures are performed on the premises of the company; appointing a special team to conduct inspections in the premises; priority in the management of urgent customs clearance procedures after hours and during holidays; priority in the management of commercial transactions such as data entry, modification and reporting for verification, and priority given to registration of statements.

Last May, the U.S. and China signed a cooperation agreement to improve the security of the supply chain between the two economies. The agreement covers the joint validation of procedures of the American C-TPAT and Chinese AEO programs.

y mejora la imagen de las empresas (reconocimiento como empresa de bajo riesgo); menor número de inspecciones o despacho agilizado si la certificación de la condición es también reconocida por países extranjeros; designación de gestores de cuentas; reconocimiento automático como expedidor conocido (KC) de conformidad con el Regulated Cargo Agent Regime (RCAR); ventajas en el ámbito de la facilitación del comercio a saber, reducción del importe establecido de la garantía bancaria, si procede; aquellas empresas que deseen mejorar sus capacidades

and criteria of the STP, companies must: have a system of security management, carry out a risk assessment of their business operations, and implement safety measures relating to the eight factors listed in the STP program (compatible elements with the SAFE Framework of the WCO).

For accreditation is necessary to: submit the application form, the safety profile and supporting documents; validation visit by Customs to all the premises of the company; certification that ensures that the company meets the requirements of the STP

Guidelines or STP criteria, for obtaining the status of STP, the company must meet the requirements of the STP Guidelines; for obtaining the STP-Plus status the company must meet minimum requirements set out in the STP criteria.

The benefits you get are: less possibility of goods inspection, quality assurance and enhances the image of the companies (recognition as low-risk company), fewer inspections and rapid clearance certificate if the certification of the condition is also recognized by foreign countries; nomination of account managers;

El programa OEA en Japón / The AEO program in Japan

En Japón, el Programa de importadores autorizados (sin el componente de la seguridad) también es de observancia aduanera y se inicia en marzo del 2001. En 2006 aparece el Programa para exportadores (incluyendo el componente de seguridad) y se añade el componente de seguridad al Programa de importadores autorizados. En abril de 2007 se unifica el sistema en un Marco para el programa OEA. Con ello, el campo de aplicación son las importaciones y las exportaciones.

En el sistema japonés participan los importadores, exportadores, operadores logísticos (transportistas, agentes de carga, compañías marítimas, compañías aéreas), agentes de aduanas, almacenistas, fabricantes. Hasta abril de 2010, el número de operadores inscritos era de 406 (73 importadores, 233 exportadores, 23 agentes, 76 almacenistas, un operador logístico). Existe legislación y reglamentos aduaneros modificados en 2001, 2006, 2007, 2008 y 2009. Así mismo, figuran un Orden Ministerial, Decreto Ministerial y Orden del DG de la Aduana. Desde octubre 2008 este país tiene un Acuerdo de Reconocimiento Mutuo con Nueva Zelanda.

Para acreditarse las empresas deben tener un historial de observancia; sistema informático; integridad financiera; y un programa de observancia. Además existen requisitos especiales para cada categoría de operador. En el proceso de admisión los pasos consisten en: consulta previa (voluntaria); autoevaluación; examen de los documentos y auditoría in situ condición de OEA; control posterior a la autorización. Si hay algún problema se impone un "Orden administrativa para su mejora". Si no se producen mejoras la condición de OEA queda revocada.


Las ventajas reservadas para las empresas OEA están referidas a: reducción de los gastos logísticos (posibilidad de presentar declaraciones sin obligación de estar presente) y de los tiempos de espera; menor control aduanero y procedimientos aduaneros simplificados; los OEA pueden comprobar por sí mismos su nivel de observancia interna; pago único general de las declaraciones una vez al mes; supresión del cargo mensual por los almacenes aduaneros; permisos más largos para los emplazamientos de los almacenistas; menor frecuencia de controles aduaneros para los almacenistas.

In Japan, the program of authorized importers (without the security component) is also customs enforcement and began in March 2001. In 2006, the program appears to exporters (including the security component) and the security component was added to the program of authorized importers. In April 2007 the system in a unified framework for the AEO program. With this, the field of application is imports and exports.


In the Japanese system importers, exporters, logistics operators (carriers, freight forwarders, shipping companies, and airlines), customs brokers, wholesalers and manufacturers participate. Until April 2010, the number of players registered was 406 (73 importers, 233 exporters, 23 agents, 76 warehouse workers, and a logistics operator). There are a legislation and customs regulations amended in 2001, 2006, 2007, 2008 and 2009. Also, there is a Ministerial Order, Ministerial Decree and Order of the DG of Customs. Since October 2008 this country has a Mutual Recognition Agreement with New Zealand.

To be accredited companies must have a record of compliance, computer system, financial integrity, and an enforcement program. There are also special requirements for each category of operator. The admissions process steps include: prior consultation (voluntary), self-assessment, review of documents and on-site audit condition of AEO, control after the authorization. If there is a problem an Administrative Order for its improvement is imposed. If there are no improvements the AEO status is revoked.

The benefits reserved for AEO companies concern: reducing logistics costs (opportunity to make statements without obligation to be present) and waiting times, lower customs control and simplified customs procedures, the AEO can see for themselves their domestic enforcement level, general single payment of the declarations once a month, removal of monthly fee of customs warehouses, longer leases for locations of the warehouse workers, less frequently customs checks for stockists.

en cuanto a la seguridad de la cadena de suministro pueden obtener financiación o asistencia a través de esquemas de asistencia para la formación y de los programas de desarrollo ofrecidos por otros organismos públicos como el Consejo para el Desarrollo Económico (EDB) y SPRING Singapore. Fuente: OMA / Aduana de Japón / APEC / Aduana de China. 

automatic recognition as a known consignor (KC) in accordance with the Regulated Cargo Agent Regime (RCAR); advantages in the area of trade facilitation, namely reduction in the established amount of the bank guarantee as the case may be, those companies wishing to improve their capabi-

lities in the security of the supply chain can obtain financing or assistance through schemes of assistance for the training and development programs offered by other agencies such as the Council for Economic Development (EDB) and SPRING Singapore. Source: WCO / Japan Customs / APEC / China Customs. 

El programa OEA en la Unión Europea: Una mirada general

THE AEO PROGRAM IN THE EU: AN OVERVIEW

Como se sabe, la Unión Europea (UE) es el mayor bloque comercial del mundo y tiene entre sus estados miembros a algunos de los países más competitivos del mundo, así como participan algunos estados cuyas economías aún se encuentran en proceso de maduración.

Como es de suponer, con diferentes idiomas, culturas y desarrollos económicos, la instauración de un único programa Operador Económico Autorizado (OEA) no ha sido un proceso fácil. Sin embargo, en enero de 2008 este bloque de países puso en vigencia las Directrices de la UE para Programas OEA de Estados Miembros.

Cada país tuvo que desarrollar su programa OEA y como principio básico las respectivas autoridades aduaneras consideraron programas nacionales activos que reconocían a empresas participantes. Es el caso de algunos países como el Reino Unido y Suecia, que ya contaban con programas comerciales compatibles bastante desarrollados. Otros todavía no habían incorporado este enfoque a la gestión de riesgos.

En general, la metodología de la UE consistió primero en desarrollar directrices y luego probarlas en el sector privado. La metodología incorpora solicitudes para asegurar el cumplimiento de medidas arancelarias y no arancelarias y de medidas de seguridad para prevenir atentados terroristas. En este sentido, la metodología de la UE califica a las empresas OEA en tres niveles:

-Simplificación aduanera. Para operadores económicos que cumplen con los criterios de cumplimiento aduanero, normas de registros contables y solvencia financiera. El portador del certificado tiene derecho al acceso a la simplificación aduanera; menos controles físicos y controles basados en documentos; tratamiento prioritario de ser seleccionado para efectos de control; y la posibilidad de solicitar un lugar específico para dicho control.

-Protección y seguridad. Para operadores económicos que cumplen con los criterios de cumplimiento aduanero, normas adecuadas de gestión de registros, solvencia financiera y mantenimiento de normas adecuadas de protección y seguridad.

-Combinación de simplificación aduanera, protección y seguridad. Para operadores económicos que cumplen con los criterios de cumplimiento aduanero, normas adecuadas de gestión de registros, solvencia financiera y mantenimiento de normas adecuadas de protección y seguridad y aspiran a todos los beneficios OEA.

El enfoque de la UE hacia el desarrollo de directrices OEA de la Comisión Europea consideró diversos elementos y pasos de los cuales podrían aprender otros países (o bloques) en el desarrollo de sus propios programas OEA:

- Incorporar programas existentes que reconocen a comerciantes cumplidores.
- Determinar los objetivos del programa, en particular los objetivos del sector privado.

As is known, the European Union (EU) is the world's largest trading bloc and has some of the world's most competitive countries among its member states, and involved some states whose economies are still in the process of maturation.

As expected, with different languages, cultures and economic developments, the establishment of a single AEO program has not been an easy process. However, in January 2008, this bloc has put into effect the EU Guidelines for AEO Programs of member states.

Each country had to develop its AEO program as a basic principle and the respective customs authorities considered active national programs that recognized member companies. This is the case in some countries like the UK and Sweden, which already had compatible well developed commercial programs. Others had not yet incorporated this approach to risk management.

In general, the EU methodology was first to develop guidelines and then tested in the private sector. The methodology incorporates applications to ensure the compliance of tariff non-tariff measures and security measures to prevent terrorist attacks. In this sense the EU methodology qualifies AEO companies at three levels:

- Customs simplification. For economic operators who meet customs compliance criteria, standards of accounting records and financial solvency. The certificate holder is entitled to access to customs simplification, less physical ins-

- Incorporar al grado máximo normas de seguridad como indicadores de probabilidad de cumplimiento con medidas arancelarias y no arancelarias, particularmente aquellos cuyo objetivo es la reducción de riesgos en la cadena de suministro. En el caso peruano el ejemplo inconfundible es BASC, programa que cuenta con el registro de terceros a sus normas.
- Incorporar toda la cadena de suministro como miembros para elegibilidad.
- Aplicar el concepto de proceso completo de debida diligencia, que requiere que los participantes verifiquen los factores de riesgo de su propia cadena de suministro.
- Realizar una prueba piloto del enfoque con empresas seleccionadas antes de finalizar las directrices.
- Publicar un manual de instrucciones que pueden seguir las empresas en preparación para solicitar el reconocimiento como OEA.
- Reconocer a las pequeñas y medianas empresas como una categoría especial.

Tomando como base programas preexistentes

El programa OEA en la Unión Europea tiene la ventaja de contar con modelos de otras administraciones de aduanas que implementaron programas anteriores y programas comerciales compatibles de estados miembros. Es el caso del programa Sistema Cliente Holandés que se centraba en evaluar la fiabilidad de las empresas tomando como base la forma en que administran sus rutinas aduaneras desde una perspectiva de análisis de riesgos.

Este programa, que luego serviría como base para el programa OEA holandés, fue principalmente utilizado internamente por la aduana holandesa en vez de establecer un contacto con las empresas. Se desarrolló sobre la base de dos conceptos fundamentales: que los bienes no constituyan un fraude y que el cumplimiento de las normas

protecciones and document-based controls, priority treatment to be selected for control purposes and the possibility of requesting a specific place for such control.

- *Protection and security. For economic operators who meet the criteria of customs compliance, appropriate standards for records management, financial soundness and maintenance of adequate standards of safety and security.*
- *Combination of customs simplification and safety and security. For economic operators that meet the criteria of customs compliance, appropriate standards for records management, financial soundness and maintenance of adequate standards of safety and security and aspire to all AEO benefits.*

The EU's approach towards the development of AEO guidelines of the European Commission considered various elements and steps which other countries could learn from (or blocks) in developing their own AEO programs

- *Incorporate recognize existing programs that recognize compliant traders.*
- *Determine the objectives of the program, including private sector objectives.*
- *Incorporate security standards to the fullest extent as indicators of likelihood of compliance and with tariff and non-tariff measures, particularly those aimed at reducing risks in the supply chain. In Peru, the unmistakable example is BASC, program that has the third-party registration to their standards.*
- *Incorporate all the supply chain as members for eligibility.*
- *Apply the concept of comprehensive of due diligence process, which requires participants to verify the risk factors for its own supply chain.*
- *Perform a pilot test of the approach with selected companies before finalizing the guidelines.*

-Post a manual that can be followed by companies in preparation to apply for recognition as an AEO.

-Recognize small and medium enterprises as a special category.

Taking existing programs as base

The AEO program in the European Union has the advantage of having models of other customs administrations that implemented previous programs and compatible commercial programs of member states. It is the case of Dutch Client System program that focused on evaluating the reliability of the companies based on how they administer their customs routines from the perspective of risk analysis.

This program, which would later serve as the basis for the Dutch AEO program was mainly used internally by Dutch customs instead of making contact with companies. Based on two fundamental concepts it was developed: that the goods do not constitute a fraud and that compliance should be encouraged. Its approach made possible the development of a control program adapted to each company. Its most important components were:

- *Preliminary review. It is the first step to determine the most appropriate solution for the company and to examine whether the authorization can be granted.*
- *Control Program. A policy in which the type, frequency and scope of the ideal and the control methods that were used and established for each customer using the customer knowledge, risk analysis and tailored regulations.*
- *Plan of treatment. Document which sets out the elements of the control program to be implemented in light of the available capacity.*

Besides this, the team that worked with the company-the client-had certain roles defined:

-Team leader. Responsible for the

debe ser promovido. Su enfoque hizo posible la elaboración de un programa de control adaptado a cada empresa. Sus más importantes componentes fueron:

- **Revisión preliminar.** La primera etapa para determinar la solución más adecuada para la empresa en cuestión y para examinar si una autorización puede ser concedida.
- **Programa de control.** Una directiva en el que el tipo, la frecuencia y el alcance de la manera ideal y los métodos de control que se utilizaban y establecían por cada cliente, utilizando el conocimiento del cliente, el análisis de riesgos y las regulaciones hechas a la medida.
- **Plan de tratamiento.** Documento que establecía los elementos del programa de control a ser implementado a la luz de la capacidad disponible.

Además de esto, el equipo que trabajaba con la empresa —el cliente— tenía definidos ciertos roles:

- **El líder del equipo.** Responsable del equipo que tomaba las medidas necesarias para determinar si se puede conceder o no una autorización, y que elemen-

tos de un programa de control supuestamente se implementará, la elaboración de un plan de tratamiento y de dirección de los controles.

- **Cliente coordinador.** Responsable de recopilar y analizar información sobre “sus” clientes, para realizar el análisis de riesgos y elaborar programas de control para cada uno de aquellos clientes, y asumir la responsabilidad del tratamiento integral de los clientes.
- **Auditor.** Responsable de las revisiones preliminares de los clientes potenciales y de las auditorías de los libros y los registros de los clientes existentes.

En general, era importante que las empresas pudieran contar con un tratamiento completamente individualizado en relación con el análisis de riesgos y un trabajo sistemático sobre los riesgos. Otras empresas eran clasificadas en grupos, en función de los tipos de bienes con que trabajan. Escalonadamente, los clientes estaban divididos dentro de cinco grupos según la complejidad de su acreditación. CS

team that took the necessary steps to determine whether or not a permission can be granted, and what elements of a supposedly control program will be implemented, the development of a treatment plan and management controls.

-Client Coordinator. Responsible for collecting and analyzing information about “his” customers, to perform risk analysis and develop control programs for each of those customers, and take responsibility for the comprehensive treatment of customers.

-Auditor. Responsible for preliminary reviews of potential customers and responsible for auditing books and records of existing customers.

In general, it was important that the companies could have a completely individualized treatment in relation to risk analysis and systematic work on the risks. Other companies were classified into groups depending on the types of goods with which they work. Step by step, customers were divided into five groups according to the complexity of its accreditation. CS

Cronología de la creación del programa OEA de la Unión Europea / Chronology of the creation of the AEO program of the European Union

Julio 2004 / July 2004	La Comisión Europea presenta al Parlamento y Consejos los cambios propuestos para la seguridad de la cadena de suministro para su transformación en ley. / <i>The European Commission presented to Parliament and Councils the proposed changes to the security of the supply chain to its transformation in law.</i>
Mayo 2005 / May 2005	Se reforma el Código Aduanero de la Comunidad para incluir los requisitos de seguridad necesarios para permitir los programas OEA. / <i>The Community Customs Code is reformed to include security requirements to allow AEO programs</i>
Junio 2005 / June 2005	La OMA publica las Normas SAFE. Junio 2006. Se emite un Modelo Compacto de OEA. / <i>The WCO publishes Standards SAFE issued. June 2006. An AEO compact model was issued.</i>
Agosto 2006 / August 2006	Se publica un informe de un caso de estudio de piloto. / <i>A report of a pilot case study was published.</i>
Junio 2007 / June 2007	Se emiten directrices para programas OEA de estados miembros. / <i>Program guidelines are issued for AEO member states</i>
Enero 2008 / January 2008	Los estados miembros dan inicio a programas OEA de conformidad con las directrices. / <i>Member states are beginning the AEO programs in accordance with the guidelines.</i>

Fuente: Aduana de Holanda (www.douane.nl) / European Commission, Taxation and Customs Union (http://ec.europa.eu/taxation_customs/) / OMA / Source: Netherlands Customs (www.douane.nl) / European Commission, Taxation and Customs Union (http://ec.europa.eu/taxation_customs/) / WCO.



Plan nacional de lucha contra el lavado de activos y financiamiento del terrorismo

NATIONAL PLAN TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

Actualmente, el Perú está trabajando en esta iniciativa concebida como Política de Estado. Se trata de una tarea a ser asumida por todas las fuerzas políticas como parte de su compromiso por combatir ambos flagelos que atentan seriamente contra la seguridad interna, orden social y económico del país.

Currently, Peru is working on this initiative conceived as a State policy. This is a task to be assumed by all political forces as part of its commitment to combat both scourges that seriously threaten the internal security, social and economic development.

Con la participación de más de 20 instituciones públicas y privadas, la Superintendencia de Banca, Seguros y AFP (SBS) está elaborando el "Plan Nacional de Lucha contra el Lavado de Activos (LA) y Financiamiento del Terrorismo (FT)" cuyas principales áreas de acción comprende la elaboración de un diagnóstico de riesgos de lavado y el diseño de la estrategia nacional para enfrentar efectivamente dichos delitos.

Según Daniel Linares, Intendente de Análisis de la Unidad de Inteligencia Financiera (UIF) de la SBS, en este emprendimiento destaca la participación del Ministerio Público, Poder Judicial, Policía Nacional, Conasev, Ministerio del Interior, Contraloría, Sunat, Banco Central de Reserva, Ministerio de Relaciones Exteriores, Devida, Ministerio de Justicia, entre otras instituciones.

Esta importante iniciativa permitirá al país contar con un único instrumento de acción que permita enfrentar con más ventajas y eficiencia a las dos actividades ilícitas que, a juzgar por los indicios de dinamis-

mo del narcotráfico y su aliado el terrorismo, están distorsionando el comportamiento de la economía y el comercio, así como promoviendo el quiebre, a través de la corrupción y la delincuencia, de una calma social necesaria para el crecimiento y desarrollo.

Recientemente en marzo, la SBS informó que recibió una misión de funcionarios del Fondo Monetario Internacional (FMI) para brindar asistencia técnica y revisar los avances en la elaboración del Plan. En dicha ocasión se anunció que el Plan sería presentado en junio de 2011 conteniendo "acciones concretas como plazos, responsables y costos aproximados para enfrentar de manera coordinada las vulnerabilidades que el sistema peruano presenta para enfrentar eficazmente estos delitos, las cuales fueron identificadas previamente en un diagnóstico de riesgos".

En el comercio exterior

En el actual marco económico nacional positivo y el crecimiento sostenido del comercio exterior, se habla de la existencia de más de 7.600 empresas exportadoras entre otras tantas importadoras. Bajo este contexto, preocupa el incremento de actividades ilícitas como el narcotráfico y el lavado de activos, frente a lo cual surge la inquietud de si el sistema de control y supervisión policial/aduanera está adaptándose a esta situación que permita a las empresas contar con una cadena logística segura.

Frente a esta preocupación, Daniel Linares señala que "de la experiencia internacional se conoce que las organizaciones criminales utilizan el comercio internacional para llevar a cabo sus actividades ilegales, es así que no es raro ver que nuestras autoridades descubran embarques de exportación con droga ca-

muflada; adicionalmente, existe otra modalidad menos conocida que tiene por finalidad la repatriación de fondos ilícitos, simulando la exportación de productos de 'elevado valor' cuya valoración justamente resulta difícil de verificar, como son por ejemplo la exportación de 'toros de lidia', 'caballos de carrera', 'productos químicos innovadores', etc."

Para Linares es innegable que el incremento de las actividades de comercio exterior trae consigo la posibilidad de que grupos u organizaciones criminales intenten aprovechar esta coyuntura para realizar sus actividades delictivas; no obstante, al mismo tiempo, también nuestras autoridades policiales y aduaneras han intensificado sus acciones de represión y control, respectivamente.

Al respecto, el especialista manifiesta que "la SBS a través de la UIF-Perú viene realizando acciones conjuntas con el Ministerio Público,

With the participation of over 20 public and private institutions, the Superintendency of Banks, Insurance and Pension Fund Administrators (SBS) is developing the "National Plan to Combat Money Laundering and the Financing of Terrorism" whose main areas of action include the development of a diagnosis of laundering risks and a design of national strategy to deal effectively with such crimes.

According to Daniel Linares, Mayor of Analysis of the Financial Intelligence Unit of the SBS the participation of the Public Ministry, Judiciary, National Police, Conasev, Ministry of the Interior, Comptroller, Sunat, Central Reserve Bank, Ministry of Foreign Affairs, Devida, Ministry of Justice, among others is highlighted.

This important initiative will enable the country to have a single instrument of action to deal with more advantages and efficiencies to both illegal activities which judging by the signs of dynamism in drug trafficking and its terrorism ally are distorting the behavior of the economy and trade as well as promoting the break, through corruption and crime from a

social calm necessary for growth and development.

Recently in March, SBS reported that officials received a mission from the International Monetary Fund to provide technical assistance and review progress in developing the Plan. On that occasion it was announced that the Plan would be presented in June 2011 containing "concrete actions such as deadlines, responsible persons and estimated costs in a coordinated manner to address the vulnerabilities that the Peruvian system has to deal effectively with these crimes, which were previously identified in a diagnosis of risks."

In foreign trade

In the current positive national economic framework and sustained growth of foreign trade, we speak of the existence of more than 7,600 exporters among many other importers. In this context, we are concerned about the increase of illegal activities like drug trafficking and money laundering, so the question of whether the system control and monitoring police / customs is adapting to this situation that allows companies to have a secure supply chain arises.

Addressing this concern, Daniel Linares notes that "from the international experience it is known that criminal organizations use international trade to carry out their illegal activities, so it's not uncommon to see that our authorities find camouflaged drug in export shipments. Additionally, there is another less known method which is intended for the repatriation of illicit funds, simulating the export of 'high value' whose value is difficult to precisely verify, such as the export of 'fighting bulls,' 'racehorses,' 'innovative chemical products,' etc.."

For Linares is undeniable that the increase in foreign trade activities brings the possibility of groups or criminal organizations seeking to exploit these opportunities for criminal activity, however, at the same time, our law enforcement authorities have intensified their actions of repression and control, respectively.

In this regard, the specialist stated that "the SBS through the FIU-Peru has been carrying out joint actions with the Public Prosecutor, PNP and Sunat in relation to the control of transboundary movements of cash which is a phenomenon linked to

PNP y Sunat, en relación al control del transporte transfronterizo de efectivo que es un fenómeno muy ligado al lavado de activos. Como resultado nos hemos enriquecido con la experiencia de estas acciones conjuntas, y estrechado vínculos sobre todo de coordinación, sin embargo, quedan varios aspectos por mejorar”.

Investigaciones de inteligencia financiera

Para la opinión pública, parte de la labor de la UIF es realizar investigaciones de inteligencia financiera vinculadas al tráfico ilícito de drogas. Sin embargo, Daniel Linares precisa que “la Unidad de Inteligencia Financiera de la SBS, realiza fundamentalmente una labor de análisis sobre la base de los reportes de operaciones sospechosas que recibe de las entidades o personas que están obligadas a reportar, denominadas sujetos obligados, y el resultado es remitido mediante informes de inteligencia financiera al Ministerio Público, siempre y cuando se encuentre indicios de lavado de activos y/o financiamiento del terrorismo, para que proceda según sus atribuciones; en tal sentido, no efectuamos una investigación según las características y alcance de la PNP o el Ministerio Público”.

Hecha la aclaración, también es importante conocer la situación de las empresas y rubros comprometidos en los análisis. Sobre este punto, el experto de la UIF/SBS señala que “a diciembre de 2010 hemos emitido 185 informes de inteligencia financiera, los cuales involucran operaciones por un monto aproximado de 3.600 millones de dólares, lo cual no significa que se esté lavando esa cantidad de dinero, dado que la UIF-Perú sólo traslada los indicios detectados y los somete a la consideración del Ministerio Público, para su posterior investigación de ser el caso”.

Respecto del número de personas y empresas involucradas, según Linares se trata de varios cientos, estando entre los rubros de mayor

incidencia, empresas de servicios, comercio y construcción, “muchas de ellas creadas solamente como ‘fachada’, para facilitar la legitimación de dinero sucio”.

Financiamiento del terrorismo

En relación a las investigaciones de inteligencia financiera que puedan revelar casos de vinculación con el financiamiento del terrorismo, la opinión pública no ha escuchado hasta ahora algunas señales y menos precisiones de casos reales que podrían revelar la relación entre empresas (exportadoras o importadoras) y agrupaciones como Sendero Luminoso o el MRTA. ¿Existen casos?

Comprensiblemente, Linares manifiesta que lamentablemente “no es posible precisar detalles debido a que se trata de información de inteligencia, no obstante, toda la información que recibimos en relación a posibles actividades relativas al financiamiento del terrorismo es comunicada a las autoridades competentes”.

Sin embargo, afirma que las agrupaciones “hacen uso de mecanismos y canales similares a los lavadores, sin embargo, en estos casos, los fondos o activos pueden también tener origen lícito, como donaciones, pero con un fin nefasto como es la realización de actos terroristas. Se han encontrado diferentes rubros en casos de este tipo, y lamentablemente tendrían conexiones en otros países”. **CS**

money laundering. As a result we have enriched the experience of these joint actions, and particularly close ties of co-ordination, however, there are several aspects to improve.”

Financial Intelligence Investigations

For the public opinion, part of the work of the FIU's is to make investigations of financial intelligence related to illicit drug trafficking. However, Daniel Linares states that “the Financial Intelligence Unit of the SBS performs analytical work primarily on the basis of suspicious transaction reports that receives from entities or persons who are required to report, named

entities, and the result is sent through financial intelligence reports to prosecutors as long as there is evidence of money laundering and / or terrorist financing, to proceed according to its powers, in that sense, we do not complete an investigation according to the nature and extent the PNP or the Public Prosecutor.”

After this clarification it is also important to know the situation of companies and items involved in the analysis. On this point, the expert from the FIU / SBS points out that “in December 2010 we issued 185 financial intelligence reports, which involve operations of approximately \$ 3,600 million, which does not mean that that amount is money laundering as FIU-Peru only moves the detected signs and submitted them to the consideration of Public Prosecutions for further investigation of the case.”

Regarding the number of people and companies involved, according to Linares there are hundreds, being commerce and construction among the highest incidence areas, and “many of them created only as a ‘front’, to facilitate the legitimization of dirty money.”

Financing of Terrorism

In relation to financial intelligence investigations that may reveal cases of connection with the financing of terrorism, the public opinion has not heard so far some signs and details of actual cases that might reveal the relationship between companies (exporters or importers) and groups such as Sendero Luminoso or MRTA. Are there cases?

Understandably, Linares says that unfortunately “it is not possible to specify details because it is intelligence, however, all information we receive in relation to any activities related to terrorist financing is communicated to the authorities.”

*However, he says that the groups “make use of mechanisms and similar channels to the washers, however, in these cases, the funds or assets may also have legal origin, such as grants, but with a pitiful fate as performing acts terrorists. Different items are in cases like this, and unfortunately have connections in other countries.” **CS***

El programa OEA tiene como objetivo ayudar a los exportadores peruanos /
The AEO program aims to help Peruvian exporters

Acceso más rápido a los mercados extranjeros y tomar ventaja de los acuerdos comerciales

FASTER ACCESS TO FOREIGN MARKETS AND TAKE ADVANTAGE OF TRADE AGREEMENTS



Fermín Cuza, presidente internacional de la Organización Mundial BASC, amplía en esta entrevista la labor de la Organización Mundial BASC en la promoción del Operador Económico Autorizado (OEA) en Latinoamérica, como corolario de lo que fue el seminario "Operador Económico Autorizado OEA en el Perú y su implementación" en el que participó como expositor este 18 de agosto pasado.

Fermin Cuza, international president of the World BASC Organization, in this interview extends the work of the World BASC Organization in promoting the AEO (OAS) in Latin America as a corollary of what was the seminar "AEO in Peru and its implementation" in which he participated as an exhibitor this August 18.

¿Por qué fomentar la implementación en el Perú del Operador Económico Autorizado (OEA)?

Perú es un actor importante en la actividad del comercio internacional de América Latina. En el 2009 exportó más de \$ 26,6 mil millones en diversos tipos de mercancías (oro, cobre, harina de pescado, petróleo, zinc, textiles, prendas de vestir, espárragos, café y otros productos). Este comercio se ve facilitado por los acuerdos comerciales con Estados Unidos, Chile, México, Canadá, Singapur, China y la Unión Europea. Perú también pertenece a la Comunidad Andina, el grupo de Cooperación Económica de Asia-Pacífico (APEC) y la Organización Mundial del Comercio (OMC).

Teniendo en cuenta estos acuerdos y el potencial de crecimiento económico que les brinda a las empresas peruanas, es imperativo que el Perú aproveche las ventajas competitivas que pueden obtener con el fin de facilitar y hacer crecer el comercio. Una de esas ventajas son los beneficios de facilitación del comercio que Perú puede asegurar a sus exportadores al adoptar el programa de Operador Económico Autorizado.

Why encourage the implementation of AEO in Peru?
 Peru is a major participant in international trade activity in

Latin America. In 2009 exported more than \$ 26.6 billion in various types of commodities (gold, copper, fishmeal, petroleum, zinc, textiles, apparel, asparagus, coffee and other products). This trade is facilitated by trade agreements with the United States, Chile, Mexico, Canada, Singapore, China and the European Union. Peru also belongs to the Andean Community, the Economic Cooperation group of Asia-Pacific (APEC) and the World Trade Organization (WTO).

Given these agreements and the potential of economic growth that provides them with Peruvian companies, it is imperative that Peru take advantage of the competitive advantages they can get in order to facilitate and increase trade. One of those benefits is the benefit of trade facilitation that Peru can ensure to their exporters in adopting the AEO program.

¿Cómo interviene BASC en este tema?

BASC está dispuesto a apoyar estos esfuerzos y trabajar directamente con las empresas que deseen participar en el programa OEA, proporcionando orientación a lo largo del proceso de solicitud y capacitando al personal operativo de la empresa en seguridad de la cadena logística.

En Perú, el Capítulo BASC Nacional, la Organización Mundial BASC (WBO) y la Organización Mundial de Aduanas (OMA) se han reunido en varias ocasiones con funcionarios de alto nivel de la autoridad aduanera (Sunat) con la finalidad de ofrecer apoyo y participación de BASC mediante la promoción del OEA a sus más de 500 empresas certificadas así como a sus asociados de negocios.

Una de esas reuniones fue la que sostuvieron las delegaciones de BASC PERÚ y de la Organización Mundial BASC, con la ex Jefa de la Sunat, señora Gloria Luque, en abril de 2010, y más recientemente, el encuentro que sostuvo con la señora Luque en la reunión anual de la OMA realizada el pasado mes de junio en Bruselas, Bélgica, donde "personalmente tuve la oportunidad de expresarle y ratificarle el apoyo de BASC a la Aduana de Perú."

Considerando que contamos con una base sólida por nuestra trayectoria institucional de 13 años, así como por la importante red de cooperación internacional desarrollada, nos sentimos muy orgullosos por la realización de este seminario OEA que tuvo lugar en Lima el 18 de agosto, y estamos seguros que fue un acontecimiento decisivo para la promoción y el apoyo de este programa en el Perú.

¿Qué significa que una empresa cuente con la certificación OEA?

El programa OEA es una herramienta importante que puede ayudar a los exportadores peruanos a obtener un acceso más rápido a los mercados extranjeros y con ello tomar ventaja de los acuerdos comerciales existentes. Al asegurar sus cadenas de suministro y unirse al programa nacional de OEA, los exportadores peruanos podrán obtener la condición internacional como exportadores seguros y confiables,

logrando mejores tiempos en los trámites aduaneros y menores costos asociados a las inspecciones de la carga.

Como ejemplo de las ventajas de la relación costo-beneficio del programa OEA, las autoridades aduaneras de EE.UU. afirman que los importadores miembros del programa OEA (C-TPAT) de ese país, tienen seis veces menos probabilidades de que su mercancía sea inspeccionada que la de los que no son miembros del programa. Además, el costo promedio de un control aduanero típico es de unos \$1.000 dólares por contenedor, según las estadísticas de CBP, sin incluir otros costos indirectos como tiempo de espera para las inspecciones, daños a la carga, producto de la inspección y la pérdida de negocios

How is BASC involved in this topic?

BASC is willing to support these efforts and work directly with companies wishing to participate in the AEO program, providing guidance throughout the application process and training staff of the company operating the supply chain security.

In Peru, the National BASC Chapter, the World BASC Organization (WBO) and World Customs Organization (WCO) have met repeatedly with senior officials of the customs authority (Sunat) in order to offer support and participation of BASC through the promotion of AEO to its more than 500 certified companies and their business associates.

One of those meetings was the one held by the delegations of Peru and BASC World BASC Organization with the Sunat Chief, Gloria Luque in April 2010, and most recently, the meeting with Ms. Luque in OMA's annual meeting held last June in Brussels, Belgium, where I personally had the opportunity to express her the support of BASC to the Customs of Peru.

Considering that we have a solid base for our institutional trajectory of 13 years, as well as the extensive developed network of international cooperation, we are very proud of this AEO seminar which was held in Lima on August 18 and we are confident that it was a crucial event for the promotion and support of this program in Peru.

causados por el incumplimiento en los tiempos de entrega.

Teniendo en cuenta estos factores, la industria peruana debe trabajar estrechamente con las autoridades aduaneras del Perú para apoyar la aplicación del programa Operador Económico Autorizado y participar en el mismo tan pronto como este esté disponible. BASC está preparado y dispuesto a apoyar a todas aquellas empresas que deseen participar en el programa de OEA.

¿Cómo avanza en el mundo la implementación del Operador Económico Autorizado?

Comenzando con el programa BASC, en 1996, la primera alianza global entre la empresa y la aduana

What does it mean when a company has the AEO certification?

The OAS program is an important tool that can help Peruvian exporters to gain faster access to foreign markets and thereby take advantage of existing trade agreements. By securing their supply chains and join the national program of the AEO, Peruvian exporters may obtain international status as a safe and reliable exporters, achieving better times in customs procedures and lower costs associated with inspections of cargo.

As an example of the cost-benefit of AEO program, the U.S. customs authorities claim that importers members of the AEO program (C-TPAT) in that country are six times less likely to have their goods inspected than those who are not members of the program. In addition, the average cost of a customs inspection is typically about \$ 1,000 per container, according to statistics from CBP, not including indirect costs such as waiting time for inspections, cargo damage, product inspection and loss business caused by the breach at the time of delivery.

Given these factors, the Peruvian industry should work closely with the customs authorities of Peru to support the implementation of AEO and participate in it as soon as it becomes available. BASC is ready and willing to support those companies wishing to participate in the AEO program.

para la seguridad en la cadena de suministro y seguido del programa C-TPAT de los Estados Unidos en 2002, el nuevo paradigma de cooperación aduana-sector privado sigue creciendo. La Organización Mundial de Aduana ha adoptado este concepto en la figura del programa OEA bajo el marco SAFE, que establece los pilares guías de la cooperación "aduanas - aduanas" y "aduanas - empresas".

Me siento orgulloso de decir que en ninguna región del mundo el entusiasmo y el crecimiento del programa OEA es más fuerte que en América Latina. Esto se debe al reconocimiento por parte de las autoridades aduaneras regionales del nuevo paradigma de cooperación con el sector privado reforzado con el reconocimiento aduanero que la seguridad y la facilitación fronteriza son compatibles.

Estos ideales se han convertido en resultados tangibles gracias al fuerte apoyo del sector privado y las aduanas, como la Oficina de Aduanas y Protección Fronteriza de EE.UU. (CBP por sus siglas en inglés), Organización Mundial de Aduanas (OMA), Banco Interamericano de


Desarrollo en Washington (BID) y la Organización de Estados Americanos (OEA-CICAD).

Bajo la dirección de Carlos Ochoa (ejecutivo del CBP), Eleanor Thornton (OMA), Sandra Corcuera (BID), y Rafael Parada (OEA-CICAD), las administraciones de aduanas de la región se han beneficiado de numerosos Programas de Capacitación, Reuniones Regionales, Seminarios Aduanas-Empresas y otros ejemplos de apoyo en los últimos dos años.

De hecho BASC también es parte activa en este proceso de implementación.

En BASC nos sentimos orgullosos de haber capacitado a especialistas de la cadena de suministro OEA en México, República Dominicana y Colombia y coordinar y liderar varios eventos de promoción OEA en países BASC. Estamos viendo los resultados: Costa Rica, Guatemala y Argentina ya han implementado sus programas, mientras que otros están en fase piloto: Colombia (listo para iniciar el 29 de septiembre de 2011), República Dominicana, Perú y México.

Además, algunos países están en fase de diseño, como Panamá y Uruguay, mientras que otros están evaluando el programa con un fuerte interés en avanzar en una fecha cercana: Nicaragua, Honduras, Ecuador, Chile, Paraguay y El Salvador (que tiene un programa llamado Ritmo, pero sin un componente de seguridad) y Jamaica (también con un programa que carece de un componente de seguridad).

Reitero nuestra complacencia en BASC por los avances logrados por estos países en el programa OEA y esperamos que Brasil, Bolivia y Venezuela se unan pronto al programa. Resumiendo, gracias a estos esfuerzos hoy en día el programa Operador Económico Autorizado sigue avanzando. El objetivo de las administraciones regionales de aduana, igual de parte de nosotros en BASC, es lograr que el programa OEA se aplique lo más pronto posible, de modo que los beneficios de reconocimiento mutuo se puedan asegurar para las empresas exportadoras de cada país. 

How the implementation of AEO progresses in the world?

Starting with the BASC program in 1996, the first global partnership between business and customs for security in the supply chain and followed by the C-TPAT program in the United States in 2002, the new paradigm of private customs-sector cooperation continues to grow. The World Customs Organization has adopted this concept in the figure of the AEO program under the SAFE Framework, which sets the guidelines for cooperation pillars "customs - customs" and "customs - business."

I am proud to say that no region of the world excitement and growth of the AEO program is stronger than in Latin America. This is due to recognition by the customs authorities of the new paradigm of regional cooperation with the private sector, reinforced by the recognition of customs that security and border facilitation are compatible.

These ideals have become tangible results thanks to strong support from the private sector and

customs, as the Bureau of Customs and Border Protection (CBP), World Customs Organization (WCO), Inter-American Development Bank in Washington (IDB) and the Organization of American States (OAS-CICAD).

Under the direction of Carlos Ochoa (CBP executive), Eleanor Thornton (WCO), Sandra Corcuera (BID), and Rafael Parada (AEO-CICAD), the customs administrations of the region have benefited from numerous training programs, regional meetings, Customs-Business Seminars and other examples of support over the past two years.

In fact, BASC is also an active part in this process of implementation.

BASC is proud to have trained specialists in the AEO supply chain in Mexico, Dominican Republic and Colombia, and coordinate and lead a number of promotional AEO events in BASC countries. We are seeing results: Costa Rica, Guatemala and Argentina have already implemen-

ted their programs, while others are being piloted: Colombia (ready to start in September 29, 2011), Dominican Republic, Peru and Mexico.

In addition, some countries are being designed, such as Panama and Uruguay, while others are evaluating the program with a strong interest in moving forward anytime soon: Nicaragua, Honduras, Ecuador, Chile, Paraguay and El Salvador (which has a program called Rhythm, but without a security component) and Jamaica (also with a program that lacks a security component).

I reiterate our complacency in BASC for the progress made by these countries in the AEO program and hope that Brazil, Bolivia and Venezuela will soon join the program. In short, thanks to these efforts today AEO program is progressing. The objective of the regional customs administrations, as well as BASC, is to make the implementation of AEO program as soon as possible so that the benefits of mutual recognition can be secured for exporting companies in each country. 

Respuesta coordinada para la seguridad del transporte de carga

COORDINATED RESPONSE FOR THE SECURITY OF CARGO TRANSPORTATION



Recientemente, la IATA hizo un llamado a los reguladores de seguridad de todo el mundo para trabajar juntos en un mayor nivel de seguridad en el transporte de carga y la recopilación de datos. La principal organización de la aviación comercial mundial, reveló su intención de dirigir un esfuerzo mundial con el fin de conseguir el control de seguridad aeroportuaria del futuro.

Recently, IATA called for security regulators around the world to work together on a higher level of security in freight transport and data collection. The main organization of global commercial aviation revealed his intention to lead a global effort to gain control of airport security in the future.

Giovanni Bisignani, director general de la Asociación Internacional de Transporte Aéreo (IATA por sus siglas en inglés), señaló durante su participación en el evento Aviation Security World (AVSEC World) realizado en noviembre pasado en Fráncfort, Alemania, su visión para una seguridad aérea inteligente la que se basa en una respuesta coordinada para la seguridad del transporte de carga.

En dicha ocasión Bisignani dijo que la sociedad disfruta de un nivel de seguridad mayor que en 2001, pero que aún podemos seguir mejorando. En tal sentido, el ejecutivo identificó aquellas áreas que requieren un mayor esfuerzo para lograrlo, puntualizando los aspectos que más preocupan a los usuarios.

Seguridad del transporte de carga

Según el máximo dirigente de la IATA, el transporte de carga aérea dirige la economía mundial. Los productos transportados por este medio representan el 35% del valor total del comercio internacional de mercancías. En 2009, las aerolíneas transportaron 26 millones de toneladas de carga internacional. Hacia 2014, esta cantidad se incrementará hasta los 38 millones. De allí que garantizar un transporte seguro y eficiente es fundamental. En este

Giovanni Bisignani, director general de the International Air Transport Association (IATA) said during his participation in the World Aviation Security (AVSEC World) event held last November in Frankfurt, Germany, his vision for an intelligently aviation safety based on a coordinated response to the security of cargo transportation.

On that occasion, Bisignani said the company enjoys a greater level of security than in 2001, but we can still continue to improve it. In this sense, the executive identified areas that require more work to do, emphasizing the issues of users concerns.

Cargo transportation security

According to the leader of IATA, the air cargo transportation runs the world economy. The products transported by this means represent 35% of the total value of international trade of goods. In 2009, the airlines carried 26 million tons of international cargo. By 2014, this amount will increase to 38 million. So, ensuring a safe and efficient transport is essential. In this context, Bisignani highlighted the following four basic principles for security programs of freight.

- **Building up the supply chain:** The entire supply chain, from manufacturer to the airport, must assume

marco, Bisignani resaltó los siguientes cuatro principios básicos para los programas de seguridad del transporte de carga.

- Planteamiento de la cadena de suministro: La totalidad de la cadena de suministro, desde el fabricante hasta el aeropuerto, debe asumir la responsabilidad de la seguridad en el transporte. El planteamiento de la cadena de suministro debe estar dirigido por la cooperación de gobiernos e industria en materia de inversión, procesos, tecnología y consultoría de riesgos. Muchos países, incluidos el Reino Unido y Estados Unidos, han adoptado soluciones avanzadas en la cadena de suministro. Esto revela que la industria está comprometida. Otra muestra de ello es que el programa de Seguridad del Transporte de Carga de IATA está ayudando a resolver este punto crítico para conseguir mayor seguridad, explicó Bisignani.

- Tecnología: El representante de

responsibility for security in transport. The approach of the supply chain should be driven by government and industry cooperation in investment, processes, technology and risk consulting. Many countries, including the United Kingdom and United States have adopted advanced solutions in the supply chain. This reveals that the industry is committed. Another example is the Security of Cargo Transportation program of IATA which is helping solve this critical point to attain greater security, said Bisignani.

- Technology: The IATA representative said we should not consider the scanning system of airports as our first line of defense, but as an effective complement to other solutions with the security of the supply chain and intelligent security. Currently, there is no official certification system that is able to scan standard size pallets or large products. "The study is in progress but much remains to take the laboratory to the airport. We must hurry in this process", he said.

IATA dijo que no debemos considerar al sistema de escáner de los aeropuertos como nuestra primera línea de defensa, pero sí como un complemento efectivo junto a otras soluciones para la seguridad de la cadena de suministro y una seguridad inteligente. En la actualidad, no existe ningún sistema con una certificación oficial que sea capaz de escanear los pallets de tamaño estándar ni productos de gran tamaño. "El estudio está en marcha pero aún falta mucho para llevarlo del laboratorio al aeropuerto. Debemos darnos prisa en este proceso", precisó.

- E-freight: El programa e-Freight de IATA ofrece una importante herramienta de información para los gobiernos. "La conversión de 20 documentos de carga en un solo formato electrónico, mejora la eficiencia y ofrece una herramienta precisa para inspeccionar al transportista, la mercancía que transporta y su destino.

- E-freight: The e-Freight program of IATA provides an important information tool for governments. "The conversion of 20 loading documents into a single electronic form. It improves efficiency and provides an accurate tool for inspecting the carrier, the goods transported by him and their destination. As the use of e-freight increases in the sector, governments should extend their application for transport within and outside its borders, and use this data to intelligently manage the safe transport of cargo", said Bisignani.

- Risk: The aviation industry has cooperated with governments to help diminish the risks identified through their intelligent systems. "But effective solutions are not achieved either unilaterally or precipitously. We have seen many cases that have not achieved the desired results. It's still early, the executive said."

Control of security in the future

IATA also called for regulators and the sector to assist in the modernization of airport scanning systems that are already 40 years old. This

A medida que el uso de e-Freight aumenta en el sector, los gobiernos deben extender su aplicación en el transporte dentro y fuera de sus fronteras, y aprovechar estos datos para gestionar de manera inteligente la seguridad del transporte de carga", dijo Bisignani.

- Riesgo: El sector aéreo ha cooperado con los gobiernos para ayudar a diluir los riesgos identificados a través de sus sistemas inteligentes. "Pero las soluciones efectivas no se consiguen de forma unilateral ni precipitada. Hemos sido testigos de muchos casos en los que no se han conseguido los resultados deseados. Aún es temprano, manifestó el ejecutivo".

Control de seguridad en el futuro

IATA también hizo un llamado a los reguladores y al sector para colaborar en la modernización de los sistemas de escáner aeroportuarios

organization has a short-and long-term security control of the next generation. In short term, they already work on concepts and processes.

"Belts, shoes and shampoos are not the problem. We must focus on finding objects that will lead to dangerous terrorists. And to be efficient, we need intelligence and technology in the security checkpoint. The large amount of data collected from passengers can help to identify risks. The entire process should be much faster and more accurate. We can not allow that passengers and users be treated as terrorists until their innocence is proven, "said Bisignani. As for the long-term vision, the path where the user enters the airport until the path where the plane arrives must be a continuous and without obstacles process.

Collection of standardized data

The collection of data is critical to aviation safety because it gives governments the ability to screen passengers and to identify possible threats. Through the International

que ya tienen 40 años de antigüedad. Esta organización tiene una visión a corto y largo plazo para el control de seguridad de la próxima generación. A corto plazo, ya trabaja en los conceptos y nuevos procesos.

“Cinturones, zapatos y champús no son el problema. Debemos centrarnos en buscar objetos peligrosos que nos lleven a los terroristas. Y para ser eficientes, necesitamos inteligencia y tecnología en el control de seguridad. La gran cantidad de datos recogidos de los pasajeros pueden ayudarnos a identificar los riesgos. Todo el proceso debe ser mucho más rápido y más preciso. No podemos consentir que los pasajeros y usuarios sean tratados como terroristas hasta que su inocencia sea probada”, dijo Bisignani. En cuanto a la visión a largo plazo, el camino desde que el usuario entra en el aeropuerto

hasta que llega al avión, debe ser un proceso ininterrumpido y sin obstáculos.

Recojo de datos estandarizada

El recojo de datos es crítico para la seguridad aérea ya que ofrece a los gobiernos la posibilidad de examinar a los pasajeros e identificar posibles amenazas. A través de la Organización Internacional de Aviación Civil (OACI), los gobiernos acordaron utilizar estándares en cuanto a datos y procesos para el recojo de información. No todos los gobiernos siguen estos estándares que buscan complementar los 5.900 millones de dólares que las aerolíneas gastan anualmente en seguridad. El costo de instalación de sistemas de seguridad que no cuentan con los requerimientos estandarizados para la solicitud de datos, es de un millón de dólares. La incorporación de un sólo elemento no estándar al siste-

ma de recopilación de datos, tiene un costo de 50.000 dólares.

Al respecto, Bisignani destacó la preocupación desatada por los nuevos requisitos en recojo de datos en India, China, Corea del Sur y México. Para el dirigente, todas estas excepciones representan un gasto de dinero y de recursos que no aportan una mejora en la seguridad o control de aduanas. Por ello, el reto es trabajar con los gobiernos para implementar sistemas estandarizados.

El 2010 Estados Unidos creó un grupo de trabajo internacional para la seguridad aérea, y el comité ejecutivo de OACI acordó en octubre de dicho año que los objetivos de la industria y los gobiernos deben estar alineados. Desde entonces se considera que ha comenzado una nueva era de cooperación, aunque el avance en palabras no significa nada si no se llevan a cabo acciones.


Fuente: IATA 

Civil Aviation Organization (ICAO), governments agreed to use data standards and processes for the collection of information. Not all governments follow these standards that are intended to complement the 5,900 million dollars spent annually on airline safety. The cost of installing security systems that do not have standardized requirements for data request is one million dollars. The incorporation of a single

non-standard element to the data collection system costs \$ 50,000.

In this regard, Bisignani highlighted the sparked concern by the new requirements for data collection in India, China, South Korea and Mexico. For the leader, these exceptions represent a waste of money and resources that do not provide an improvement in security and customs control. Therefore, the challenge is to work with governments

to implement standardized systems.

In 2010, the United States created an international working group for aviation safety, and the executive committee of ICAO agreed in October of that year that the objectives of industry and governments must be aligned. Since then it is considered that a new era of cooperation have begun, although progress in words means nothing if no actions are performed. Source: IATA 

Debe saber que... / You should know that...

El sistema de transporte aéreo de carga consiste en una enorme y compleja red de distribución que une a fabricantes y transportistas con gentes de carga, aeropuertos donde se clasifican, manipulan y se cargan y descargan las aeronaves. La demanda de los negocios y los consumidores por rapidez y un eficiente manejo de la carga para un rápido envío de mercancías, ha impulsado el veloz crecimiento de esta industria en las últimas tres décadas. IATA (International Air Transport Association) es una de las alrededor de 230 líneas aéreas que representan el 93% del tráfico aéreo regular internacional.

The system of air cargo is a large and complex distribution network linking manufacturers and shippers with people loading, which classifies airports, handling and loading and unloading aircraft. Demand for business and consumers for speed and efficient cargo handling for a quick shipment of goods has driven the rapid growth of this industry in the last three decades. IATA (International Air Transport Association) is one of some 230 airlines representing 93% of scheduled international air traffic.

C-TPAT y OEA, lo mismo pero diferentes

C-TPAT AND AEO, SAME BUT DIFFERENT



Los que están inmersos en el mundo del comercio exterior ya están familiarizados con los programas Trade Partnership Against Terrorism (C-TPAT) de Estados Unidos y el Operador Económico Autorizado (OEA) de la Organización Mundial de Aduanas (OMA). Ambos son programas de seguridad enfocados en la cadena de suministros. ¿Cuál es la situación de sus similitudes, diferencias, significados, etc.?


Según la consultora estadounidense Integration Point Global, ambos son programas voluntarios nacidos en respuesta a la amenaza del terrorismo mundial y tienen el objetivo central de asegurar y facilitar el comercio mundial sobre la base de sus trabajos en las cadenas de suministros, así como los beneficios que ofrecen, son similares. Sin embargo, existen diferencias entre ambos programas.

La principal diferencia es que, desde su inicio en 2001, el C-TPAT es un

programa enfocado en las importaciones de EE.UU., mientras que el OEA –vigente desde 2008– cubre tanto las importaciones como las exportaciones de un país. Existen alrededor de 30 programas diferentes en 56 países basados en el Marco Normativo de la OMA.

Por su parte, el C-TPAT cuenta actualmente con más de 10.000 miembros en EE.UU., y tiene reconocimiento mutuo con alrededor de seis países (el acuerdo más reciente fue con China en mayo pasado). La acreditación de C-TPAT comprende un proceso de 3 pasos para la certificación, validación y formalización, mientras que la acreditación OEA comprende un proceso de 8 pasos.

Además, estos programas son independientes, lo que significa que ser un miembro de C-TPAT no es lo mismo que ser un miembro OEA, porque las medidas de seguridad requeridas son diferentes según el país, a menos que exista un Acuerdo de Mutuo Reconocimiento (AMR) entre el C-TPAT y un programa específico de Operador Económico Autorizado.

A pesar de las diferencias, el enfoque basado en riesgos adoptados por C-TPAT y OEA proporciona un menor riesgo en la cadena de suministro, mejora la comercialización y aumenta los activos, así como fortalece el valor de marca. Estos programas mejoran la seguridad a lo largo de todos los puntos de la cadena de suministro. Fuente: Integration Point. 

Those immersed in the world of foreign trade are familiar with the Trade Partnership Against Terrorism (C-TPAT) in the U.S. and the Authorized Economic Operator (AEO) of the World Customs Organization (WCO) programs. Both are safety programs focused on the supply chain. What is the status of their


similarities, differences, meanings, and so on?

According to Global Integration Point, a U.S. consultancy, both are voluntary programs born in response to the threat of global terrorism and central aim of securing and facilitating global trade on the basis of their work in supply chains, as well as the benefits they offer are similar. However, there are differences between the two programs.

The main difference is that since its inception in 2001, the C-TPAT is a program focused on U.S. imports, while the AEO – valid since 2008 – covers both imports and exports of a country. There are about 30 different programs in 56 countries based on the WCO Framework of Standards.

For its part, the C-TPAT now has more than 10,000 members in the U.S. and has mutual recognition with around six countries (the most recent agreement was with China last May). The C-TPAT accreditation includes a 3 step process for certification, validation and formalization, while the AEO accreditation process includes 8 steps.


Moreover, these programs are independent, which means to be a member of C-TPAT is not the same as being an AEO member because the required safety measures are different from country to country, unless there is a Mutual Recognition Agreement between the C-TPAT and an AEO specific program.

Despite the differences, the risk-based approach adopted by C-TPAT and AEO provides a lower risk in the supply chain, improve marketing and increase assets, and strengthen the brand value. These programs improve security along all points of the supply chain. Source: Integration Point. 


China y Estados Unidos colaboran con la seguridad del comercio

CHINA AND THE UNITED STATES WORK WITH TRADE SECURITY

A inicios de mayo pasado, China y Estados Unidos firmaron un acuerdo de colaboración para mejorar la seguridad y facilitación del comercio. Alan D. Bersin, comisionado del Customs and Border Protection (CBP) de EE.UU. y Yu Guangzhou, ministro de Aduanas de la República Popular de China firmaron un plan de acción para los próximos cinco años el 9 de mayo, el cual cubre todos los aspectos de los programas de seguridad de la cadena de suministro de ambos países, incluyendo la validación de los procedimientos.

Además de cooperar en muchos aspectos de la aplicación de la ley, incluyendo el intercambio de información, cooperación, capacitación y asistencia técnica, ambos países se centrarán en reforzar las investigaciones, allanamientos y decomisos desde el inicio de la cadena de suministro a través de los puntos de fabricación, almacenamiento y transporte de mercancías ilegales antes de que lleguen a los mercados extranjeros. Fuente: CBP. 

In early May, China and the U.S. signed an agreement to improve security and trade facilitation. Alan D. Bersin, Commissioner of Customs and Border Protection (CBP) from the U.S. and Yu Guangzhou, Minister of Customs of the Republic of China signed an action plan for the next five years on May 9, which covers all aspects of security programs of the supply chain of both countries, including validation procedures.

In addition to cooperate in many aspects of law enforcement, including information exchange, cooperation, training and technical assistance, both countries will focus on strengthening investigations, searches and seizures since the start of the supply chain through the points of manufacture, storage and transportation of illegal goods before they reach foreign market. Source: CBP. 

Inician programa europeo de vigilancia marítima Perseus

BEGINNING OF PERSEUS, A EUROPEAN MARITIME SURVEILLANCE PROGRAM

A mediados de marzo pasado se dio comienzo al proyecto Perseus (Protection of European Borders and Seas through the Intelligent Use of Surveillance), el cual busca la protección, sobre la base de un sistema europeo integrado, de los mares y las fronteras europeas. Con un presupuesto de 43,7 millones de euros y una duración de cuatro años, es una de las primeras y más importantes iniciativas financiadas en el marco del VII Programa Marco de I+D de la UE.

El proyecto incrementará la efectividad de los sistemas actuales al crear un entorno compartido de información marítima que beneficiará tanto a los centros nacionales de coordinación, como a la Agencia Europea de Fronteras Exteriores, Frontex, y la Agencia Europea de Seguridad Marítima (EMSA). Este "sistema de sistemas", aprovechará toda la información disponible en las agencias europeas y nacionales, la integrará y la procesará.

Mediante dos pruebas a gran escala, Perseus permitirá demostrar la viabilidad de un sistema europeo y marcará el estándar y las bases para su desarrollo final. Será el primer sistema de vigilancia marítima a escala europea que podrá detectar embarcaciones pequeñas y vuelos a baja cota.

La primera prueba tendrá lugar hacia 2013 en el Mediterráneo Occidental y se centrará en el control del tráfico procedente del Atlántico. La segunda, será en 2014 y se llevará a cabo en el Mediterráneo Oriental en la zona del Mar Egeo, con una potencial expansión hasta el Mar Negro.

In mid-March the Perseus project (Protection of European Borders and Seas through the Intelligent Use of Surveillance) began. This project seeks protection on the basis of an integrated European system of European seas and borders. With a budget of 43.7 million euros and duration

of four years, is one of the first and most important initiatives funded under the Seventh Framework Programme of I+D in the EU.

The project will increase the effectiveness of current systems by creating a shared environment of maritime information that will benefit national coordination centers, the European External Borders Agency, Frontex and the European Maritime Safety Agency (EMSA). This "system of systems" will use all available information on the European and national agencies. It will integrate and process it.

In two large scale tests, Perseus will demonstrate the viability of a European system and set the standard and the basis for its final development. It will be the first maritime surveillance system at European level which can detect small boats and low-altitude flights.

The first test will take place around 2013 in the Western Mediterranean and will focus on traffic control from the Atlantic. The second will be in 2014 and will take place in the Eastern Mediterranean in the Aegean Sea area with a potential expansion to the Black Sea. Source: Indra, España. 


BASC tuvo destacada participación en reunión aduanera

BASC HAD OUTSTANDING PARTICIPATION IN CUSTOMS MEETING

Del 30 de mayo al 3 de junio pasados, se realizó en la República Dominicana la XIV Conferencia Regional de Directores Generales de Aduanas de las Américas y del Caribe (CRDGA) y la Trigésima Segunda Reunión de Directores de Aduanas de América Latina, España y Portugal (COMALEP). En el encuentro, en el que participó Kunio Mikuriya, secretario general de la Organización Mundial de Aduanas (OMA), funcionarios y especia-

listas desarrollaron temas relativos a las nuevas estrategias del comercio transfronterizo, la cooperación y la seguridad internacional de las aduanas.


Fermín Cuza, presidente internacional de la Organización Mundial BASC (WBO), participó como expositor en el segundo evento junto a representantes de más de 25 autoridades aduaneras, del Banco Interamericano de Desarrollo (BID), OMA y el Customs and Border Protection (CBP).

Como resultado de dicha participación, el Coordinador de Aduanas de Honduras solicitó la asistencia de BASC para celebrar un evento entre el sector privado y la aduana hondureña con la finalidad de promover la implementación del OEA en ese país. Así mismo, los representantes regionales de aduanas participantes propusieron se designe al señor Cuza, como contacto de BASC para los temas relativos a la aplicación del programa OEA en sus respectivos países. 

From May 30 to June 3, the XIV Regional Conference of Customs Directors General of the Americas and the Caribbean (RCCDG) was held in the Dominican Republic and the Thirty-Second Meeting of Heads of Customs of Latin America, Spain and Portugal (COMALEP). At the meeting, where Kunio Mikuriya, secretary general of the World Customs Organization (WCO) participated, officials and

specialists issues developed new strategies of cross-border trade, cooperation and international security of customs.

Fermin Cuza, international president of the World BASC Organization (WBO), participated as an exhibitor in the second event with over 25 representatives of customs authorities, the Inter-American Development Bank (IDB), WCO and Customs and Border Protection (CBP).

As a result of such participation, the Coordinator of Customs of Honduras requested the assistance of BASC to hold an event from the private sector in order to promote implementation of the implementation of AEO in that country. In addition, regional representatives of customs participants proposed the appointment of Mr. Cuza as BASC contact for issues relating to the implementation of AEO in their respective countries. 



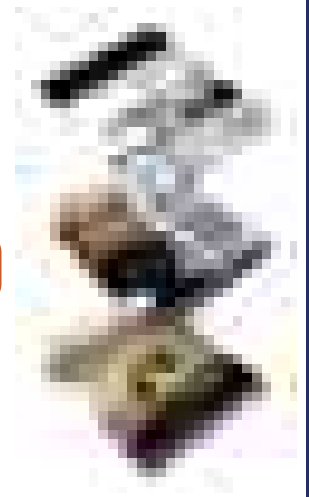
Medio especializado en el Supply Chain Security (SCS), con información nacional e internacional y las últimas tendencias y acontecimientos de seguridad en la carga.

Anuncie aquí

Grupo Objetivo : Directores y ejecutivos de empresas de comercio internacional, gremios, entidades públicas y privadas del sector, autoridades institucionales nacionales e internacionales relacionadas.
Distribución : Física (4,000 ejemplares) y virtual (10,000 contactos)
Periodicidad : Bimensual **Idioma** : Español / Inglés
Informes : (01) 612-8300 Anexo 2276 / apoyo.imagen2@basceru.org



BUSINESS ALLIANCE FOR SECURE COMMERCE





XXXI Curso de Auditores Internacionales BASC en Lima

XXXI COURSE OF BASC INTERNATIONAL AUDITORS IN LIMA

A finales de junio pasado se realizó en Lima el XXXI Curso de Auditores Internacionales BASC en el que luego de cinco días de intensa capacitación y evaluación los participantes

recibieron la acreditación como Auditor Internacional BASC. Este curso es organizado por la Organización Mundial BASC (WBO) bajo un criterio itinerante para dar oportunidad a profesionales de diversos países y empresas


At the end of June, the XXXI Course of Basc International Auditors was held in Lima in which after five days of intensive training and evaluation, the participants received accreditation as a Basc International Auditor. This course is organized by the World Basc Organization (WBO) under a traveling criterion to give opportunity to professionals from different countries and affiliates, to have competent people to support the process of compliance and continuous improvement of the Basc

Management System and Security Control. On that occasion they were 10 new certified professionals that henceforth, Peru Chapter will take into account for the various audits including Basc certification process.


The closing ceremony of the course was attended by Maria del Carmen Masias, president of Basc Peru, Jorge Valencia, director of Offer Control of the National Commission for Development and Life without Drugs (DEVIDA); Harvey Gomez, executive director of Basc Dominican Republic and instructor of the course, and Juan Mendoza

afiliadas, de contar con personas competentes que apoyen el proceso de cumplimiento y mejora continua del Sistema de Gestión en Control y Seguridad Basc. En dicha ocasión fueron 10 nuevos profesionales certificados que en adelante, el Capítulo Perú, tendrá en cuenta para realizar las diversas auditorías que comprende el proceso de certificación Basc.

A la ceremonia de clausura del Curso asistieron María del Carmen Masías, presidenta de Basc Perú; Jorge Valencia, director de Control de Oferta de la Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA); Harvey Gómez, director ejecutivo de Basc República Dominicana e instructor del curso; y Juan Mendoza Abarca, Primer Fiscal Antidrogas del Callao del Ministerio Público, quienes hicieron la entrega formal del diploma y el credencial respectivos.

Como se recuerda, Basc implementa en 14 países su Sistema de Gestión en Control y Seguridad que minimiza el riesgo de narcotráfico, lavado de activos, sabotaje, y otras amenazas que afectan la cadena de suministro conformada por exportadores, importadores, transportistas, terminales portuarios y aéreas, de almacenamiento, agencias marítimas y aduaneras, líneas aéreas y navieras, empresas de seguridad, entre otros. 

Abarca, Anti-Drugs Prosecutor of Callao, who made the formal delivery of the diploma and the respective credential.

As recalled, Basc implemented its Control and Security Management System in 14 countries which minimizes the risk of drug trafficking, money laundering, sabotage and other threats that affect supply chain comprised of exporters, importers, carriers, port and air terminals, storage, shipping and customs agencies, airlines and shipping companies, security companies, among others. 

Tendencias del mercado de la cocaína

MARKET TRENDS FOR COCAINE


De acuerdo al "Informe mundial sobre las drogas 2010" de la Oficina Contra la Droga y el Delito de las Naciones Unidas (UNODC), en los Estados Unidos se ha registrado una disminución a largo plazo de la demanda por cocaína. Se estima que en 1982 10,5 millones de personas habían consumido cocaína; en 2008 esa cifra fue de 5,3 millones, es decir la mitad. Sin embargo, el número de consumidores de esta droga en Europa se ha duplicado en el último decenio, de 2 millones en 1998 a 4,1 millones en 2008. En 2008, el valor del mercado europeo (US\$ 34.000 millones) era prácticamente igual al de América del Norte (US\$ 37.000 millones).

La región de América del Norte es el mayor mercado de cocaína del mundo, y le corresponde casi el 40%. En 2008 se necesitaron 196 toneladas métricas de cocaína pura para satisfacer la demanda en esa región. Para poder surtir esa cantidad (considerando las incautaciones, el consumo en los países de tránsito y la pureza), habría sido necesario despachar más de 309 toneladas métricas de la región andina hacia esa zona. Esa cantidad supone casi la mitad de la cocaína originaria de dicha región, cantidad menor a la de hace algunos años. Los análisis forenses de la cocaína incautada en EE.UU. revelan que la mayor parte de lo consumido en América del Norte fue producida en Colombia. Según el documento, el consumo de cocaína en EE.UU. viene disminuyendo desde hace tiempo, particularmente desde el 2006.

Europa: mercado creciente

El segundo mayor flujo de cocaína en el mundo es hacia Eu-




ropa, y aumenta con rapidez. Los mayores mercados para esta droga en Europa son el Reino Unido, España, Italia, Alemania y Francia. Los niveles de prevalencia del consumo de cocaína son mayores en Reino Unido y en España que en EE.UU. Se estima que el consumo de cocaína en Europa en 2008 fue de 124 toneladas y que para satisfacer esa demanda se transportaron 212 toneladas desde América del Sur, es decir casi una cuarta parte de la producción total. Una proporción mayor de esa cantidad procede del Perú y Bolivia. Fuente: UNODC. 

According to the "2010 World Drug Report" of the United Nations Office on Drugs and Crime (UNODC), a long-term decline in demand for cocaine has been reported in the United States. It is estimated that in 1982, 10.5 million people had used cocaine, in 2008 that figure was 5.3 million, or half. However, the number of consumers of this drug in Europe has doubled in the last decade, 2 million in 1998 to 4.1 million in 2008. In 2008, the European market value (U.S. \$ 34,000 million) was almost equal to that of North America (U.S. \$ 37,000 million).

The North American region is the largest cocaine market in the world and accounts for almost 40%. It took 196 metric tons of pure cocaine to satisfy demand in that region in 2008. To fill this (considering seizures, consumption in countries of transit and purity), it was necessary to dispatch more than 309 tons of the Andean region to the area. That amount represents nearly half the cocaine originating in that region, much lower than in recent years. Forensic analysis of cocaine seized in the U.S. reveal that most of what is consumed in North America was produced in Colombia. The report says cocaine use in the U.S. has been declining for some time, particularly since 2006.

Europe: increasing market

The second largest flow of cocaine in the world is towards Europe, and it grows rapidly. The largest markets for cocaine in Europe are the United Kingdom, Spain, Italy, Germany and France. Prevalence levels of cocaine are greater in the UK and Spain than in America. It is estimated that cocaine use in Europe in 2008 was 124 tons and to meet that demand 212 tons were transported from South America, almost a quarter of total production. A greater proportion of that amount comes from Peru and Bolivia. Source: UNODC. 

Comunidad Andina también apunta al programa OEA

ANDEAN COMMUNITY ALSO POINTS TO THE AEO PROGRAM

Los directores de Aduanas de los países de la Comunidad Andina (CAN) y el secretario general de la Organización Mundial de Aduanas (OMA), Kuneo Mikuriya, coincidieron en la necesidad de impulsar actividades y programas conjuntos para el fortalecimiento de capacidades, facilitación del comercio y modernización aduanera en la su-

The directors of customs in the countries of the Andean Community (CAN) and the secretary general of the World Customs Organization (WCO), Kune Mikuriya, agreed on the need to promote joint activities and programs for capacity strengthening, trade facilitation and customs modernization in


brejión andina. Arribaron a este acuerdo en el marco de la XXVI Reunión del Comité Andino de Asuntos Aduaneros realizado en Lima a finales del 2010.


La directora de Aduanas de Bolivia, Eva Quino, en su condición de presidenta del Comité Aduanero Andino, dijo que los países de la CAN esperan que la influencia de

the Andean subregion. They reached this agreement in the framework of the XXVI Andean Committee on Customs Matters Meeting held in Lima in late 2010.

The Director of Customs of Bolivia, Eva Quino, in her capacity as president of the Andean Customs Commit-

tee, said the CAN countries expect that the influence of the WCO expand and increase to other customs action designed to facilitate trade and improve the free movement of goods. This will allow the creation of the Andean AEO, subject that is analyzed by experts of the committee.

Fuente: Pymex.pe 

tee, said the CAN countries expect that the influence of the WCO expand and increase to other customs action designed to facilitate trade and improve the free movement of goods. This will allow the creation of the Andean AEO, subject that is analyzed by experts of the committee. Source: Pymex.pe 

Nueva normativa aduanera en China

NEW CUSTOMS LEGISLATION IN CHINA

Desde el 1 de enero pasado, en China están vigentes los recientes cambios referentes a nuevos requisitos para el despacho de los envíos de importación y exportación. En ese sentido, todos los importadores y exportadores de/a China están obligados a registrarse y obtener el Código de Registro de Aduanas (Código CR de 10 dígitos) o a utilizar un agente autorizado que ya lo posea.

Este código debe ser incluido en todos los formularios de declaración de aduanas para todos los envíos, excepto para documentos y efectos personales. Las empresas transportistas recomiendan que el exportador / importador se ponga en contacto con sus socios comerciales en China para asegurarse de que poseen el Código de Registro (Código CR) para acelerar el proceso del despacho aduanero, ya que en caso contrario, todos los envíos de importación o exportación se-


rán retenidos por las autoridades aduaneras chinas hasta obtener dicho código.

Así mismo, todos los envíos -a excepción de documentos- que se importen o exporten de/a China necesitan incluir en la documentación el Código Armonizado (Código HS) y una descripción detallada y veraz de las mercancías. El código HS ayuda a clasificar las mercancías y acelerar el despacho de aduanas. Estos nuevos requisitos se aplican a todos los operadores logísticos. *Fuente: TNT Express, DHL.* 

From January 1 in China the recent changes regarding new requirements for the clearance of import and export shipments are in effect. In that sense, all importers and exporters from / to China are required to register and obtain the Customs Registration Code (CR 10 digits) or use an

authorized agent who already has it.

This code must be included in all the customs declaration forms for all shipments, except for documents and personal effects. Transport companies recommend that the exporter / importer contact with business partners in China to ensure that they have the Registration Code (CR Code) to accelerate the process of customs clearance, because otherwise, all shipments of import or export will be retained by the Chinese customs authorities to obtain the code.

Also, all shipments, except for documents, which are imported or exported from / to China need to include in the documentation the Harmonized Code (HS Code) and a detailed and accurate description of the goods. The HS code helps with the classification of goods and accelerate the customs clearance. These new requirements apply to all logistics operators. Source: TNT Express, DHL 

Rige nueva norma de seguridad aduanera en Europa

NEW SECURITY STANDARD GOVERNS CUSTOMS IN EUROPE

Como parte del código aduanero de la Comunidad Europea, desde el 1 de enero de 2011 se encuentran en vigor los nuevos procedimientos de seguridad conocidos como Sistema de control de importaciones (ICS), sistema electrónico de manejo de la declaración sobre seguridad para la importación de mercancías dentro del territorio aduanero de la Unión Europea (UE).


El ICS ayudará a las autoridades aduaneras a realizar un análisis de riesgo de envíos en el primer puerto de entrada a la UE utilizando información electrónica antes de la llegada física del envío. Hasta antes, no existían requisitos legales para proporcionar información previa a la llegada; sin embargo, ahora las Declaraciones Sumarias de Entrada (ENS) electrónicas son obligatorias para todos los envíos de paquetes pequeños y carga que se originen fuera de la UE y se dirijan a cualquiera de los 27 estados miembros de la UE, Noruega o Suiza. Aunque aplican diferentes plazos de entrega para el envío de la información, esta regulación aplica a todos los medios de transporte (aéreo, carretero, marítimo y ferroviario).

La legislación del ICS se enmarca en el Plan Estratégico Multi-anual (MASP) europeo. Se trata de la hoja de ruta diseñada por la Comisión Europea para modernizar y fortalecer los procesos aduaneros con el objetivo de eliminar el papeleo. Esto forma parte de una serie de iniciativas que se materializarán en el periodo 2011 – 2014.

Desde el presente año, todos los agentes económicos que participan en las operaciones de aduana y logística internacional tendrán que proporcionar los datos de seguridad a través de declaraciones

electrónicas, antes de que las mercancías entren o salgan fuera de la Unión Europea.

Recientes incidentes de seguridad aérea de carga han demostrado que el refuerzo de los sistemas de Aduanas análisis de riesgos es esencial para una buena seguridad. El acceso temprano de los datos de seguridad, es decir, antes que las mercancías lleguen a la frontera, permitirá un movimiento de carga más eficiente permitiendo a las autoridades aduaneras realicen un mejor análisis de riesgo.


El tipo de datos de seguridad que se pide a los comerciantes varía en función de los medios de transporte y la fiabilidad de los agentes económicos que participan en la operación. Puede incluir, por ejemplo, una descripción de las mercancías, la información sobre el expedidor o exportador, la ruta de las mercancías y los peligros potenciales. Los plazos para la presentación de los datos preliminares de seguridad también varían de acuerdo a los medios de transporte: desde 24 horas antes de la carga de la carga marítima a 1 hora antes de la llegada para el tráfico por carretera o incluso menos para el transporte aéreo. Desde el 1 de julio de 2009 era posible que los comerciantes presenten su declaración anticipada de manera opcional. Desde el 1 de enero de 2011 es obligatoria. Fuente: Comisión Europea, UPS, Fedex, otros. 

From January 1, 2011, the new security procedures known as import control system (ICS) and the electronic system of management of declaration about security for the import of goods within the customs territory

of the European Union (EU) is in force as part of the Customs Code of the European Community.

The ICS will help Customs authorities to conduct a risk analysis of shipments in the first port of entry to the EU using electronic information before the physical arrival of the shipment. Before that, there were no legal requirements to provide pre-arrival information, but now the entry summary declarations (ENS) are mandatory for all shipments of small packages and cargo originating outside the EU and target any of the 27 EU member states, Norway or Switzerland. Although different deadlines apply for sending the information, this regulation applies to all means of transport (air, road, sea and rail).

The law of the ICS is part of the Multi-Annual Strategic Plan (MASP) in Europe. This is the roadmap designed by the European Commission to modernize and strengthen customs procedures in order to eliminate paperwork. This is part of a series of initiatives that will be materialized in the period 2011 to 2014. From this year, all traders involved in customs operations and international logistics will have to provide data security through electronic declarations before the goods enter or leave outside the European Union.

The deadlines for submission of preliminary safety data also vary according to the means of transport: from 24 hours prior to loading of cargo ships for 1 hour prior to arrival to road traffic or even less for air transportation. From July 1, 2009 it was possible for traders to submit their early statement as an option. From January 1, 2011 is mandatory. Source: European Commission, UPS, Fedex and others. 

La OACI revisa guía de seguridad de la carga

ICAO REVIEWS THE CARGO SECURITY GUIDE

La Organización de Aviación Civil Internacional (OACI) ha elaborado nuevas recomendaciones para la seguridad de la carga aérea siguiendo las operaciones de inteligencia realizadas a finales de octubre de 2010 para interceptar paquetes bomba en dos vuelos a Estados Unidos.


La organización anunció a finales del 2010 que las directrices de la revisión de seguridad de la cadena de suministro serían enviadas a los 190 países miembros hasta que estén listas en 2011. Las directrices se centran en medidas para inspeccionar la carga antes de ser enviada al aeropuerto y procedimientos para proteger los envíos de interferencias antes de ser cargados a bordo.

En particular, las directrices recomiendan que los Estados miembros de la OACI introduzcan tecnologías de detección de carga, aunque esto plantea problemas a los países relativamente pobres que no pueden contar con equipos de inspección asequibles. Así mismo, la recomendación de la OACI no precisa cómo grandes volúmenes pueden ser examinados antes de la carga.

Fuente: Janes 

The International Civil Aviation Organization (ICAO) has developed new recommendations for air cargo security following intelligence operations conducted in late October 2010 to intercept parcel bombs on two flights to the United States.

The organization announced at the end of 2010 that the guidelines of the security review of the supply chain would be sent to 190 member countries until they are ready in 2011. The guidelines focus on measures to inspect cargo before it is sent to the airport and procedures to protect the shipments of interference before being loaded on board.


In particular, the guidelines recommend that the Member States of ICAO introduce cargo detection technologies, but this create problems for relatively poor countries which cannot rely on affordable inspection equipment. In addition, the recommendation of ICAO does not specify how large volumes can be examined before they are loaded. Source: Janes 

Práctica de amenaza terrorista en puerto ENAPU-Arica

THE PRACTICE OF TERRORIST THREAT IN ENAPU-ARICA PORT

En los recintos portuarios del terminal Arica de la Empresa Nacional de Puertos de Perú (ENAPU), en febrero pasado se realizó un simulacro de amenaza terrorista, que consistió en una infiltración vía terrestre y marítima con la colocación de un artefacto explosivo. Durante el ejercicio, las autoridades

constataron que la instalación portuaria cumple con los parámetros y estándares de protección marítima para prevenir, detectar y mitigar, junto con una adecuada coordinación con los organismos afines de emergencia locales, la contención de este tipo de riesgos. ENAPU-Arica cuenta desde el

año 2004 con el asesoramiento de la OPR Germanischer Lloyd Chile, que en el terreno evaluó los procedimientos y planes de contingencia establecidos en el plan de protección de la instalación portuaria aprobados por la Autoridad Portuaria Nacional. Fuente: Mundo Marítimo. 

Last February a terrorist threat simulation was conducted in the port premises of the Arica terminal of Peru's National Ports Authority (ENAPU), which consisted of a land and sea infiltration by placing an explosive device. During the exercise, the

authorities found that the port facility complies with the maritime security parameters and standards to prevent, detect and mitigate the containment of such risks along with an appropriate coordination with related local emergency agencies. Since 2004,

ENAPU-Arica counts on the advice of OPR Germanischer Lloyd Chile which assessed the procedures and contingency plans in the field established in the protection plan of the port facility approved by the National Port Authority. Source: Mundo Marítimo. 



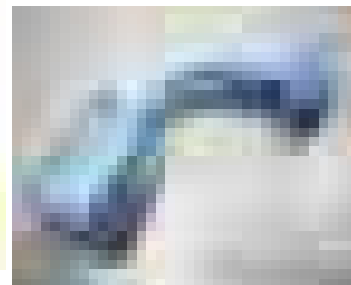
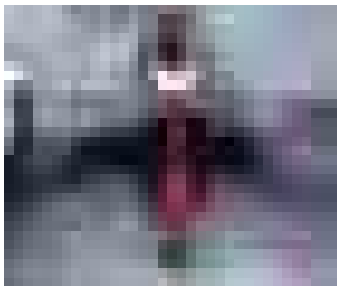
Más Opciones

Más Soluciones

FLINK SAC
Precintos y Dispositivos para Control y Seguridad

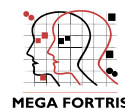
El Sauce 145 Surquillo - Lima - Perú. Teléfonos 273-7179 - 273-7178 Fax 273-7425

e-mail flink@terra.com.pe / ventas@precintosflink.com Visite www.precintosflink.com



KLICKER & FLEXIKLICK

CERTIFICADO ISO 17712 "H"
HIGH SECURITY SEAL
LA NUEVA GENERACION EN PRECINTOS DE SEGURIDAD



NO
ARRIESGUE



LA COMPETITIVIDAD
DE SU EMPRESA

IMPLEMENTE EL
SGCS - BASC

SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD BASC



BUSINESS ALLIANCE FOR SECURE COMMERCE

www.bascperu.org

Teléfono: (01) 612-8300 E-mail: afiliaciones@bascperu.org