

**CARGA AÉREA**

**Situación en la Unión  
Europea de la información  
anticipada**

**ITS SITUATION IN THE EUROPEAN UNION  
ADVANCE AIR CARGO INFORMATION**

**Empresas peruanas  
pueden certificar  
en Gestión Anti Soborno**

**PERUVIAN COMPANIES CAN CERTIFY  
IN ANTI BRIBERY MANAGEMENT**

**El terrorismo  
apunta a la  
expansión  
geográfica**

**TERRORISM POINTS TO  
GEOGRAPHIC EXPANSION**

ISO 18788:2015 - SGOS.  
La Internacionalización  
de la gestión de las  
empresas de seguridad  
(Pág. 22)

A 30 años de la  
Inspección No  
Intrusiva.  
(Pág. 24)

Programa CSI ha  
escaneado 65 millones  
de contenedores en 10  
años.  
(Pág. 29)

## ¿Qué sectores pueden contar con la Certificación BASC?

La Certificación BASC está presente en los siguientes sectores:



**Comité Editorial / Editorial Board**

Raúl Saldías Haettenschweiler  
Patricia Siles Álvarez  
César Venegas Núñez

**Director / Director**  
César Venegas Núñez

**Edición / Redacción / Editor / Writer**  
Unices Montes Espinoza

**Coordinación / Coordinator**  
Vanessa Alzamora

**Suscripciones y Publicidad / Subscription & Advertising**  
vanessa.alzamora@bascp Peru.org

**Diagramación e Impresión / Design and Press**  
Grupo Visión Publicidad S.A.C.



BUSINESS ALLIANCE FOR SECURE COMMERCE

Alianza Empresarial para un Comercio Seguro  
(Capítulo BASC PERÚ)

Jirón Francisco Graña 335, Magdalena del Mar  
Lima - Perú  
Teléf.: (511) 612-8300  
www.bascp Peru.org

**Consejo Directivo / Directors Board**

**Presidente del Directorio**  
Sociedad Nacional de Industrias - S.N.I.  
Raúl Saldías Haettenschweiler

**Vicepresidente**  
Sociedad de Comercio Exterior - COMEX  
Patricia Siles Álvarez

**Director Secretario**  
Asociación de Servicios Aeroportuarios Privados - ASAAP  
Arturo Cassinelli

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

**Director**  
Sociedad Nacional de Pesquería - SNP  
Ricardo Bernaldes Parodi

**Director**  
Asociación Peruana de Operadores Portuarios - ASPPOR  
César Ballón Izquierdo

**Director Vocal**  
Asociación Marítima del Perú - ASMARPE  
Guillermo Acosta Rodríguez

**Director**  
Asociación de Agentes de Aduana del Perú - AAP  
Jaime Miró Quesada Pflucker

**Director**  
Asociación de Exportadores - ADEX  
Rafael del Campo Quintana

**Director**  
Asociación Peruana de Agentes Marítimos - APAM  
Sabino Zaconeta Torres

**Director**  
Cámara de Comercio del Lima - C.C.L.  
Juan A. Morales Bermúdez

Consejo Nacional de Usuarios de Distribución  
Física Internacional de Mercancías - CONUDFI

**Past President**  
María del Carmen Masías

**Gerente General**  
César Venegas Núñez

Cargo Security® es una publicación trimestral 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)

# Contenido

## CONTENT

### PALABRAS DEL PRESIDENTE / WORDS OF THE PRESIDENT

**2** Satisfacción del deber cumplido  
SENSE OF ACCOMPLISHMENT

### BASC PERÚ 20 AÑOS / BASC PERU 20 YEARS

**5** BASC PERÚ 20 años. Temas, Empresas, Instituciones y Autoridades  
BASC PERÚ 20 YEARS. TOPICS, COMPANIES, INSTITUTIONS AND AUTHORITIES

### CIBERSEGURIDAD / CYBERSECURITY

**11** Perú incrementa su capacidad técnica en Ciberseguridad  
CIBERSEGURIDAD / CYBERSECURITY PERU INCREASES ITS TECHNICAL CAPACITY ON CYBERSECURITY

**14** Gestión de la Ciberseguridad según el ISO/IEC 27032:2012  
CYBERSECURITY MANAGEMENT ACCORDING TO ISO/ IEC 27302:2012

### PORTADA / COVER

**17** El terrorismo está apuntando a la expansión geográfica  
TERRORISM IS EXPANDING GEOGRAPHICALLY

### NORMALIZACIÓN / STANDARIZATION

**22** ISO 18788:2015 – SGOS. La Internacionalización de la gestión de las empresas de seguridad privada  
PRIVATE SECURITY COMPANIES MANAGEMENT GOING INTERNATIONAL

### COMERCIO SEGURO / SECURE COMMERCE

**24** A 30 años de la Inspección No Intrusiva  
30 YEARS FROM NON-INTRUSIVE INSPECTION

**26** El transporte aéreo mundial y la seguridad en el 2016  
WORLD AIR TRANSPORT AND SECURITY IN 2016

### INSPECCIÓN / SCREENING

**29** Programa CSI ha escaneado 65 millones de contenedores en 10 años  
65 MILLIONS OF CONTAINERS HAVE BEEN SCANNED BY THE CSI PROGRAM IN 10 YEARS

**31** Situación en la Unión Europea de la información anticipada para la carga aérea  
SITUATION IN THE EUROPEAN UNION OF ADVANCE AIR CARGO INFORMATION

### EMPRESAS / COMPANIES

**33** TALMA líder en servicios Aeroportuarios  
TALMA – LEADER IN AIRPORT SERVICES

**38** Corporación SEALERS inaugura nuevo laboratorio para precintos  
SEALERS CORPORATION INAUGURATES NEW LABORATORY FOR SEALS

### CORRUPCION / CORRUPTION

**35** Empresas peruanas pueden certificar en Gestión Anti Soborno  
PERUVIAN COMPANIES CAN CERTIFY IN ANTI BRIBERY MANAGEMENT

### MUNDO BASC / WORLD BASC

**39** ANAB realiza Auditoría Testificada a la auditoría de BASC PERÚ a TALMA SERVICIOS AEROPORTUARIOS S.A.  
ANAB CONDUCTS A WITNESS AUDIT TO THE AUDIT CARRIED OUT BY BASC PERU TO TALMA SERVICIOS AEROPORTUARIOS S.A.

**39** BASC PERÚ ponente principal en la Comisión de Alto Nivel Anti Corrupción (CAN)  
BASC PERU MAIN PRESENTER AT THE HIGH LEVEL ANTI-CORRUPTION COMMISSION

**40** Foro "Lavado de Activos"  
FORUM ON MONEY LAUNDERING



# Satisfacción del deber cumplido

## SENSE OF ACCOMPLISHMENT

**T**al como adelanté en nuestra edición anterior, con la tristeza del alejamiento, pero con la gran satisfacción de los logros alcanzados, ha llegado el momento de dejar la presidencia del Consejo Directivo de BASC PERÚ después de casi dos décadas de haber compartido con diferentes señores directores las decisiones que han guiado el accionar de nuestra organización.

En febrero de 1998 inicié mi participación como directivo de BASC PERÚ, habiendo ocupado desde entonces los cargos de Vocal, Vicepresidente y luego Presidente en tres periodos, dos veces representando a la Sociedad Nacional de Industrias (SNI) y una por el Consejo Nacional de Usuarios de Distribución Física Internacional (CONUDFI), incluyendo el cargo de Presidente del Consejo Directivo de la WBO (siglas en inglés de Organización Mundial BASC) durante dos mandatos de dos años cada uno, completando 04 años en tan honroso cargo.

Quien suscribe este editorial fue testigo del camino recorrido por esta noble organización sin fines de lucro que inició sus operaciones en condiciones muy precarias: su primera "sede" quedaba en un espacio (cedido en las oficinas de CONUDFI en el último piso de la antigua sede de ADEX) apenas suficiente para albergar un pequeño escritorio, una computadora y un archivador de metal, prestados por la Embajada de los Estados Unidos de América en Perú.

Su posterior crecimiento y desarrollo fue fruto del esfuerzo y la dedicación compartida entre sus directores, el primero de ellos liderado por Carlos Bruce y posteriormente, mi antecesor en el 2008, nuestro recordado colega Carlos Lazarte Hoyle (+), y los colaboradores que paulatinamente fueron cambiando.

Como sabemos, los diversos directorios "Ad honorem" que han dirigido los destinos de BASC PERÚ durante estos 20 años, son integrados por ejecutivos y funcionarios que representan a los gremios empresariales relacionados al comercio exterior peruano. Los fundadores fueron tres: Asociación de Exportadores (ADEX), Cámara de Comercio Americana del Perú (AmCham) y el Consejo Nacional de Usuarios del Sistema de Distribución Física Internacional (CONUDFI). Actualmente nuestro Consejo Directivo está conformado también por: Sociedad de Comercio Exterior (ComexPerú), Asociación de Servicios Aeroportuarios Privados (ASAEP), Sociedad Nacional de Pesquería (SNP), Asociación Peruana de Operadores Portuarios (ASSPOR), Asociación Marítima del Perú (ASMARPE), Asociación de Agentes de Aduana del Perú (AAP), Asociación Peruana de Agentes Marítimos (APAM),

**A**s I mentioned in our previous edition, I am sad to be leaving, but glad for the goals accomplished. It is time to leave the presidency of the Board of Directors of BASC PERU after almost two decades of having shared the decisions that have led the course of our organization with other directors.

In February 1998, I became part of the senior management team of BASC PERU, having served before as Member of the Board, Vice-president and then President in three periods, twice representing the National Society of Industries (SNI in Spanish) and one time representing the National Council of Users of the International Physical Distribution System (CONUDFI in Spanish), including the position of President of the Board of Directors of the WORLD BASC ORGANISATION (WBO) during two mandates of two years each, completing a total of for years in such distinguished position.

I have witnessed firsthand how far this notable non-profit organization has come since it started operating under very difficult conditions: its first "headquarter" was in a space (in the offices of CONUDFI on the last floor of the former office of ADEX), which was barely enough to set up a small desk, a computer, and a cabinet supplied by the Embassy of the United States of America in Peru.

Its further growth and development was thanks to the effort and dedication of its board of directors, the first one led by Carlos Bruce and then by my predecessor in 2008, our dear colleague Carlos Lazarte Hoyle (+), as well as all employees that changed gradually.

As we know, the different ad-honorem board of directors that have led the destiny of BASC PERU over the last 20 years, are formed by executives and businessmen that represent the trade unions related to Peruvian international trade. The founding members were three: The Association of Exporters (ADEX), the American Chamber of Commerce of Peru (AMCHAM) and the National Council of Users of the International Physical Distribution System (CONUDFI). Today, our Board of Directors also includes the Association of International Trade (COMEX PERU), the Association of Private Airport Services (ASAEP), the National Fishing Association (SNP), the Peruvian Association of Port Operators (ASSPOR), the Marine Association of Peru (ARMARPE), the Association of Customs Agents of Peru (AAP), the Peruvian Association of Maritime Agents (APAM), the National Society of Industries (SNI) and the Chamber of Commerce of Lima (CCL).

This industry presence gives us an entry to the private sector, which has been key to strengthen our growth. Also, our permanent work with the authorities has paved the way to expand out horizons by relating

Sociedad Nacional de Industrias (SNI) y Cámara de Comercio de Lima (CCL).

Esta representatividad que nos otorga el sector privado ha sido clave para fortalecer nuestro crecimiento, así como el trabajo permanente con las autoridades allanó el camino para ampliar nuestros horizontes al relacionarnos con importantes entidades supranacionales y nacionales.

Mantenemos convenios con la Autoridad Portuaria Nacional (APN), Cámara de Comercio Americana del Perú (AMCHAM), Centro de Información y Educación para la Prevención del Abuso de Drogas (CEDRO), Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA), Dirección General de Capitanías y Guardacostas (DICAPI), Ministerio del Interior con intervención de la Policía Nacional del Perú (PNP), Ministerio Público con intervención de la Fiscalía de la Nación, Poder Judicial (PJ), Superintendencia de Banca, Seguros y AFP (SBS) con intervención de la Unidad de Inteligencia Financiera (UIF).

Así hemos cerrado el círculo con tres grupos de Stakeholders: empresas, autoridades e instituciones; cada uno de ellos pilares fundamentales de nuestra organización y componentes de toda una comunidad de comercio seguro a nivel mundial.

El reconocimiento de esta comunidad hacia BASC PERÚ es producto de nuestra presencia activa en los temas de interés para la seguridad de la cadena de suministro, asuntos relacionados al tejido de la red internacional de riesgos y amenazas: narcotráfico, terrorismo, ciberataques, lavado de activos, contrabando, corrupción, robos sistemáticos, entre otros.

En los últimos diez años hubo logros importantes. En el 2008, BASC PERÚ logró ser el primer capítulo nacional BASC en obtener la certificación en la Norma de Gestión de Calidad ISO 9001, salto que reforzó su crecimiento y desarrollo.

En el 2009, por ejemplo, como consecuencia de las gestiones iniciadas por BASC PERÚ en Washington DC, con ocasión del IV Congreso Mundial BASC, se promovió un acercamiento entre la Oficina de las Naciones Unidas contra las Drogas y el Crimen (UNODC por sus siglas en inglés) y las autoridades peruanas para un proyecto, el cual ahora es una realidad en el puerto del Callao: el Programa Global de Control de Contenedores, cuya operación está a cargo de la Autoridad Portuaria Nacional (APN).

Asimismo, para apoyar el proceso de implementación en el Perú del Programa OEA, en el año 2010 se ejecutó un plan de apoyo a la SUNAT a través de la capacitación a sus funcionarios, lo que consideramos facilitó dicho proceso. Similar apoyo se brindó a la Aduana Nacional de Bolivia con miras a la creación de su propio programa OEA, lo cual sucedió en 2013.

En el 2011, tras la decisión de nuestro Consejo Directivo de contar con una sede institucional propia, se decidió iniciar el proceso correspondiente, el mismo que culminó con la inauguración de nuestra funcional sede institucional en febrero de 2016.

Bajo la decisión de seguir desarrollando nuestra

us with important supranational and national entities.

We maintain agreements with the National Port Authority (APN), the American Chamber of Commerce of Peru (AMCHAM), the Center of Information and Education for Drug Abuse Prevention (CEDRO in Spanish), the National Commission for Life without Drugs (DEVIDA), the General Directorate of Port Captaincy and Safeguard (DICAPI), the Homeland Security Department through the intervention of the National Police Department of Peru (PNP), the Public Ministry through the District Attorney Office, the Judiciary Branch (PJ), the Banking, Insurance and Retirement Pension Fund Superintendence (SBS) with the intervention of the Financial Intelligence Unit (UIF).

This way, we have come full circle with three groups of stakeholders: companies, authorities and institutions; each one represents a main pillar for our organization and are elements for a safe trade community at an international level.

The recognition of this community to BASC PERU is thanks to our active presence regarding issues of interest for a safe supply chain, affairs related to the international network of risks and threats: drug smuggling, terrorism, cyberattacks, money laundering, smuggling, corruption, systematic robberies, among other.

In the past 10 years, there were some major achievements. In 2008, BASC PERU managed to become the first national BASC chapter to obtain the Quality Management Standard ISO 9001 certification, thereby reinforcing its growth and development.

In 2009, for example, as a result of the initiatives of BASC PERU in Washington DC, on the occasion of the IV BASC World Congress, an approach between the United Nations Office of Drugs and Crime (UNODC) and the Peruvian authorities was encouraged for a project, which is now a reality in the Port of Callao: The Global Program of Containers Control, which is supervised by the National Port Authority (APN).

Also, to favor the implementation process of the OEA Program in Peru, in 2010, we executed a support plan to SUNAT by training its employees, facilitating such process. We also provided assistance to the National Customs Authorities of Bolivia towards the creation of its own OEA program, which was completed in 2013.

In 2011, after our Board of Directors agreed it was necessary to have our own institutional branch, it was decided to start the appropriate process, which came to a conclusion with the inauguration of our functional institutional headquarter in February 2016.

Considering it was necessary to continue fostering our continuous improvement, in 2015 it was decided to build up the skills of our own auditors to become "Lead Auditor" for the ISO 9001 (Quality), ISO 28000 (Security in the Supply Chain) standards. In addition, they received

mejora continua, en el 2015 se decide impulsar la capacitación de nuestros auditores con las competencias de "Auditor Líder" en las normas ISO 9001 (calidad), ISO 28000 (seguridad de la cadena de suministro), adicionalmente se les capacitó en las normas ISO 22301 (continuidad del negocio), ISO 27001 (seguridad de la información), ISO 31000 (gestión de riesgos) e ISO 19600 (compliance) con la prestigiosa Professional Evaluation and Certification Board (PECB), organización certificadora con sede en Canadá.

En esta misma senda, BASC PERÚ consigue en 2016 la acreditación ante la ANSI-ASQ National Accreditation Board (ANAB) como organismo certificador y casa matriz de las normas ISO 9001:2015 (calidad) e ISO 28000:2007 (seguridad de la cadena de suministro), convirtiéndose en el primer capítulo BASC en brindar el servicio de certificación ISO a nivel internacional. En ese mismo año se certificó a las primeras empresas en ambas normas.

En febrero del presente año, BASC PERÚ se convierte en el primer organismo certificador en formar un equipo de auditores líderes en la norma ISO 37001:2016 Sistema de Gestión Anti Soborno (SGAS), y actualmente se encuentra en proceso de acreditación a nivel de casa matriz para esta certificación ante la organización acreditadora ANAB, así como, adicionalmente, está en similar proceso de acreditación en las normas ISO 9001 (calidad), ISO 14001 (medio ambiente) e ISO 18001 OHSAS (salud y seguridad en el trabajo) ante INACAL.

En lo personal, acompañar a BASC PERÚ en esta ruta de logros y crecimiento ha sido el resultado de un compromiso de tomar en serio la lucha contra toda actividad ilícita que ponga en riesgo la seguridad del comercio peruano y de la cadena de suministro del comercio internacional. Profesionalismo e integridad han sido el motor propulsor y el timón, respectivamente, que han orientado nuestra navegación en mares no muy calmos durante estos años. ¿La recompensa? Es tan sencilla como invaluable: la satisfacción del deber cumplido.

Finalmente, mi reconocimiento a los ex presidentes y miembros de directorio que me antecedieron porque sin sus aportes no habría sido posible hacer de BASC PERÚ lo que es hoy. Con igual énfasis mi agradecimiento a nuestros colaboradores internos, de manera particular a César Venegas Núñez, nuestro gerente general, por el innegable profesionalismo y calidad de su gestión, así como a nuestros auditores externos que promueven con su labor un comercio exterior más seguro.

Muchas gracias a las 844 empresas afiliadas a BASC PERÚ, sin ellas no existiríamos ni tendríamos razón de ser. A ellas nos debemos y servimos.

Raúl Saldías Haettenschweiler  
Presidente / President  
BASC PERÚ

training on the ISO 22301 Standard (Business Continuity), ISO 27001 (Information Security Management), ISO 31000 (Risk Management) and ISO 19600 (Compliance) at the prestigious Professional Evaluation and Certification Board (PECB), certifying body with headquarters in Canada.

In 2016, following the same direction, BASC PERU obtained the accreditation before the ANSI-ASQ National Accreditation Board (ANAB) as certifying body and parent house of the ISO 9001:2015 (Quality) and ISO 28001:2007 (Security Management System for the Supply Chain). This made us the first BASC chapter to provide the ISO certification service at an international level. That same year, we certified the first companies in both standards.

In February this year, BASC PERU became the first certifying body to create a team of lead auditors in the ISO 37001:2016 Anti-Bribery Management System (SGAS) Standard. In fact, we are now going through an accreditation process, at a parent company level for this certification, before the certifying body, ANAB. Also, under accreditation process before the INCAL, are the ISO 9001 (Quality), ISO 14001 (Environment) and ISO 18001 OHSAS (Occupational Health and Safety) Standards.

On a personal note, I would like to say that accompanying BASC PERU along this course of achievements and growth is the result of our serious commitment about fighting all illegal activities that jeopardize the security of the Peruvian trade and the supply chain of the international commerce. Our professionalism and integrity have been the driving force leading our way during difficult years. And, our simple yet invaluable reward is the satisfaction of having fulfilled our duty.

Finally, my recognition goes out to all former presidents and members of the board of directors because without their contribution it would have been impossible for BASC PERU to be what it is today. Also, my highest gratitude to our internal employees, specially Cesar Venegas Nuñez, our General Manager, for his undeniable work ethic and outstanding performance during its management, as well as to our external auditors for fostering a more secure international trade.

Thank you very much to all 844 companies associated to BASC PERU, without you we wouldn't have a reason to be here. We exist thanks to all of you and put ourselves at your service.

# BASC PERÚ 20 años

## BASC PERÚ 20 YEARS

Temas, Empresas, Instituciones y Autoridades / TOPICS, COMPANIES, INSTITUTIONS AND AUTHORITIES

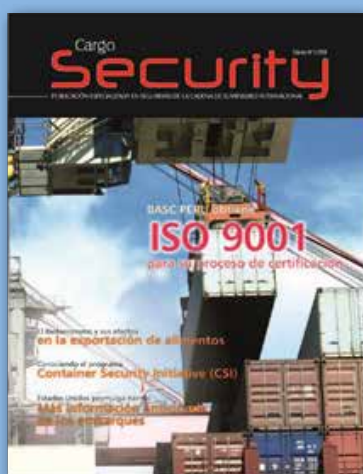
Finalizando nuestro homenaje a las dos décadas de existencia de nuestra organización, presentamos algunos momentos que han marcado los cambios y los desafíos que influyeron en el crecimiento y desarrollo de BASC PERÚ.

Finalizing our tribute to our two decades of existence, we present some moments that have marked the changes and challenges that influenced the growth and development of BASC PERU.

### 2008 A LA FECHA

#### INFORMACIÓN PARA LA CADENA DE SUMINISTRO

#### INFORMATION FOR THE SUPPLY CHAIN



Cargo Security salió a la luz en el 2008, coincidiendo con la obtención de la certificación en la Norma ISO 9001 Sistema de Gestión de la Calidad por parte de BASC PERÚ.

“Tiene en sus manos el resultado de la experiencia de una organización con más de 10 años de operaciones en el Perú desarrollando la nueva cultura empresarial del comercio seguro. El desafío es (...) modificar el paradigma del concepto de competitividad en la actividad de exportación en particular y del comercio exterior en general.”, señalaba en la presentación de la primera edición, el entonces presidente de BASC PERÚ, Raúl Saldías Haettenschweiler.

Cargo Security came to light in 2008, coinciding with obtaining ISO 9001 Quality Management System certification by BASC PERU.

“You have in your hands the result of the experience of an organization with more than 10 years of operations developing the new business culture of secure trade in Peru. The challenge is (...) to modify the paradigm of concept of competitiveness in exports in particular and of foreign trade in general.” pointed out in the presentation of the first edition, the then president of BASC PERÚ, Raúl Saldías Haettenschweiler.

### 2008 EL PROGRAMA OEA

#### THE AEO PROGRAM

A través de INFORMATIVO BASC PERÚ, boletín creado en 2002 (en la vista, la edición 46 de enero 2008), dimos cuenta del inicio en Europa del Marco Normativo para Asegurar y Facilitar el Comercio Internacional (SAFE Framework of Standards en inglés) a partir de enero de ese año. Actualmente este boletín circula vía on-line.

Through INFORMATIVO BASC PERÚ, our bulletin created in 2002 (the image is the 46th edition of January 2008), we covered the start in Europe of the SAFE Framework of Standards in January 2008. Currently this newsletter circulates via online.



### 1998 A LA FECHA

#### CONCIENCIANDO LA CADENA DE SUMINISTROS

#### AWARENESSING THE SUPPLY CHAIN

Una importante herramienta de concienciación utilizada por BASC PERÚ desde sus inicios, es la difusión de afiches, los cuales son donados a las empresas certificadas para que sean colocados en lugares estratégicos de sus instalaciones y oficinas.

An important awareness tool used by BASC PERU since its inception, is the dissemination of posters, which are donated to certified companies to be placed in strategic locations of their facilities and offices.



## La certificación BASC nos obligó a realizar ciertos controles que no hacíamos

FEDERICO ARNONE ARIZONA  
GERENTE GENERAL DE DEPSA

1) Considero que nuestra empresa tenía la necesidad de una certificación internacional si quería brindar un servicio para empresas exportadoras. Era un pedido de nuestros clientes. Sosiego que las certificaciones serán cada día más una exigencia si queremos participar en un mercado internacional, somos exportadores de nuevos productos no tradicionales en el mercado internacional y por ser un país en donde si siempre cosa, ayuda mucho contar con una certificación internacional.

2) La solicitud de certificación BASC nos obligó a realizar ciertos controles que anteriormente la empresa no los realizaba. Esto nos ayudó con algunos clientes exportadores, porque para ellos significaba una garantía que se cumplían normas que el gobierno norteamericano solicitaba para agilizar el ingreso de su mercancía en ese país del norte. Para nuestros clientes la significó agilizar sus operaciones de exportación.



3) Entre nuestros planes para el año 2007 está el de conciliar a todo nuestro personal, tanto en las plantas certificadas como en las que todavía no lo han realizado, que trabajen bajo las normas BASC nos da la garantía de que nuestros procedimientos son los adecuados para evitar sorpresas desagradables e inadecuadas. Me equivoqué de seguridad haciendo en el año de contar con el servicio logístico de seguridad e interferencias de

4 | Revista - Diciembre 2006

2006

## CAMBIO DE CULTURA EN LAS EMPRESAS PERUANAS

### CHANGE OF CULTURE IN PERUVIAN COMPANIES

En el 2006, cuando BASC PERÚ cumplía 9 años de operaciones, la certificación BASC, tras 4 años de creada, ya había logrado consolidarse como la herramienta líder del comercio seguro. Así lo establecían ejecutivos de empresas líderes.

In 2006, when BASC PERÚ was celebrating 9 years of operations, the BASC certification, after 4 years of creation, had already consolidated its position as the leading tool in secure commerce. This was recognized by executives of leading companies.

2006

## EL TERRORISMO TAMBIÉN

### THE TERRORISM ALSO

A finales de 2006, bajo la presidencia del Ing. Carlos Lazarte Hoyle (+), BASC PERÚ daba cuenta del giro institucional para estar al tono de la tendencia en esos momentos: el terrorismo se convertía en otro objetivo que cambiaría el contenido de nuestras operaciones.

At the end of 2006, under the presidency of Ing. Carlos Lazarte Hoyle (+), BASC PERU announce the institutional turn to be in tune with the trend at that time: terrorism became another objective that would change the content of our operations.

**Satisfechos por la labor cumplida**

Este mes de diciembre BASC PERÚ cumple nueve años de operaciones volando por la seguridad de la cadena logística de distribución de nuestro comercio exterior. Considero que se trata de una labor muy fructífera de la única organización privada que ha hecho suya la preocupación diaria por evitar que elementos delincuenciales utilicen los embarques de exportación para lograr sus fines delictivos.

Recordamos que hasta setiembre del 2001, nuestra preocupación se centraba en evitar la contaminación del contrabando y el narcotráfico fundamentalmente. Posterior a esa fecha, nuestro enfoque se ha ampliado para prestar también una atención particular a las acciones potenciales que puede realizar el terrorismo internacional.

En efecto, las grandes potencias (mercados de primera importancia) han hecho un tema de seguridad nacional el control de la cadena logística global que siguen los bienes (y personas) que ingresan a sus territorios.

En este sentido, las autoridades de esos países realizan cada vez más controles con mayor rigurosidad, en tanto que los importadores piden a sus clientes (proveedores) en el exterior más celo en asegurar sus mercaderías contra posibles intromisiones ilícitas. De ahí que nuestras exportaciones deben demostrar una cadena limpia y eficiente, lo cual se consigue sólo operando con sistemas de seguridad estandarizados y de reconocimiento internacional.

BASC ha demostrado cumplir esa exigencia y por ello ha venido destacando año tras año como una organización de primer nivel en todos los países que opera, logrando trabajar estrechamente con instituciones mundiales como la Organización Mundial de Aduanas (OMA) para enfrentar el reto de estandarizar el mundo, por ejemplo, hemos avanzado en medidas y gestiones reconocidas de seguridad logística.

Para el personal de trabajo que esperamos seguir de todos lados nuestras amistades como Estados Unidos.

Carlos Lazarte Hoyle  
Presidente



## 1998 A LA FECHA COOPERACIÓN INTERNACIONAL INTERNATIONAL COOPERATION

La cooperación internacional ha sido un soporte fundamental para el desarrollo de BASC PERÚ. Ejemplo de ello ha sido el apoyo recibido del US CBP a través del C-TPAT, cuyo Comisionado, Ralph Basham, envió en marzo de 2007, un Certificado de Reconocimiento a nuestra institución.

International cooperation has been a fundamental support for the development of BASC PERU. An example of this has been the support received from the US CBP through the C-TPAT, whose Commissioner, Ralph Basham, sent us in March 2007, a Certificate of Recognition.



### "... introdujimos los principios del BASC en la negociación del TLC y ellos recogieron estos temas para concordarlos con su CTPAT..."



Ahora, con la aprobación definitiva del esperado TLC con EE.UU., en manos del Ministerio de Comercio y Turismo (Mincetur) se encuentra el cabal aprovechamiento de las oportunidades que este ofrece para las empresas peruanas. La ministra Mercedes Araoz, nos demuestra en esta breve entrevista lo bien enterada y preparada que está, también, en el tema de seguridad para enfrentar su gran desafío.

Mercedes Araoz, ministra en funciones del Comercio Exterior, revelaba la influencia de BASC PERÚ en las negociaciones del tratado de libre comercio entre el Perú y los Estados Unidos. En su momento, otras altas autoridades han manifestado su complacencia de nuestro apoyo a los grandes objetivos del país.

## 1998 A LA FECHA INFLUENCIA EN POLITICAS DE GOBIERNO INFLUENCE ON GOVERNMENT POLICIES

Nuestra consolidación como entidad privada líder en comercio seguro, ha merecido el reconocimiento de las autoridades peruanas. Mercedes Araoz, actual presidenta del Consejo de Ministros y segundo vicepresidente del Perú, quien a finales de 2007, en su condición de ministra de Comercio Exterior, revelaba la influencia de BASC PERÚ en las negociaciones del tratado de libre comercio entre el Perú y los Estados Unidos.

En su momento, otras altas autoridades han manifestado su complacencia de nuestro apoyo a los grandes objetivos del país.

Our consolidation as a private entity lead in secure commerce, has earned the recognition of the Peruvian authorities. Mercedes Araoz, current president of the Council of Ministers and second vice president of Peru, who at the end of 2007, in her capacity as Minister of Foreign Trade, revealed the influence of BASC PERÚ in the negotiations of the free trade agreement between Peru and the USA.

At its time, other high authorities have expressed their satisfaction with our support for the country's major objectives

### Medidas para enfrentarlo requiere alianza entre los sectores público y privado

## La corrupción ha rebasado la capacidad del Estado

MEASURES TO FACE IT REQUIRE AN ALLIANCE BETWEEN THE PUBLIC AND PRIVATE SECTORS  
CORRUPTION HAS SURPASSED THE CAPACITY OF THE STATE



Entrevista al Sr. Ricardo Vinuales, Jefe Supremo Provisional de la Sala de Derecho Constitucional y Social Plenario de la Corte Suprema de Justicia de la República.  
Interview with Mr. Ricardo Vinuales, Provisional Supreme Judge of the Plenary of the Constitutional and Social Law of the Supreme Court of Justice of the Republic.

Por qué se dice que la corrupción representa una amenaza seria para el Estado de Derecho?  
Why do they say corruption represents a serious threat to the rule of law?  
La corrupción perverte el orden público, afecta e interfiere con la actividad económica, genera corrupción y corrupción de la actividad económica, interfiere con la actividad económica, interfiere con la actividad económica, interfiere con la actividad económica.

## La administración pública peruana aún no implementa la norma ISO 19600

THE PERUVIAN PUBLIC ADMINISTRATION HAS NOT YET IMPLEMENTED ISO 19600



Para Feod Khoury Z., Presidente Ejecutivo del Instituto Integridad y Gobernanza y ex Contralor General de la República, la corrupción cuesta al Perú más de 3,000 millones de dólares anuales en un soborno generoso con la impunidad y el no cumplimiento de las normas.  
According Feod Khoury Z., Executive President of the Integrity and Governance Institute and former Comptroller General of the Republic, corruption costs to Peru more than \$ 3,000 million annually in a generous bribe with the impunity and lack of compliance of the norms.

Hay corrupción en el sector público, gobiernos locales, gobiernos regionales, instituciones públicas y en el sector privado. Esta institucionalización de la corrupción refleja pobreza o carencia de valores, ética, y principios. ¿Cuál es el estado de la corrupción en el Perú?  
There is corruption in the public sector, local governments, regional governments, public institutions, and the private sector. This institutionalization of corruption reflects a lack or lack of values, ethics and principles. How do you think these illegal activities manifest corruption in Peru?

La corrupción sigue siendo uno de los principales problemas en el Perú.  
Corruption remains one of the main problems in Peru.

## Hay una reducción del espacio cocallero, pero aparecen nuevas rutas aéreas, marítimas, fluviales y terrestres.

THERE IS A REDUCTION OF THE COCA LEAF ROUTE, BUT THERE ARE ALWAYS NEW ROUTES APPEARING, WHETHER AIR, MARITIME, IN LAND OR BY RIVER.



Para la Presidente Ejecutiva de la Comisión Nacional para el Desarrollo y Vida sin Drogas-DEVIDA, Cecilia Medina, esta situación convierte a la lucha contra las drogas en un asunto más complejo.  
For the Executive President of the National Commission for the Development and Life without Drugs-DEVIDA, Cecilia Medina, this situation turns the battle against the use of drugs into an even more complex matter.

¿Cómo describiría brevemente la situación general del narcotráfico en el Perú durante los últimos cinco años?  
How would you briefly describe the general situation of drug smuggling in Peru over the last five years?  
El narcotráfico está siendo combatido desde muchos frentes. Los decretos de drogas se han implementado a partir del 2011 por parte del Procuraduría General de la Nación (PGN) y el organismo autónomo Integridad y Gobernanza (IYG) del Poder Judicial. Hemos managed to reduce the value for the transportation of cocaine by 50% in 2015. Thus, we are reducing the demand for the smuggling from the overseas.

### Gestión Gubernamental GOVERNANCE



"un programa de seguridad (...) es una iniciativa país en la que todos (...) debemos estar involucrados y trabajar conjuntamente"

"A SECURITY PROGRAM (...) IS AN INITIATIVE AS A COUNTRY IN WHICH WE ALL SHALL BE INVOLVED AND WORK JOINTLY"

Martín Ramos Chávez, Superintendente Nacional de la SUNAT  
Superintendent General of SUNAT.

El flamante principal funcionario de la autoridad aduanera nos ofrece su visión sobre temas clave de la seguridad del comercio exterior peruano.  
The brand new main official of the customs administration authority in Peru shares his vision regarding key issues on the safety of Peruvian foreign trade.

Como es de su conocimiento, desde los acontecimientos del 11-S de 2001 los mercados desarrollados incorporaron el tema de la seguridad...  
As you are aware, since the events of 9/11 2001, developed markets included the safety issue as a new element when managing...



## 2005 A LA FECHA COMERCIO SEGURO DESCENTRALIZADO

### DECENTRALIZED SECURE COMMERCE

La preocupación de BASC PERÚ por asegurar todos los eslabones del comercio exterior peruano, fortaleció la expansión de sus actividades en diferentes zonas del país.

En el 2005 la zona sur fue destino de una serie de actividades técnicas y de difusión, los cuales posteriormente se multiplicaron a nivel nacional.

The concern of BASC PERU to secure all the links of Peruvian foreign trade, strengthened the expansion of its activities in different areas of the country.

In 2005, the southern area was the destination of a series of technical and dissemination activities, which subsequently multiplied nationwide.

## 2006... NARCOTRAFICO SIGUE PREOCUPANDO

### DRUG TRAFFICKING STILL CONCERN

A pesar de los esfuerzos, no solo en el Perú, el narcotráfico se mantiene como una preocupación central para el comercio seguro. BASC PERÚ realiza diversas gestiones con la finalidad de desterrar este problema.

Despite the efforts, not only in Peru, drug trafficking remains a central concern for secure commerce. BASC PERU does efforts in order to eliminate this problem.



## 2007 CERTIFICACIÓN BASC FACILITÓ IMPLEMENTACIÓN DEL CÓDIGO PBIP

### BASC CERTIFICATION FACILITATE IMPLEMENTATION OF ISPS CODE

Tras la vigencia del Código Internacional para la Protección de Buques e Instalaciones Portuarias (PBIP) desde julio de 2004, BASC PERÚ enfatizó la certificación BASC de empresas peruanas, lo cual les facilitó implementar dicho Código con más facilidad.

After the begin of the International Ship and Port Facility Security Code (ISPS) in July 2004, BASC PERU strengthen he BASC certification of Peruvian companies, which made it easier for them to implement this Code.



Entrevista / Interview

## Énfasis en los controles, perfiles sospechosos y la presentación de la carga

### EMPHASIS ON THE CONTROLS, AND REPORTING SUSPICIOUS PROFILES OF THE LOAD

Estas son prácticas seguras claves para Trabajos Marítimos S.A. (TRAMARSA), cuyo gerente general, Mario Hart, destaca para dar a conocer los esfuerzos que realizan con el propósito de minimizar y neutralizar los riesgos de narcotráfico, terrorismo y robo en las cargas de sus clientes.

*These are safe keys for Trabajos Marítimos SA (TRAMARSA), whose general manager, Mario Hart, stands to publicize the efforts in order to minimize and neutralize the risks of drug trafficking, terrorism and robbery charges its customers.*



Considerando la presencia de actividades ilícitas en nuestro medio ¿Cuál es su preocupación de la actual situación de la seguridad logística en el comercio exterior?

Nuestra experiencia nos demuestra que debemos tener una preocupación latente, no se pueden descuidar las operaciones de carácter logístico que nos involucran. Hoy en

intrusión y el contrabando de drogas en las cargas de nuestros clientes.

¿Qué formas tienen las amenazas a la seguridad a la cadena de suministro y en especial la carga en las zonas de sus actividades?

Las amenazas son variadas la principal, como lo mencionamos anteriormente, es el narcotráfico. Pero

Due to the presence of illegal activities in our environment. What is your current concern about logistics security situation in foreign trade?

Our experience shows us that we have an underlying concern; we can not overlook the logistical operations that concern us. Today, the

## 1998... LIDERAZGO EMPRESARIAL COMPROMETIDO

### COMMITTED BUSINESS LEADERSHIP

BASC PERÚ fue creada por la empresa privada y con sus líderes estamos siempre trabajando con el interés mutuo de hacer más competitivo el comercio exterior peruano.

BASC PERU was created by the private company and with its leaders we are always working with the mutual interest of making to Peruvian commerce more competitive.

la / Interview

## El crecimiento no va de la mano con mayor infraestructura ni medidas para un comercio seguro

### GROWTH DOES NOT GO HAND IN HAND WITH MAJOR INFRASTRUCTURE OR MEASURES TAKEN FOR A SECURE COMMERCE

Pedro Olachea Álvarez Calderón, presidente de la Sociedad Nacional de Industrias, el Perú discute el éxito en crecimiento comercial y la amenaza de actividades ilícitas en la cadena de suministro nacional.



Pedro Olachea Álvarez Calderón, presidente de la Sociedad Nacional de Industrias / President of the National Society of Industries.

Pedro Olachea Álvarez Calderón, Presidente of the National Society of Industries, discusses the success between the commercial success and the threat of all the illicit activities in the International Supply chain.

El crecimiento del comercio exterior del Perú va de la mano de la

In the current positive economic situation of Peru and the

Entrevista / Interview

## Implementación del Usuario Aduanero Certificado debe ser lo antes posible

### THE IMPLEMENTATION OF THE CERTIFIED CUSTOMS USER MUST BE AS SOON AS POSSIBLE

Frente al actual escenario de comercio seguro que impera en el mercado global, Alfonso García Miño, presidente encargado de la Confederación Nacional de Instituciones Empresariales Privadas (CONIEP), sostiene que la implementación de esta figura basada en el programa Operador Económico Autorizado (OEA) de la Organización Mundial de Aduanas (OMA), asegurará la cadena logística del comercio peruano.



Facing the current scenario of secure trade that prevails in the global market, Alfonso García Miño, president in charge of the National Confederation of Private Business Associations (CONIEP), states that the implementation of this figure based in the Authorized Economic Operator's program of the World Customs Organization (WCO), will secure the logistics chain of the Peruvian trade.

Aunque para países como el nuestro puede no ser muy relevante, en los mercados más importantes del mundo la preocupación por un flujo

de lado el control de mercancías, para ello se debe ir pautas hacia una aduana moderna que permita un flujo comercial eficaz. En ese sentido, tenemos en

Despite the fact that for countries like ours that may not be quite relevant, in the worldwide biggest markets the concern about its

Entrevista / Interview

## "La seguridad es la inversión que constantemente se encuentra en nuestro radar"

### SECURITY IS THE INVESTMENT THAT IS CONSTANTLY ON OUR RADAR"



Para una corporación logística líder como BANSÁ, brindar soluciones para sus clientes va de la mano con brindar seguridad logística a sus cargas. Emilio Fantozzi Temple, gerente general del Grupo BANSÁ, nos detalla cómo cumplen eso.

For a corporation as BANSÁ leading logistics, providing solutions to its customers goes hand in hand with providing logistics security burdens. Emilio Fantozzi Temple, general manager of Grupo BANSÁ, details how they comply with that.

## "El BASC desempeña un papel de liderazgo en las Américas"

"THE BASC PLAYS A LEADERSHIP ROLE IN THE AMERICAS"



Para el señor Kunio Mikuriya, Secretario General de la Organización Mundial de Aduanas (OMA), este liderazgo es ejecutado "no sólo entregando el mensaje de seguridad a la comunidad empresarial, sino también subrayando la importancia de la cooperación con las administraciones de aduanas y las autoridades."

For Mr. Kunio Mikuriya, Secretary-General of the World Customs Organization (WCO), this leadership is executed "not only delivering the message of security to the business community, but also highlighting the importance of cooperation with Customs administrations and enforcement authorities."

**¿**Cuáles son los principales retos a los que se enfrenta la Organización Mundial de Aduanas (OMA) teniendo en cuenta el panorama actual del comercio mundial?

La OMA se compone de 182 Miembros, que van desde los países menos adelantados y los países en desarrollo hasta los países desarrollados. Sus desafíos en el actual panorama del comercio mundial?

**W**hat are the main challenges facing the World Customs Organization (WCO) given the current global trade landscape?

The WCO consists of 182 Members, ranging from Least Developed and Developing Countries to Developed ones. Their challenges in the current global trade landscape differ. We constantly develop and update instruments and tools that enhance trade facilitation.

2002...

## VITRINA MUNDIAL AUSPICIOSA AUSPICIOUS WORLDWIDE SHOWCASE

BASC PERÚ llega al actual desafiante escenario global con el claro propósito de ser un jugador líder en el campo de la seguridad de la cadena internacional de suministro.

Para ello, está potenciando progresivamente su condición de entidad certificadora a la altura de las necesidades globales de las empresas.

BASC PERU arrives to the current challenging global scenario with the clear purpose of being a leading player in the international supply chain security field.

For this, it is progressively enhancing its status as a certification entity that be at the global needs of companies.



"...las auditorías de BASC definitivamente pueden contribuir a nuestra validación positiva"

"...BASC AUDITS CAN CONTRIBUTE DEFINITELY TO OUR POSITIVE VALIDATION"

**B**rad Skinner, director del programa estadounidense C-TPAT (Customs-Trade Partnership Against Terrorism), el programa de seguridad líder a nivel mundial,

a 10.080 compañías asociadas, representando 11 sectores logísticos. Los 4.400 importadores que están participando en el programa representan más del 50% en términos de valor aduanero de todo

mejores prácticas, las cuales se están convirtiendo en estándares. "Participamos en muchos foros en Estados Unidos compartiendo nuestras experiencias, también estamos viendo que en muchas



Gracias al CICTE de la OEA

# Perú incrementa su capacidad técnica en Ciberseguridad

THANKS TO THE CICTE OF THE OEA

## PERU INCREASES ITS TECHNICAL CAPACITY ON CYBERSECURITY

**E**n abril de 2017 el Comité Inter Americano Contra el Terrorismo – CICTE (Inter-American Committee Against Terrorism) de la Organización de Estados Americanos (OEA) realizó su 17ava sesión en Washington, Estados Unidos, y entre los temas tratados estuvo la situación de la ciberseguridad en la región.

Como se sabe, desde el 2002 el CICTE ha desarrollado una amplia gama de actividades de asistencia técnica y de programas de fortalecimiento de capacidades para apoyar a los Estados Miembros de la OEA para prevenir, combatir y eliminar el terrorismo. Hoy, cuenta con 10 programas divididos en seis amplias áreas: controles fronterizos, controles financieros, protección de infraestructura crítica, asistencia legislativa y consultas, ejercicios de gestión de crisis, y desarrollo de políticas y coordinación internacional.

Con el rápido desarrollo del Internet y la extensión de su uso masivo en la región ha surgido la amenaza del crimen cibernético, la cual es enfrentada en cooperación con entidades nacionales y regionales de los sectores público y privado. La OEA trabaja en el fortalecimiento de las capacidades de seguridad cibernética entre sus Estados Miembros brindando asistencia técnica a nivel de políticas.

Durante la reunión señalada el pasado mes de abril, se presentó el documento Summary of Cybersecurity Activities Implemented by the CICTE Secretariat (Recuento de actividades de seguridad cibernética implementadas por la secretaria del CICTE) donde se puede apreciar detalles de las actividades realizadas en la región.

Según el informe, en el caso del Perú la entidad de la OEA inició su apoyo en abril del 2006 cuando representantes peruanos asistieron a un seminario sobre seguridad cibernética en Miami. Este tipo de asistencia a eventos técnicos prosiguió en diferentes destinos hasta el 2009. En mayo del 2010 un equipo de un proyecto de ciberseguridad de la OEA viajó a Lima en calidad de misión de asistencia técnica con la finalidad de desarrollar planes para la creación de un equipo de respuesta para incidentes de seguridad computarizada (Computer Security Incident Response Teams – CSIRT) y de una estrategia nacional de ciberseguridad.

En general, el recuento de eventos hasta el 2016 alcanza una cifra aproximada de 50 y se refieren a asistencias de técnicos peruanos a diversos tipos de

**I**n April 2017, the Inter-American Anti-Terrorist Committee–CICTE of the Organization of American States (OEA) held its 17th session in Washington, United States of America to discuss issues on cybersecurity in the region, amongst other.

As it is known, since 2002, the CICTE has developed a wide range of activities on technical assistance and capacities building programs to support the Member States of the OEA to prevent, combat and eradicate terrorism. Today, the CICTE has 10 programs divided in six broad categories: border controls, financial controls, critical infrastructure protection, legislation assistance and consulting, crisis management exercises, policy making and international coordination.

The rapid development of internet and spread of its mass use across the region has raised the threat of cybercrimes, which poses a risk to national and regional entities of the public and private sectors. The OEA is making efforts to strengthen the capacities on cybersecurity among its Member States, providing technical assistance on policy-making.

The Summary of Cybersecurity Activities Implemented by the CICTE Secretariat, detailing the activities held in the region was presented last April.

According to this report, in the case of Peru, the OEA started its support in April 2006 when Peruvian representatives attended a seminar on cybersecurity in Miami. This type of participation on technical events repeated in different destinations until 2009. In May 2010, a team from a cybersecurity project of the OEA travelled to Lima as technical assistance mission to work on plans for the creation of a Computer Security Incident Response Teams – CSIRT as well as a national strategy on cybersecurity.

In general, the number of events held until 2016 amount to around 50 and they all refer to the participation of Peruvian technicians in different types of training courses, national and international, including the ones mentioned herein below due to their importance regarding the development of the Peruvian technical capacity.

## Institucionalidad peruana para la seguridad cibernética

### INSTITUTIONAL STRUCTURE OF PERU FOR CYBERSECURITY

De acuerdo al CICTE, en el Perú el organismo que asume la responsabilidad en las iniciativas vinculadas con la seguridad cibernética y el delito cibernético es el PeCERT (Perú Coordinación de Emergencias en Redes Teleinformáticas) nombre del equipo peruano de respuesta a incidentes de seguridad cibernéticos (CSIRT por sus siglas en inglés), creado en 2009.

La asistencia técnica de la OEA para desarrollar un marco de seguridad cibernética para el país es asumida por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). La investigación de los delitos cibernéticos y las responsabilidades correspondientes le competen a la División de Investigación de Alta Tecnología (DIVINDAT), comprendida en la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú (PNP).

Si bien el PeCERT es un CSIRT operativo con responsabilidades a nivel nacional, en la actualidad se encuentra abocado a la tarea de revisar y actualizar sus mecanismos, procedimientos y políticas en materia de respuesta ante incidentes. Perú no cuenta con una estrategia o política nacional oficial de seguridad cibernética, pero trabaja actualmente en su elaboración.

En el aspecto legislativo, la aprobación de tres leyes –la Ley que Incorpora los Delitos Cibernéticos al Código Penal (Ley 27309), la Ley de Protección de Datos Personales (Ley 29733) y la Ley de Delitos Cibernéticos (Ley 30096)– ha fortalecido el marco jurídico con que cuenta el país para promover la seguridad cibernética y combatir el delito cibernético. Se encuentran en estudio otras modificaciones de leyes en vigor.

La DIVINDAT presenta una limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado. Además, mientras los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en el Perú, la conciencia social de la seguridad cibernética es generalmente baja.

According to the CICTE, in Peru, the authority in charge of initiatives related to security, cybersecurity and cybercrime is the PeCERT (Peru Coordination of Emergencies in Tele information Networks), name of the Peruvian team of cybersecurity incident response (CSIRT by its acronym in English), created in 2009.

The technical assistance of the OEA to develop a cybersecurity framework for the country is undertaken by the National Office of Electronic and Information Government (ONGEI). The investigation of cybersecurity crimes and the relevant accountabilities are undertaken by the Division of High Technology Investigation (DIVINDAT in Spanish), which belongs to the Criminal Investigation Department (DIRINCRI in Spanish) of the National Police Department of Peru (PNP).

Although PeCERT is an operating CSIRT with accountabilities at a national level, today it is focused on supervising and updating its mechanisms, procedures and policies regarding incident response issues. Peru does not have a strategy or national official policy on cybersecurity, but its currently working on it.

Regarding legislation issues, the approval of the three laws – the law that incorporates Cybercrimes to the Judicial Code (Act 27309), the Law to Protect Personal Information (Act 29733) and the Law of Cybersecurity Crimes (Act 30096)- has strengthened the legal framework of the country to promote cybersecurity and tackle cybercrimes. Other legal modifications are under consideration.

The DIVINDAT has limited technical capacity to handle electronic evidence in the court and lacks a disclosure policy for the private sector. Also, while the electronic government services and the electronic commerce continues to grow in Peru, the social awareness of cybersecurity is usually low.

Fuente / Source: Informe Ciberseguridad 2016, OEA – BID / Tendencias de seguridad cibernética en América Latina y El Caribe, OEA, 2014  
Cybersecurity Report 2016, OEA – BID/Trends on Cybersecurity in Latin America and the Caribbean, OEA, 2014.

capacitación, nacionales e internacionales, incluyendo a los que citaremos a continuación por su relevancia en el desarrollo de la capacidad técnica peruana.

En mayo de 2011 oficiales peruanos y de otros 30 países participaron en una reunión hemisférica de seguridad cibernética en Miami, donde se enfocaron en el fortalecimiento de la coordinación y el intercambio de información. En junio de 2012 oficiales peruanos participaron en un ejercicio de manejo de crisis de seguridad cibernética en Guatemala. Al siguiente mes, en Lima, un equipo de la OEA realizó una misión de asistencia técnica CSIRT y en julio los técnicos peruanos participaron en un evento similar en Uruguay. A finales de ese mes Perú organizó un curso de entrenamiento de manejo de incidentes y luego en setiembre siguiente un equipo peruano viajó a Canadá donde se realizó una mesa redonda para discutir la elaboración de políticas en ciberseguridad. En el mes siguiente Perú organizó una reunión de trabajo avanzado sobre intrusiones en redes.

En setiembre de 2013 el gobierno peruano, junto con la OEA, realizaron un ejercicio sobre manejo de crisis de seguridad cibernética basado en pruebas de canales de comunicación y la capacidad nacional del nivel de respuesta a los ataques. A finales de 2014 Perú atendió una reunión de trabajo sobre seguridad internacional y diplomacia en Colombia.

En abril de 2015 integrantes de un proyecto de ciberseguridad de la OEA realizaron una misión técnica en Lima para desarrollar la estrategia nacional de ciberseguridad con la contribución de entidades gubernamentales, autoridades policiales y judiciales, académicos y responsables de infraestructura crítica.

En marzo de 2016 cinco oficiales peruanos estuvieron presentes en Miami en un entrenamiento sobre ciberdelitos internacional en la preservación de evidencia digital e investigaciones basadas en Internet, organizado por los servicios secretos de EEUU y la OEA. A finales de ese mes, en Washington, representantes peruanos participaron en una discusión sobre el futuro de la gobernanza de Internet.

En ese mismo mes, OEA/CICTE condujo una misión técnica en Perú para presentar consideraciones y recomendaciones para el borrador de la estrategia nacional sobre ciberseguridad y discutir los siguientes pasos para concluir el proceso de la estrategia nacional. Posteriormente la organización presentó el documento "Cyber Security Considerations for a safer Peru" (Consideraciones de ciberseguridad para un Perú más seguro) proveyendo recomendaciones para la implementación segura de los objetivos de la Agenda Digital, lo cual mereció por parte del gobierno peruano que entregara al OEA/CICTE el marco de seguridad cibernética para su revisión.

En setiembre de 2016 el Perú fue seleccionado como beneficiario del proyecto Creating a Career Path in Digital Security (Creando un camino profesional en seguridad digital) una iniciativa desarrollada por el Programa de Ciberseguridad de la OEA en cooperación con Young Americas Business Trust and the Citi Foundation. Finalmente, en noviembre OAS/CICTE apoyó la participación de un oficial peruano en la conferencia Meridiano, un evento realizado en México con el propósito de compartir las mejores prácticas e intercambiar información sobre asuntos de protección de información para infraestructura crítica. ■

In May 2011, Peruvian officers and 30 from other countries attended a hemispheric meeting on cybersecurity held in Miami, where they focused on the strengthening coordination and exchanging information. In June 2012, Peruvian officers took part of a cybersecurity crisis management exercise in Guatemala. The following month, in Lima, a team of the OEA carried out a technical assistance mission CSIRT and in July, Peruvian technicians participated on a similar event in Uruguay. At the end of that month, Peru organized an incident management training course and then, in September, a team of Peruvians traveled to Canada for a round table to discuss policy-making strategies on cybersecurity. The next month, Peru arranged a work meeting about intrusion in networks.

In September 2013, the Peruvian government, together with the OEA, carried out an exercise on cybersecurity crisis management based on tests to communication channels and the national capacity to response to attacks. By the end of 2014, Peru attended a work meeting on international security and diplomacy in Colombia.

In April 2015, members of a cybersecurity Project by the OEA held a technical mission in Lima to develop a national strategy on cybersecurity with the help from government entities, police and judiciary authorities, scholars and parties responsible for critical infrastructure.

In March 2016, five Peruvian officers attended a training session held in Miami about international cybercrime as a way to preserve digital evidence and internet-based investigations, which was organized by the secret services of the USA and the OEA. By the end of that month, in Washington, Peruvian representatives took place in a debate on the future of governance in Internet.

That same month, the OEA/CICTE led a technical mission in Peru to present some inputs and recommendations for the draft of the national strategy on cybersecurity and discuss the following steps to complete the process of the national strategy. Then, the organization submitted the report "Cyber Security Considerations for a Safer Peru", making recommendations for the safe implementation of the objectives of the Digital Agenda, which Peru was supposed to present to the OEA/CICTE as part of the cybersecurity frameworks for its revision.

In September 2016, Peru was selected as beneficiary of the project "Creating a Career Path in Digital Security", an initiative developed by the Cybersecurity Program of the OEA in cooperation with Young Americas Business Trust and the Citi Foundation. Finally, in November OAS/CICTE supported the participation of a Peruvian official in the Meridian conference, an event held in Mexico to share the best practices and exchange information on the protection of information for critical infrastructure. ■

Fuente / Source: OEA – CICTE / BID

# Gestión de la Ciberseguridad según el ISO/IEC 27032:2012

## CYBERSECURITY MANAGEMENT ACCORDING TO ISO/IEC 27302:2012

(Parte I)

Por: Giancarlo Gómez Morales (\*)

En la Actualidad es muy común escuchar el término "Ciberseguridad" (Certificaciones, Postgrados, Maestrías, consultoras, equipamiento, etc.), término que ayuda a entender la importancia de la Seguridad y el debido resguardo de la información e infraestructuras en el ciberespacio. Pero este aspecto de la seguridad no es un tema nuevo, esta arista se encuentra inmersa en el campo de la seguridad informática y, en un ámbito más amplio, en la Seguridad de la Información. La siguiente tabla proporciona una visión general de algunas normas que usan la definición de ciberseguridad:

Today, it is very common to listen to the term "cybersecurity" (Certifications, Post-graduate courses, Masters, Consulting companies, equipment, etc.), a word that helps understanding the importance of Security and adequate safekeeping of the information and infrastructures in the cyberspace. However, this aspect of security is not a new, provided it is immersing in the field on cybersecurity, and, in a larger scope, in the Information Security. The following chart provides a general vision of some standards used to define cybersecurity:

N°	Origen	Documento	Término	Organización	CDI	Intención	Motivación	Amenazas
01	ISO/IEC JTC1/SC27	27032	Ciberseguridad	ISO	Sí	Solo los activos destinados a Internet	No Diferenciación entre las actividades maliciosas o no	Sólo los activos virtuales conectados a Internet, sin activos físicos
02	ISO/IEC JTC1/SC27	27000	Seguridad de la Información	ISO	Sí	Cualquier Origen de Riesgo en el Espacio Cibernético	No Diferenciación entre malicioso o no Intencional	Cualquier activo
03	UIT-T	X.1205	Ciberseguridad	UIT	Sí	Cualquier Origen de Riesgo en el Espacio Cibernético	No Diferenciación entre las actividades maliciosas o no	Cualquier activo
04	NIST	SP 800-39	Ciberseguridad	NIST	NO	Riesgo originado exclusivamente en el espacio cibernético	Sólo cubre orígenes maliciosos (ataques cibernéticos)	Sólo los activos virtuales conectados a Internet, sin activos físicos
05	ISACA	Cybersecurity fundamentals	Ciberseguridad	ISACA	Sí	Certificación CSX	Origen malicioso	Activos en el Ciberespacio



## El ISO/IEC 27032:2012

La norma ISO/IEC 27032:2012 “Tecnología de la información - Técnicas de seguridad - Directrices para la Ciberseguridad” (publicada en julio del 2012) proporciona un marco de orientación para mejorar el estado de la Ciberseguridad, usando para ello los aspectos estratégicos y técnicos relevantes para esa actividad y sus dependencias con otros dominios de seguridad, en particular:

- Seguridad de la información (considerando que la información es el activo más relevante de cualquier organización),
- Seguridad en redes,
- Seguridad en el Internet, y
- La protección de infraestructuras críticas de información.

## ISO/IEC 27032:2012

The ISO/IEC 27032:2012 “Information Technology” - Security Techniques – Guidelines for Cybersecurity” (Published in July 2012) provides a framework of guidelines to improve the condition of the Cybersecurity, using strategic and technical aspects that are relevant to such activity and its dependency relationship with other security areas, mainly:

- Information Security (considering information is the most important asset of any organization)
- Network Safety
- Internet Safety and
- Protection of Critical Infrastructure of Information

### Estructura de la Norma



### La naturaleza de la Ciberseguridad

La siguiente figura explica la relación entre la Ciberseguridad con otros ámbitos de seguridad, como la Seguridad de la Información, Seguridad de Red, Seguridad en aplicaciones, etc.

### Nature of Cybersecurity

The following figure explains the relation between Cybersecurity with other security fields such as Information Security, Network Security, Application Security, etc.



## Dominios de la Ciberseguridad

Los dominios de la Ciberseguridad son los diferentes campos de las actividades económicas, sociales y políticas donde se pueden presentar las amenazas. Como puede ser apreciado en el cuadro respectivo, cada dominio enfrenta diferentes tipos de amenaza.

## Cybersecurity Domains

The domains of Cybersecurity are the different fields of the economic, social and policy fields where threats could arise. As shown in the chart, each domain faces different types of threats.

N°	DOMINIO	DETALLE
01	Seguridad de las comunicaciones	Protección contra una amenaza a la infraestructura técnica de un sistema cibernético que pueda conducir a una alteración de sus características para llevar a cabo actividades no previstas por sus propietarios, diseñadores o usuarios.
02	Seguridad Operacional	Protección contra la corrupción prevista de procedimientos o flujos de trabajo que tendrán resultados que no fueron intencionados por sus propietarios, diseñadores o usuarios.
03	Seguridad de la información	Protección contra la amenaza de robo, supresión o alteración de datos almacenados o transmitidos dentro de un sistema cibernético.
04	Seguridad física	Protección contra amenazas físicas que pueden influir o afectar el bienestar de un sistema cibernético. Ejemplos podrían ser acceso físico a servidores, inserción de hardware malicioso en una red, o coerción de usuarios o sus familias.
05	Seguridad Pública/Nacional	Protección contra una amenaza cuyo origen proviene del ciberespacio, pero puede amenazar los bienes físicos o cibernéticos de una manera que tendrá un beneficio político, militar o estratégico para el atacante. Ejemplos podrían ser 'Stuxnet' o ataques a DOS a gran escala en utilidades, sistemas financieros de comunicaciones u otras infraestructuras públicas o industriales críticas.

**Dominios de la Ciberseguridad**  
Fuente: ENISA  
ggomez@esan.edu.pe

## Partes interesadas en el Ciberespacio

El Ciberespacio no pertenece a ninguna persona o empresa, todo el mundo participa y tiene participación en él, para los fines del ISO 27032 las partes interesadas en el Ciberespacio se clasifican en los siguientes grupos:

- Los consumidores, incluyendo personas y organizaciones privadas y públicas;
- Los proveedores, incluyendo, pero sin limitarse a los proveedores de servicios de Internet, y los proveedores de servicio de aplicaciones.

## Activos en el Ciberespacio

Un activo se define como algo que tiene valor para la organización. Hay muchos tipos de activos, incluyendo los siguientes:

- La información,
- Software,
- Hardware, tal como un computador;
- Servicios, como la electricidad;
- Las personas, sus habilidades y experiencia, y
- Los activos intangibles, como la reputación y la imagen ante los clientes.

## Cyberspace Stakeholders

Cyberspace does not belong to any person or Company. In fact, the entire world participates and is involved in it. For ISO 27302 purposes, the stakeholders of Cyberspace are classified as follows:

- Consumers, including natural persons and legal entities private and public.
- Providers, including but not limiting to internet service providers and application service suppliers

## Assets in the Cyberspace

An asset is defined as something valuable for the organization. There are several types of assets, including:

- Information
- Software
- Hardware, such as computer
- Services, such as electricity
- People, its skills and experience
- Intangible, such as reputation and image before clients

(\*) El señor Gómez posee las certificaciones CISO and CPO at OSIPTEL, LA ISO27001, ITIL, ISO 22301, ISO 31000, UNE 166002 / ggomez@esan.edu.pe  
Mr. Gomez holds the CISO and CPO certifications at OSIPTEL, the ISO 27001, ITIL, ISO 22301, ISP 31000, UNE 166002/ ggomez@esan.edu.pe



# El terrorismo está apuntando a la expansión geográfica

## TERRORISM IS EXPANDING GEOGRAPHICALLY

**E**n julio de 2017 el Departamento de Estado de Estados Unidos de América (United States Department of State) publicó su documento "Country Reports on Terrorism 2016" (Reportes Nacionales de Terrorismo 2016), señalando que aunque los ataques terroristas y las muertes por terrorismo disminuyeron globalmente por segundo año consecutivo en 2016, los grupos terroristas continuaron aprovechando territorios con gobiernos débiles y conflictos en curso para expandir su alcance y promover ataques alrededor del mundo.

Para este organismo estadounidense el Estado Islámico de Irak y Siria (ISIS por sus siglas en Inglés) siguió siendo la mayor amenaza terrorista para la seguridad global, pese a haber sido expulsado de aproximadamente una cuarta parte del territorio que tenía en Siria e Irak a principios de año, gracias a los esfuerzos combinados de las Fuerzas de Seguridad iraquíes y los grupos armados sirios, habilitados y respaldados por los 73 miembros de la Coalición Mundial para derrotar a ISIS.

Al mismo tiempo, los esfuerzos diplomáticos contribuyeron a fortalecer una amplia gama de controles de viaje que ayudaron a reducir el flujo de combatientes terroristas extranjeros a territorios controlados por ISIS en Irak y Siria. Así, junto con las muertes en el campo de

**I**n July 2017, the United States Department of State published its document "Country Reports on Terrorism 2016", stating that although terrorists' attacks and the fatalities caused by it have decreased at a global level for the second year in a row in 2016; some terrorists' groups continued taking advantage of weak government territories and conflicts in course to expand their scope and execute attacks around the world.

For this American agency, the Islamic State of Iraq and Syria (ISIS by its acronym in English) remains the largest terrorist threat for international security, even though it has been expelled of approximately a fourth portion of the territory that it had in Syria and Iraq at the beginning of the year, thanks to the joint efforts of the Security Authorities from Iraq and armed groups from Syria, supported by the 73 member of the World Coalition to defeat ISIS.

At the same time, the diplomatic efforts help strengthen a wide range of travel control that help reducing the flow of foreign terrorists to territories controlled by ISIS in Iraq and Syria. Still, due to the deaths on the battle field, the reduction of the flow of recruits left ISIS in its lowest point since 2014. However, ISIS (like other terrorists' groups) uses as strategy an intense geographic

batalla, la reducción del flujo de reclutas dejó a ISIS en su punto más bajo desde al menos 2014. Sin embargo, ISIS (como otros grupos terroristas) utiliza como estrategia un intenso flujo geográfico de sus integrantes, por lo que explota los flujos de refugiados y migrantes para camuflar el viaje de sus combatientes hacia países de interés para sus objetivos.

Por otro lado, el reclutamiento de extremistas violentos a través de las redes sociales siguió siendo fundamental para ISIS, por lo que Estados Unidos y sus socios trabajaron en estrecha colaboración con las compañías de medios sociales y otros para contrarrestar legalmente y restringir el uso de Internet con fines terroristas.

## Europa

De acuerdo al Departamento de Estado de EEUU, Europa sufrió amenazas terroristas de diversas fuentes en 2016, incluidas organizaciones terroristas extranjeras que operan desde Irak y Siria, como ISIS y al-Nusrah Front (filial de al-Qaeda en Siria) y de combatientes terroristas extranjeros europeos. Ante el aumento de la presión militar en 2016, ISIS realizó ataques terroristas contra objetivos simbólicos y espacios públicos europeos. Varios países miembros de la Unión Europea (UE) informaron un aumento en la tasa de retorno de combatientes terroristas extranjeros desde Siria e Irak.

## América Latina

En relación a Latinoamérica el documento "Country Reports on Terrorism 2016" afirma que las organizaciones delictivas transnacionales siguieron representando una amenaza importante para la región, y la mayoría de los países se esforzó por investigar las posibles conexiones entre las organizaciones terroristas y la actividad delictiva.

Para la región los desafíos relacionados con la delincuencia transnacional siguen siendo la principal preocupación de seguridad. La corrupción, la debilidad de las instituciones gubernamentales, la insuficiente cooperación interinstitucional, la legislación débil o inexistente y la falta de recursos siguieron siendo las principales causas. "Sin embargo, algunos países, como Brasil y Trinidad y Tobago, han logrado avances significativos en sus esfuerzos antiterroristas" señala el informe.

Asimismo, dice que el grupo terrorista Sendero Luminoso de Perú se mantuvo activo, pero con menor

flow of its members, exploiting the flow of refugees and immigrants to hide terrorists when they travel to countries of interest for their target.

On the other hand, the recruiting of violent extremists through social networks continues to be essential for ISIS. This is why the United States and its partners are working closely with social media and other parties to fight legally and restrict the use of internet for terrorism purposes.

## Europe

According to the Department of the United States of America, Europe suffered terrorist's attacks from different sources in 2016, including international terrorist's organizations that operate from Iraq and Syria, such as ISIS and al-Nusrah Front (branch of al-Qaeda in Syria) and European terrorists. Due to the increase of military presence in 2016, ISIS executed terrorist's attacks against symbolic targets and public European spaces. Several countries member of the European Union (EU) informed of an increase in the rate of return of international terrorists from Syria and Iraq.

## Latin America

Regarding Latin America, the "Country Reports on Terrorism 2016" states that the criminal organizational at an international level continued to represent an important threat for the region and the majority of the countries made an effort to investigate the potential connections between the terrorist's organizations and criminal activities.

For the region, the challenges related to international crimes remain the biggest security threat. Corruption, weakness of government

bodies, lack of inter-institutional cooperation, weak or lack of legislation and resources are still the main causes. However, some countries, such as Brazil and Trinidad and Tobago, have made significant progress regarding anti-terrorist efforts", states the report.

Also, it is said that the terrorist group from Peru, Sendero Luminoso, remained active, but with less strength, and focused mainly in criminal activities, while the borders of Argentina, Brazil and Paraguay remain an important regional connection of weapons, narcotics, counterfeiting, human trafficking, counterfeiting and money laundering, all of which are sources for funding terrorism.

**“Los grupos terroristas con base en el Medio Oriente encuentran algo de apoyo en América Latina a pesar de la distancia geográfica...”**

**“Terrorists groups based in the Middle East find a little of support in Latin America despite the long geographic distance...”**

fuerza, y se centró principalmente en actividades delictivas, en tanto que las áreas tri- fronterizas de Argentina, Brasil y Paraguay siguieron siendo un importante nexo regional de armas, narcóticos, productos pirateados, tráfico de personas, falsificación y lavado de dinero, todas fuentes potenciales de financiamiento para organizaciones terroristas.

Llama la atención la afirmación siguiente: “Los grupos terroristas con base en el Medio Oriente encuentran algo de apoyo en América Latina a pesar de la distancia geográfica. El llamado a combatir en Irak o Siria atrajo a un número limitado de reclutas de América Latina y partes del Caribe, que ofrecieron áreas de apoyo financiero e ideológico para ISIS y otros grupos terroristas en Medio Oriente y el sur de Asia. Además, en 2016 Hizballah mantuvo algunos partidarios financieros, facilitadores y simpatizantes en la región que podrían solicitar apoyo para desarrollar y expandir sus actividades allí.”


## Perú

En relación a Sendero Luminoso (SL) la agencia estadounidense considera que fue una amenaza continua en 2016 para la seguridad interna de Perú aunque constituida en una sola facción activa cuya área de actividad e influencia se limitaba a la zona de emergencia militar especial conocida como Apurímac, Ene y el valle del río Mantaro (VRAEM), una región remota y accidentada ligeramente más grande que Suiza, que representa más de la mitad de la cocaína producida en Perú.

Para mantenerse SL participa en todos los aspectos logísticos del narcotráfico en su área de influencia: recolecta “impuestos revolucionarios” de los involucrados en el tráfico de drogas, y por un precio, proporciona seguridad y transporta narcóticos a esas organizaciones.

En materia de seguridad fronteriza, las autoridades peruanas de inmigración recopilaron información biométrica limitada de los visitantes. A los ciudadanos de países vecinos se les permitió viajar al Perú por tierra utilizando solo tarjetas de identificación nacionales. No había requisitos de visa para los ciudadanos de la mayoría de países de Europa Occidental, Central y Oriental, así como de México.

El Gobierno peruano colaboró con la Oficina de Aduanas y Protección de Fronteras de los Estados Unidos (CBP) en el uso de la información del viajero para mejorar la seguridad al determinar y mitigar el riesgo del viajero antes de la llegada y la partida. En julio (2016), el gobierno de Perú comenzó a emitir pasaportes biométricos con medidas de seguridad mejoradas para los ciudadanos peruanos.

En octubre de 2014, la policía peruana arrestó a Muhammad Ghaleb Hamdar, ciudadano libanés sospechoso de tener vínculos con Hizballah. Según los informes, había residuos y restos de explosivos en su departamento. En abril de 2016 un juez extendió el período de detención preventiva de Hamdar otros 15 meses. En octubre, se solicitó una condena de 30 años de prisión para Hamdar por cargos de terrorismo y falsificación de documentos. Hamdar permanecía en prisión preventiva a fines de 2016. 

The following statements are to be noted: “Terrorists groups based in the Middle East find a little of support in Latin America despite the long geographic distance. The call to fight Iraq and Syria attracted a limited number of recruits from Latin America and part of the Caribbean, who offered financial support areas for ISIS and other terrorists groups in the Middle East and the south of Asia. Also, in 2016, Hizballah kept financial supporters, facilitators and supporters in the region that could provide support to conduct and expand their activities in that region.”


## Peru

Regarding Sendero Luminoso (SL), the American agency thinks that it was a continuous threat in 2016 for the internal security of Peru, although it is formed in only one active faction, which area of operation and influence is limited to the special military emergency area known as Apurimac, Ene and the valley of the Mantaro River (VRAEM), a remote and rugged area slightly larger than Switzerland, that represents more than half the cocaine produced in Peru.

In order to finance itself, SL takes part in all the logistic aspects of drug smuggling in its area of influence: gathering “revolutionary taxes” from the parties involved in drug trafficking, providing security in exchange of a payment and transporting drugs to these organizations.

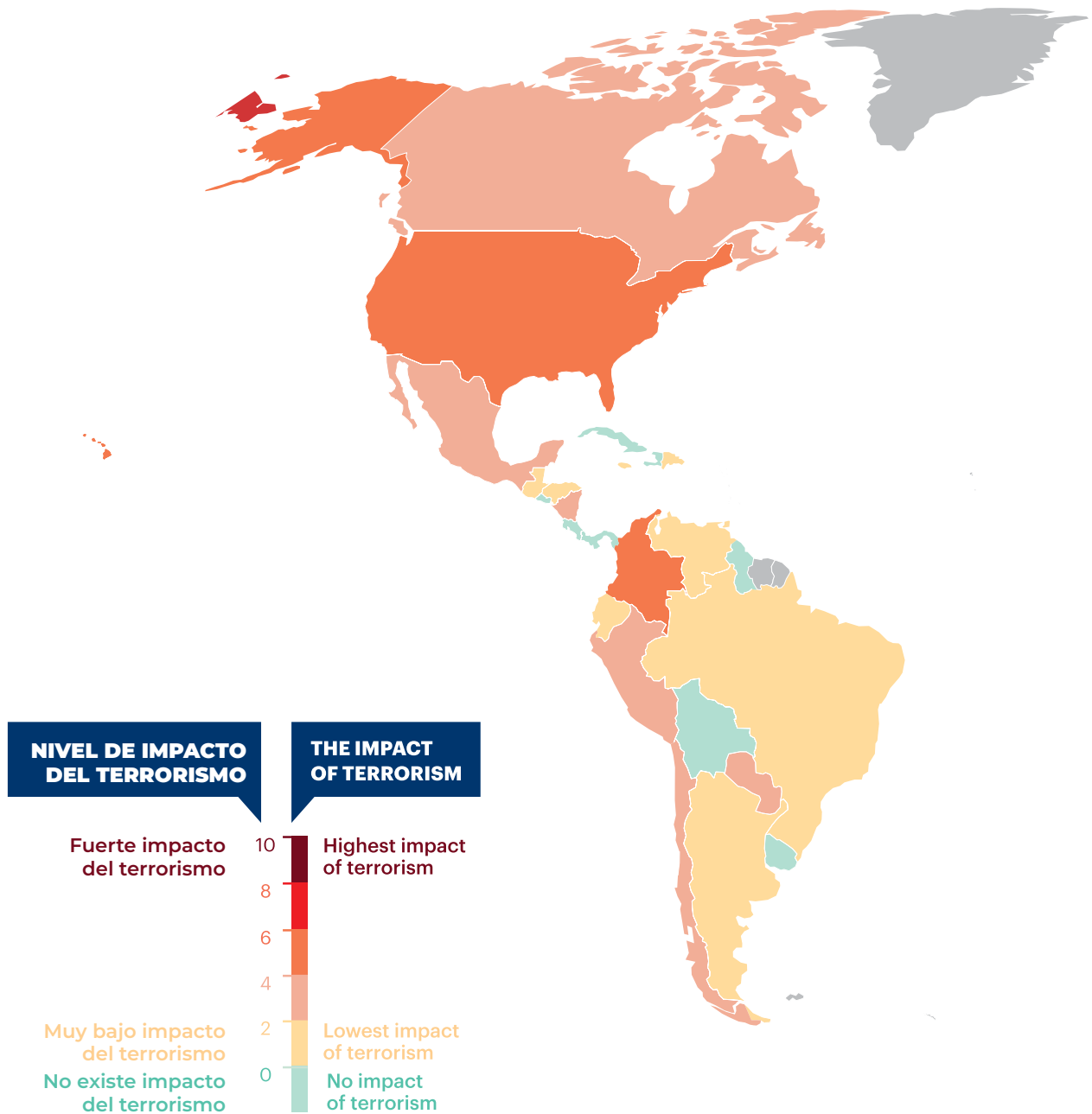
Regarding border security, Peruvian immigration authorities gathered biometric information limited to visitors. Citizens from neighboring countries were allowed to travel to Peru by ground transportation using only national identity cards. There were no visa requirements for most of the citizens from Europe Occidental, Central and Oriental as well as Mexico.

The Peruvian Government collaborated with the Customs and Border Protection Office of the United States in the use of the information of the traveler to improve security when determining and mitigating the risk of travelers before arriving and after the departure. In July 2016, the government of Peru started issuing biometric passports with better security measures for Peruvian citizens.

In October 2014, the Peruvian police arrested Muhammad Ghaleb Hamdar, Lebanese citizen which was a suspect of maintaining relation with Hizballah. According to the reports, there were wastes of explosives in his apartment. In April 2016, a judge extended the preventive prison period of Hamdar for 15 months. In October, it was requested a period of 30 years for Hamdar for terrorism and falsification of documents. Hamdar remained in preventive prison by the end of 2016. 

# IMPACTO GLOBAL DEL TERRORISMO

## GLOBAL IMPACT OF TERRORISM

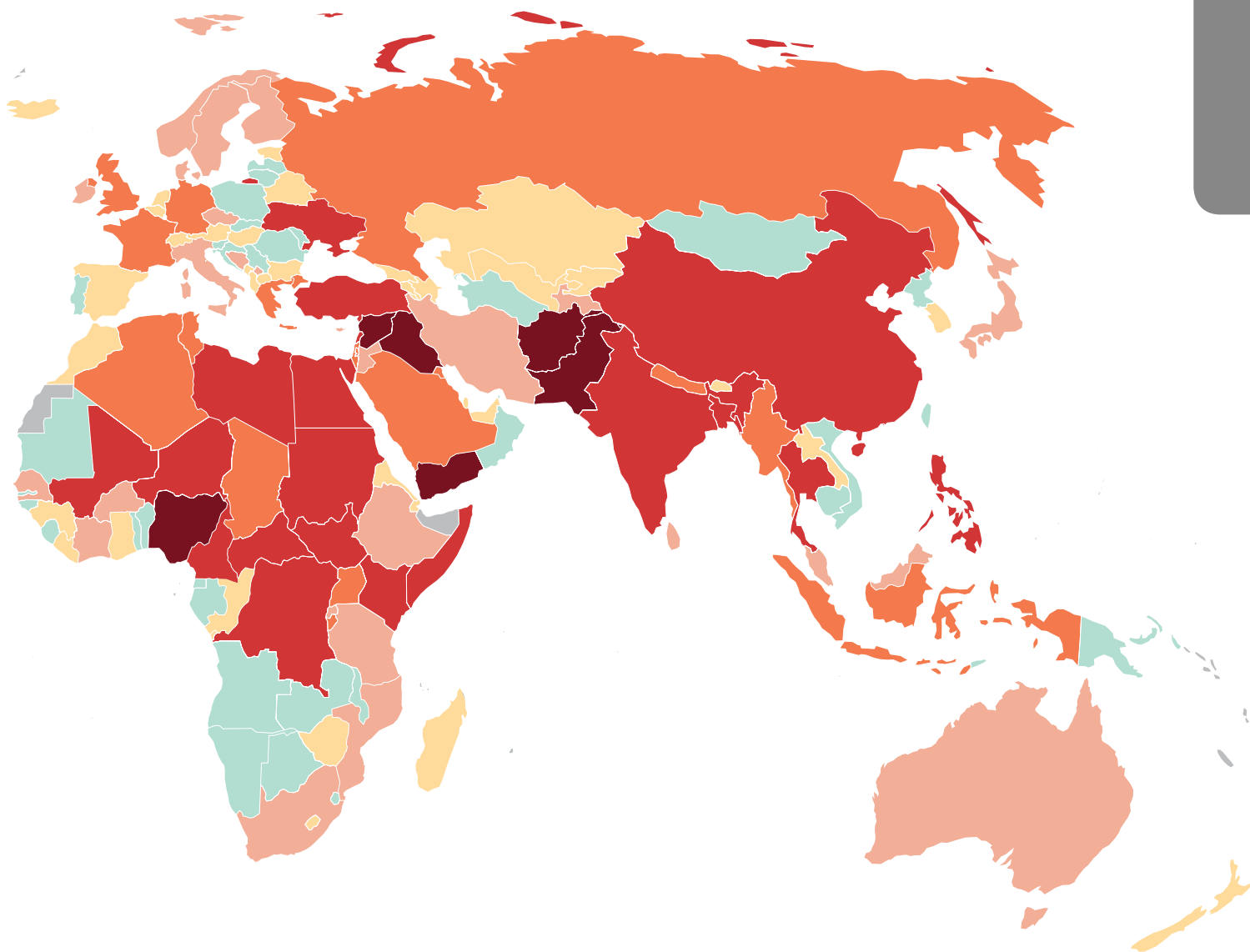


Fuente / Source: Global Terrorism Index 2016, The Institute for Economics and Peace (IEP)

El más reciente documento "Global Terrorism Index 2016" (Índice de Terrorismo Global 2016) que publica The Institute for Economics and Peace (IEP) revela que en 2015 las cifras totales de atentados y muertes por terrorismo descendieron en ambos casos en un 10%. El informe revela que se ha producido un cambio en el patrón de los últimos cuatro años. En el 2015 el número total de muertos descendió en un 10%, la

The latest document "Global Terrorism Index 2016" published by the Institute for Economics and Peace (IEP) showed that in 2015, the total figures of attacks and fatalities due to terrorism decreased by 10% in both scenarios.

The report stated that a change of pattern over the last four years have occurred. In 2015, the total number of fatalities decreased by 10%, the first plunge since 2010. However,



primera caída desde 2010. Sin embargo, la expansión de las actividades de algunos grupos terroristas a otros países está planteando nuevas amenazas en otras partes del mundo.

the expansion of activities of some terrorist's groups to other countries represent a new threat in other parts of the world.

Fuente / Source: Global Terrorism Index 2016



**Escribe: Ing. Miller Alexis Romero Cárdenas (\*)**

ISO 18788:2015 - SGOS

## La Internacionalización de la gestión de las empresas de seguridad privada

PRIVATE SECURITY COMPANIES  
MANAGEMENT GOING INTERNATIONAL

Por primera vez en la historia las empresas de seguridad privada podrán establecer un marco internacional de gestión que les permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar la gestión de sus operaciones.

Es el comité técnico ISO/TC 292 el encargado de la Seguridad y Resiliencia de la Sociedad, aquel que en su excelente gestión se ha encargado de normalizar para la seguridad de la cadena de suministro (Familia ISO 28000) y la Continuidad del Negocio (Familia ISO 22301), el que identificó la necesidad mundial de que las empresas que prestan o contratan servicios de seguridad privada presten sus servicios en un marco de cumplimiento legal (Compliance) y respeto por los derechos humanos.

El entorno mundial actual nos deja entrever claramente, que las empresas de seguridad privada no realizan evaluación y gestión alguna sobre los efectos de la ejecución de sus operaciones sobre las comunidades; es por ello que la norma internacional ISO 18788 basa sus requisitos en documentos internacionales que siempre han salvaguardado estos principios, como son el documento de Montreux el cual establece las obligaciones jurídicas internacionales y buenas prácticas de los estados relativas a las operaciones de empresas privadas militares y de seguridad durante el conflicto armado; el código internacional de conducta para los proveedores de servicios de seguridad privada (ICoC) y los principios rectores sobre empresas y derechos humanos de las naciones unidas en pro de "proteger, respetar y remediar".

Las empresas de seguridad privada que realmente deseen contar con una gestión moderna en sus operaciones, deben olvidar en su concepto estratégico la concepción de constituirse únicamente para proteger activos y la deben complementar con el respeto (Compliance) que deben tener con sus partes interesadas y la capacidad de remediar (Continuidad de negocio) los efectos que generen el normal desarrollo de sus actividades, en pro de proteger su imagen y reputación y la de sus clientes.

For the first time in history, private security companies will be able to establish an international management framework that enables them to establish, implement, operate, monitor, review, maintain and improve the management of their operations.

They will do this through the technical committee ISO/TC 292 is responsible for the Security and Resilience of the Society. This Committee has been in charge of establishing the standards for the security of the supply chain (ISO 28000 Family) and Business Continuity (ISO 22301 Family); it has also identified the world's need for companies to provide or hire private security services within a legal compliance framework (Compliance) and respect for human rights.

The current world scenario allows us to clearly see that the private security companies are not conducting any assessment or management on the effects of the execution of their operation on the communities. Therefore, the international ISO 18788 Standard bases its requirements in the international documents that have always safeguarded these principles, such as the Montreux, which establishes the international legal obligations and good practices of the states related to the operations of military private companies and security during the armed conflict; the international code of conduct for the private security services (ICoC) and the regulation principles on companies and human rights of the united nations to "protect, respect and remediate".

Private security companies that really want to have a modern management of their operations must leave behind their strategic concept of constituting themselves only to protect assets and shall complement it with the respect (Compliance) that their stakeholders shall have and the capacity to remediate (Business Continuity), the effects generated by the normal development of their activities, in favor of protecting their image and reputation and that of their clients.



Una empresa de seguridad privada que implemente y certifique el estándar ISO 18788:2015, podrá garantizar a sus partes interesadas que los derechos humanos y libertades fundamentales son respetados, salvaguardando vidas y bienes y previniendo actos ilegales, a través de un Sistema de Gestión de Operaciones de Seguridad Privada – SGOS – basado en la gestión de riesgos. Ahora, las empresas de seguridad privada tienen la oportunidad de mostrar y mejorar sus operaciones manteniendo su seguridad y la de sus partes interesadas.

Se moderniza la gestión de operaciones de seguridad al crearse la necesidad de que tanto empresas de seguridad privada como sus clientes, están en la obligación de realizar gestión de riesgos con la finalidad de prevenir incidentes, mitigar y remediar sus consecuencias y evitar su recurrencia.

Bajo la anterior premisa se crea la variable diferenciadora que en adelante los clientes establecerán a las empresas de seguridad como requisito para su continuidad y ser competitivos en el sector.

Es satisfactorio ver hoy en día cómo la organización mundial ISO ha venido trasladando al sector privado principios y buenas prácticas que anteriormente, se creía, correspondían únicamente al Estado, como es en este caso la protección de los derechos humanos y en otros similares la prevención del soborno/corrupción (ISO 37001).

Por primera vez una norma internacional ISO incluye el derecho internacional humanitario (DIH) como un requisito, derecho que puede ser violado en un contexto donde la gobernanza puede ser débil y el estado de derecho socavado.

Un sistema de gestión de operaciones de seguridad privada – SGOS -, al igual que todos los sistemas de gestión ISO, no asegura, pero incrementa la probabilidad de realizar operaciones más profesionales para sus clientes, proporcionando confianza a estos y a sus demás partes interesadas; en un marco de compliance (requisitos obligatorios/voluntarios) y respeto de los derechos humanos.

Manteniendo la línea de la seguridad en la cadena de suministro y la continuidad del negocio para la seguridad y resiliencia de la sociedad difundidas por el ISO/TC 292; esta norma basa su estructura de alto nivel y enfoque PHVA en la gestión de riesgos por cadena de suministro, componente infaltable de los sistemas de gestión ISO 28000 (SGSCS) e ISO 22301 (SGCN); de ahí la importancia de la competencia en gestión de riesgos por cadena de suministro para implementadores, administradores y auditores/evaluadores de un sistema de gestión de operaciones de seguridad – SGOS-.

Una norma ISO más que ratifica la eficacia del sistema de gestión en la calidad y efectividad de su modelo de gestión de riesgos; modelo que al adaptarse y apropiarse por la organización establecerá la línea para implementar los requisitos exigidos por la norma ISO 18788 y las buenas prácticas definidas en sus anexos de orientación para su uso.

Bienvenidas empresas de seguridad privada, a lo que se constituye ya, como el modelo más moderno e internacional para realizar operaciones de seguridad. ■

A private security company that implements and certified the ISO 18788:2015 standard will be able to ensure the respect to the human rights and fundamental liberties of their stakeholders, safeguarding lives and assets, thereby preventing illegal activities through the Private Security Operations Management System – SGOS - based on risk management. Today, private security companies have the chance to demonstrate and improve their operations maintaining their security and that of their stakeholders.

The operations management is renewed by creating the need that both private security companies and their clients are obliged to manage their risks to prevent incidents, mitigate and remediate their consequences and prevent its recurrence.

Under the premise above, the differentiating variable considering that from now on clients will established the security companies as requirement for their continuity and be competitive in the industry.

It is satisfactory to see today how the world organization ISO has transferred to the private sector principles and good practices that before belonged only to the government, as in the case of human rights protection and other similar to the prevention of bribery/corruption (ISO 37001).

For the first time, an international ISO standard includes the international humanitarian right (DIH) as requirement, a right that can be violated in a context where governance can be weak and the state of right undermined.

A private security operating management system – SGOS -, as other ISO management systems, does not assures, but increases the probability of conducting more professional operations for its clients, providing trust to them and other interested parties; in a compliance framework (mandatory/voluntary requirements) and respect for human rights.

Regarding security in the supply chain a business continuity for the security and resilience of the society published by ISO/TC 292; this standard bases its high level structure and PHVA approach in the risk management per supply chain, key element of the ISO 28000 (SGSCS) and ISO 22301 (SGCN) Standards. Therefore, the importance of the competence in risk management per supply chain for doers, administrators and auditors/assessors of a security operating management system-SGOS.

Another ISO standard that ratifies the efficiency of the quality management system and the efficiency of its model of risk management; which when adapting to the organization will establish a baseline to implement the requirements of the ISO 18788 and the good practices defined on its annexes.

Welcome private security companies, to what it is already known as the most modern and international model to conduct your security operations. ■

(\*) Gerente General de CONSULTORES & AUDITORES EN GESTIÓN SAS. Partner y Entrenador Autorizado PECB para Latinoamérica <https://www.linkedin.com/in/ingmillerrromero/>



# A 30 años de la Inspección No Intrusiva

## 30 YEARS FROM NON-INTRUSIVE INSPECTION

**H**istóricamente la usanza en el comercio internacional ha sido la gestión del control de la carga que ingresa al territorio de un país a través de un examen físico por parte de la autoridad aduanera. Esta operación cuya intención es verificar básicamente la conformidad del tipo de bien y su cantidad transportada, además de posibles productos de contrabando, continúa hasta hoy, aunque con una intención adicional: verificar si en el cargamento pudiesen estar escondidos armas y materiales de destrucción masiva que obedezcan a objetivos terroristas.

Actualmente, la misión antiterrorista de muchos países industrializados no se limita al examen físico de la carga cuando llega a sus puertos, sino también adicionalmente están utilizando sistemas de inteligencia de diversas fuentes para identificar envíos de alto riesgo con la finalidad de concentrar sus recursos de inspección en tales envíos.

En este marco, combinando políticas de facilitación del comercio legítimo con sus propias reglamentaciones de seguridad (restricciones y requisitos), estos países aplican centenares de leyes propias con sus decenas de agencias gubernamentales para mejorar sus posibilidades de detección de carga peligrosa o de alto riesgo.

Asimismo, como apoyo adicional a estas actividades, los países han emprendido iniciativas particulares como el uso de tecnología de inspección no intrusiva (NII por sus siglas en inglés), para aumentar la efectividad de la revisión de la carga sin ralentizar el flujo comercial.

### Tres décadas

De acuerdo a la Organización Mundial de Aduanas (OMA) los primeros sistemas NII fueron instalados a finales de la década de los 80 y hasta el 2008 en el mundo había 1.150 escáneres de contenedores que eran usados para controles aduaneros (300 en Norteamérica,

**H**istorically, the tradition in international commerce has been the management of the control of the cargo entering the territory of a country through physical exam by customs. This operation whose purpose is to basically verify compliance of the type of asset and the quantity transported; plus, the potential counterfeiting products, continues up to date, although it has an additional objective: verify if the cargo is hiding weapons and mass destruction materials for terrorist's purposes.

Today, the anti-terrorist mission of many industrialized countries is not limited to the physical examination of the cargo when it arrives to the ports, but also to use intelligence systems of different sources to identify high risk shipments to concentrate the inspection resources on such shipments.

In this framework, combining the policies of legal commerce facilitation with its own security regulations (restrictions and requirements); these countries apply thousands of own laws with many government bodies to improve their possibility to detect hazardous or high risk cargo.

Also, as additional support to these activities, the countries have developed specific initiatives such as the use of non-intrusive technology (NII) to increase the efficiency of the revision to the cargo without delaying the commercial flow.

### Three Decades

According to the World Customs Organization (WCO), the first NII systems were implemented at the end of the 80's and up to 2008, in the world, there were 1 150 containers scanners that were used for customs controls (300 in North America, 100 in Latin America, 150 in Africa, 300 in Europe, 100 in the Middle East and 200 in Asia).

According to the American Customs, today the United States of America has 309 NII systems distributed across its main entry ports, which enables to examine maritime

Latinoamérica 100, África 150, Europa 300, Medio Este 100 y Asia 200).

Según la aduana estadounidense, actualmente los Estados Unidos cuentan con 309 de sistemas NII desplegados en sus principales puertos de entrada, los cuales les permiten examinar contenedores marítimos, camiones comerciales y vagones de ferrocarril, además de vehículos privados. Para este país la detección de radiación es un componente estratégico de los sistemas de NII para combatir el terrorismo nuclear y radiológico.

Entre los tipos de estos equipos de detección que utilizan están el de Radiation Portal Monitors (RPM), Radiation Isotope Identification Devices (RIID) y los Personal Radiation Detectors (PRD). EEUU tiene actualmente desplegados 1.469 RPM, 2.811 RIID y 29.345 PRD en todo su territorio.

### Ejemplo en Sudamérica

La Organización Puerto Cartagena (principal puerto de Colombia) emplea herramientas de inspección no intrusiva (NII) desde mediados del 2016 para apoyar el trabajo de las autoridades con el objetivo de incrementar la competitividad colombiana mediante la reducción de tiempos y costos de trámites aduaneros.

Según la empresa, las máquinas garantizan la visión de imágenes en tiempo real. En contenedores pueden revisar hasta 80 vehículos de distintos tamaños por hora y en la carga en pallets acelera la revisión de cargas consolidadas, mientras que el equipo de Trazas puede trabajar en cualquier condición de iluminación e incluso detecta la presencia de químicos tóxicos industriales.

Con el uso de los escáneres los tiempos de inspección física han pasado de 24 horas, en promedio, a 15 minutos, reducción que permite la baja de costos de almacenaje. Asimismo, este nuevo sistema y la Nueva Regulación Aduanera permitirán reducir las operaciones marítimas de importación de 130 horas (estudio USAID 2016) a 48 horas.

El pasado enero de 2017 el gerente general de la Sociedad Portuaria Regional Cartagena afirmó en relación a este equipamiento que "Todo lo que se ve aquí en los sistemas de información hoy lo están leyendo los sistemas en Washington, que es lo que permite a la carga colombiana cuando llega a los puertos de EE.UU. para que obtengan un tránsito inmediato evitando demora en los puertos", sin duda una considerable ventaja comercial. El ejecutivo también señaló que la inversión en instalación, equipo y entrenamiento de personal, llegó a los 9 millones de dólares.

Fuente / Source: OMA / US CBP / Prensa internacional

containers, commercial trucks and railway wagons, apart from private vehicles. For this country, the detection of radiation is a strategic component of the NII systems to fight nuclear and radiologic terrorism.

Among the types of these detection equipment, there is the Radiation Portal Monitors (RPM), Radiation Isotope Identification Devices (RIID) and Personal Radiation Detectors (PRD). The United States of America, currently has 1469 RPM, 2811 RIID and 28345 PRD across its entire territory.

### Example in South America

The Cartagena Port Organization (main port of Colombia) uses non-intrusive tools (NII) since mid-2015 to support the work of authorities to increase the Colombian competitiveness by reducing timeframes and customs proceedings costs.

According to the company, the equipment ensures the visualization of images in real-time. In containers, they can examine up to 8 vehicles of different sizes per hour and in the cargo on pallets, it expedites the examination of consolidated cargoes; while the equipment of Trazas can work under any lighting condition and even detect the presence of industrial chemical toxics.

Thanks to the use of scanners, the physical inspection timeframes have gone from 24 hours, average, to 15 minutes; a reduction that also lowers the storage costs. Likewise, this new system and the new Customs Regulation allows to reduce maritime imports operations from 130 (USAID 2016 Study) to 48 hours.

Last January 2017, the general manager of the Regional Port Society of Cartagena stated that regarding this equipment "Everything seen here in the information systems is being read y the systems in Washington, which enables the Colombian cargo to have an immediate transit when it arrives to the ports of the United States of America, avoiding delays on the ports", which is a huge commercial advantage. He also noted that the investment for the installation, equipment and staff training amounted to 9 million dollars.

**M C L Z 5 0 0**

**BLOQUEA  
DOS PUERTAS  
CON UN PRECINTO**



Seguridad • Identificación • Control



MEGA FORTIS  
G R O U P

**COLOCACIÓN**



**LIBERACIÓN**





MCLZ 500

 Av. El Sauce 145 - Surquillo Lima - Perú

 Telf.: 273 7179 / 273 7181

 989 290 391

 ventas@flink.pe

[www.flink.pe](http://www.flink.pe)



# El transporte aéreo mundial y la seguridad en el 2016

## WORLD AIR TRANSPORT AND SECURITY IN 2016

**P**ara la International Air Transport Association (IATA) las medidas para seguir volando de manera segura han evolucionado durante los 16 años transcurridos desde el 11 de septiembre de 2001. Esta importante organización señala que los desafíos continúan, siendo que entre los retos más urgentes figuran la implementación de estándares globales y el intercambio de datos entre los gobiernos, las autoridades de supervisión y la industria.

Según refiere en su Memoria Anual 2017, lanzada en junio pasado, actualmente uno de los principales problemas que la industria aérea ve en el horizonte es la prohibición de artículos electrónicos en la cabina del avión, medida que se podría extender a otros países. Como se sabe, esta prohibición obedece a medidas de prevención establecidas por algunos países contra posibles acciones terroristas.

Para enfrentar la amenaza del terrorismo en la industria aeronáutica, en el 2016 la IATA pidió a los gobiernos trabajar en asociación, entre ellos y con las líneas aéreas, para contrarrestar estas amenazas, reconociendo en este ámbito el papel crucial de la International Civil Aviation Organization (ICAO u OACI por sus siglas en castellano). También instó a comprometer todos los recursos posibles, particularmente los recursos de inteligencia; y compartir información para asegurar que tales medidas sean apropiadas y efectivas.

En este escenario, los planes de seguridad de IATA cubren cinco elementos principales: 1) Promover normas mundiales, 2) Hacer frente a las amenazas emergentes, 3) Alentar una cultura de seguridad, 4) Promover el intercambio de información relacionada con la seguridad y, 5) Promover el reconocimiento normativo de los sistemas de gestión de seguridad y protección.

**A**ccording to IATA (International Air Transport Association) the measures to keep flying safely have evolved during these 16 years elapsed after September 11, 2001. This organization points out that there are still challenges, and one of the most urgent is the implementation of global standards and exchange of data between Governments, supervision authorities and the airline industry.

As per their 2017 Annual Review, published last June, one of the main problems in the airline industry is currently the aircraft cabin ban on Personal Electronic Devices, measure which might be extended to other countries. It is well-known that this ban was taken as a preventive measure stated by other countries against potential terrorist attacks.

In 2016, IATA requested the Governments to work together, between them and the airlines as to confront terrorist attack threats in the airline industry, acknowledging the crucial role of the International Civil Aviation Organization (ICAO). Likewise, IATA urged to use all the possible resources, mainly intelligence resources and to share information in order to assure such measures are appropriate and effective.

In this scenario, the IATA security plans comprise five main elements: 1) Foster world standards, 2) Confront rising threats, 3) Encourage a culture of security, 4) Boost exchange of data related to security and 5) Promote acknowledgement of regulated security and protection systems.

## Nuevo plan de seguridad

Actualmente está en marcha el Plan Global para la Seguridad de la Aviación GAsEP (Global Aviation Security Plan) que sustituye a la estrategia global de la OACI sobre Seguridad de la Aviación ICASS (ICAO Comprehensive Aviation Security Strategy). Es un plan en implementación que reunirá a la OACI, Estados, Industria y otras partes interesadas, para afrontar los problemas actuales y emergentes de la seguridad de la aviación mundial; siendo la seguridad un pilar fundamental para el crecimiento y la sostenibilidad de la industria de la aviación mundial.

## A new security plan

The GAsEP (Global Aviation Security Plan) for Aviation security is currently under way, which replaced the ICASS (ICAO Comprehensive Aviation Security Strategy), a global strategy from the OACI about Aviation Security. This is an ongoing implementation plan that will reunite the OACI, Governments, Airline Industry and other interested parties with the aim of confronting current and potential problems in the world aviation security for which security will be the main key to growth and sustainability of the world aviation industry.

## La carga aérea

### AIR CARGO

En relación a la carga aérea, según IATA en 2016 las aerolíneas transportaron 53.9 millones de toneladas métricas de mercancías, lo que representa alrededor del 35% del comercio mundial por valor, lo que equivale a 5.5 trillones de dólares en bienes al año, o 15.3 mil millones de dólares en bienes cada día. El crecimiento de la carga aérea se recuperó en 2016 luego de varios años de estancamiento.

El objetivo actual de la industria es desarrollar soluciones de cadena de suministro centradas en el cliente que mejoren la calidad, brinden una mayor visibilidad y permitan una mejor previsibilidad.

IATA está trabajando con transportistas, transitarios y toda la cadena de valor de la carga aérea para promover una agenda basada en la mejora de la digitalización de la industria a través de la creciente adopción de la hoja de porte electrónica y e-flete (e-AWB) y el desarrollo de plataformas y herramientas mejoradas de intercambio de datos; mejorar la seguridad, la protección y la eficiencia mediante la implementación y aplicación de normas y estándares internacionales, armonizando los objetivos y midiendo el desempeño de la cadena de carga aérea de extremo a extremo. Muchos programas en esta área se agrupan bajo la iniciativa StB Cargo (Simplificar el negocio de la carga aérea), que desde 2017 es el paraguas de todas las iniciativas de transformación en carga aérea.

Varios países, en particular, Canadá, Estados Unidos y los países miembros de la Unión Europea, están solicitando información anticipada de la carga antes de cargar la aeronave. Esta información (Pre-Loading Advance Cargo Information - PLACI), asegura un escrutinio adicional para mitigar los riesgos de seguridad.

IATA está trabajando con Canadá (programa Pre-Load Air Cargo Targeting – PACT); los Estados Unidos (Air Cargo Advance Screening – ACAS); y la Comisión Europea (programa PRECISE) para desarrollar sistemas de orientación electrónica que identifiquen la carga de alto riesgo antes de su carga. En 2016, IATA y FIATA (asociación de transportistas internacionales) acordaron manejar un programa de carga aérea administrado conjuntamente (Programa de Carga Aérea IATA-FIATA – IFAPC) diseñado para modernizar la relación entre los transportistas y las aerolíneas.

Regarding air cargo, according to IATA in 2016, airlines transported 53.9 million metric tons of merchandise, representing around 35% of world commerce per value, which is equivalent to \$ 5.5 trillion in goods yearly, or \$ 15.3 million in goods daily. The cargo growth was recovered in 2016, after several years of being stuck.

The airline industry's mean goal is to develop solutions of supply chain focused on the customers, improving quality and providing a higher visibility as well as allowing a better foreseeability.

The IATA is working along with carriers, freight agents and all the value chain involved in the air cargo industry in order to promote an agenda based on an industry digitalization improvement through the rising implementation of e-freight and e-AWB and development of platforms and tools improved for data exchange; as well as to improve security, protection and efficiency by implementing and applying international rules and standards, determining objectives and measuring the air cargo chain end to end. Several programs in this field are grouped under the StB Cargo (Simplifying the business cargo), which since 2017 is the umbrella for all the initiatives of air cargo transformation.

Several countries, mainly Canada, USA and member states EU member countries are requesting advance cargo information before being loaded to aircrafts. This information (Pre-Loading Advance Cargo Information - PLACI) guarantees an additional screening in order to mitigate security risks.

IATA is working together with Canada (Pre-Load Air Cargo Targeting – PACT program), USA (Air Cargo Advance Screening – ACAS) and the European Commission (PRECISE program) for developing electronic orientation systems, which can identify high-risk cargo before loading. In 2016, the IATA and FIATA (International Federation of Freight Forwarders Associations) agreed to manage jointly a program of air cargo (Air Cargo Program IATA-FIATA – IFAPC) designed to modernize the relation between carriers and airlines.

Entre los temas más importantes en el campo de seguridad que enfrenta la aviación comercial mundial se encuentra el intercambio de información entre las autoridades y los operadores aéreos. La IATA respalda plenamente una enmienda al Anexo 17 de la OACI que requiere que las naciones brinden información en apoyo de las evaluaciones de riesgo de los operadores, un componente integral de los sistemas de gestión de la seguridad (SeMS), pero las líneas aéreas continúan teniendo dificultades para acceder a la información de seguridad.

### La seguridad cibernética

La naturaleza interconectada de la aviación civil requiere un enfoque global, regional y local para abordar el creciente riesgo de la amenaza cibernética. En noviembre de 2016 se produjo la Declaración de Bucarest, documento que promueve la conciencia y la preparación para la seguridad cibernética y contiene recomendaciones para el intercambio de información sobre ciberseguridad.

IATA continúa asociándose con los cosignatarios del Plan de Acción de Ciberseguridad de Aviación Civil: OACI, Consejo Internacional de Aeropuertos (ACI), Organización de Servicios de Navegación Aérea Civil (CANSO) y el Consejo Internacional de Coordinación de Asociaciones de Industrias Aeroespaciales (ICCAIA).

### Seguridad inteligente

Smart Security (Seguridad Inteligente) es una iniciativa conjunta de IATA y el Airport Council International – ACI (Consejo Internacional de Aeropuertos) cuyo objetivo es un futuro donde los pasajeros pasen por controles de seguridad aeroportuaria con mínimos inconvenientes, donde los recursos de seguridad sean asignados en función del riesgo y donde se optimizan las instalaciones aeroportuarias. Los elementos de Smart Security se están introduciendo por etapas, comenzando con las innovaciones de procesos y pasando a tecnologías de detección avanzadas y la introducción de conceptos de seguridad basados en riesgos.

Smart Security no es una solución única para todos, y los aeropuertos que implementan sus diversos elementos están siendo asistidos con Smart Security Opportunity Assessments (SSOA). IATA ha llevado a cabo SSOA en 26 aeropuertos del mundo. En 2016, el progreso de Smart Security se realizó en América del Norte con la Autoridad Canadiense de Seguridad del Transporte Aéreo (CATSA) y la Administración de Seguridad del Transporte de EE. UU. (TSA).

### Prohibición de dispositivos electrónicos

En marzo de 2017, varios países implementaron la prohibición de dispositivos electrónicos personales más grandes que un teléfono celular, como computadoras portátiles, tabletas y reproductores portátiles de DVD, en la cabina de los vuelos internacionales a sus territorios. Esta medida obedece al temor de que tales dispositivos pueden ser usados para ocultar explosivos.

En mayo de 2017, IATA facilitó una cumbre de seguridad para abordar las preocupaciones emergentes sobre las restricciones a dichos dispositivos. La industria aérea está trabajando con los gobiernos para encontrar una solución aceptable a este problema de tal manera se minimice las molestias a los pasajeros. ☒

One the most important issues in the security field, which world commercial aviation has to deal with, is exchange of data between authorities and airlines. IATA fully backs up an amendment to ICAO's Annex 17, which requires countries to provide information for risks assessments of airlines, an overall component of the SeMS (Security Management Systems); however, the airlines keep finding difficult to access this security information.

### Cyber Security

The interconnected nature of civil aviation requires a global, regional and local approach in order to address the emerging risk of cyber security threats. In November 2016, Bucharest Declaration was proclaimed, document promoting awareness and preparation for cyber security and containing recommendations for data exchanging related to cyber security.

The IATA keeps associating with the Civil Aviation Cyber Security Action Plan signatories: ICAO, Airport Council International (ACI), Civil Air Navigation Services Organization (CANSO) and the International Coordinating Council of Aerospace Industry Associations (ICCAIA).

### Smart Security

Smart Security is an initiative together with IATA and the ACI - Airport Council International aiming at finding a future where passengers go through airport security screenings with minimal inconvenient, where security resources are to be assigned according to the risk and where airport facilities are optimized. The elements of Smart Security are being distributed by stages, starting from processes innovation, then cutting edge detection technologies to implementation of security concepts based on risks.

Smart Security is not an only one solution for everybody; airports implementing its different elements are assisted by Smart Security Opportunity Assessments (SSOA). The IATA has implemented the SSOA in 26 airports across the world. In 2016, Smart Security progressed in North America, a work together with the CATSA - Canadian Air Transport Security Authority and TSA – U.S.A. Transport Security Administration.

### Ban on Personal Electronic Devices

In March 2017, several countries implemented the measure of banning personal electronic devices bigger than a mobile phone, such as laptops, tablets and portable DVD players in aircraft cabins from international flights to their territories. This measure obeys to fear that such devices can be used to hide explosive.

In May 2017, the IATA organized a security summit with the purpose of addressing all the emerging concerns related to bans on such devices. The airline industry is working along with the Governments as to find an acceptable solution to this problem such that the inconvenient caused to the passengers can be minimized. ☒

# Programa CSI ha escaneado 65 millones de contenedores en 10 años

65 MILLIONS OF CONTAINERS HAVE BEEN SCANNED BY THE CSI PROGRAM IN 10 YEARS

El programa Container Security Initiative (CSI), creado en 2006, opera en 60 puertos ubicados en 35 países, desde los cuales provienen más del 85% de todos los contenedores de carga con destino a puertos estadounidenses. Los puertos CSI se ubican en el Norte, Sur y Centroamérica, Europa, Asia, África y el Oriente Medio.

The CSI - Container Security Initiative program, created in 2006, operates in 60 ports located in 35 countries, which more than 85% of all the cargo containers are coming from with destination to American ports. The CSI ports are located in the North, South and Central America, Europe, Asia, Africa and Middle East.

De acuerdo al World Shipping Council (WSC), la organización mundial que agrupa a los transportistas navieros, hasta el 2014 eran transportados a nivel mundial 255.2 millones de contenedores TEU's (todos totalmente cargados) sumados los de exportación e importación. Los dos principales países que mueven más de estos contenedores son Estados Unidos y China.

En exportación China ocupa el primer lugar (ver cuadro), habiendo registrado en dicho año 36 millones de TEU's frente a los 11.9 millones de TEU's por los Estados Unidos. En importación los papeles se revierten: el primer lugar lo ocupó los Estados Unidos con 19.6 millones de TEU's y China el segundo puesto con 14.7 millones de TEU's. Respecto a la Unión Europea (UE), en el 2014 sus exportaciones alcanzaron los 16.02 millones de TEU's y

According to the WSC - World Shipping Council, global organization encompassing sea freights, 255.2 millions of TEUs containers (fully loaded) were transported globally up to 2014, including export and import containers. The two main countries transporting most of these containers are the USA and China.

Regarding exports, China holds the first place (see table below), having recorded during said year, 36 millions of TEUs containers, in comparison to 11.9 million of TEUs of the USA. When come to import the role is inverted: The USA holds the first place with 19.6 million of TEUs and China in second place with 14.7 million of TEUs. Regarding the EU – European Union, its exports reached 16.02 million of TEUs and export, 17.52 millions of TEUs in 2014. Overall, 90% of commerce is

## Exportadores top de carga contenerizada

En Millones de TEU's

Top Cargo container exporters in millions of TEUs

	País	2014	2010
1	China	36.00	31.30
2	USA	11.90	11.20
3	South Korea	5.93	5.20
4	Japan	5.28	5.74
5	Indonesia	4.00	3.00
	WORLD	127.60	--
	EU Total	16.02	14.85

## Importadores top de carga contenerizada

En Millones de TEU's

Top Cargo container importers in millions of TEUs

	País	2014	2010
1	China	19.6	17.6
2	USA	14.70	12.0
3	South Korea	6.55	6.10
4	Japan	5.09	4.50
5	Indonesia	3.17	2.50
	WORLD	127.60	-----
	EU Total	17.52	16.78

Fuente / Source: World Shipping Council

### ¿Qué hace la CSI?

- Identifica contenedores de riesgo elevado. El US CBP emplea tecnología automatizada para identificar los contenedores que plantean un riesgo potencial terrorista, basado en trabajo de inteligencia.
- Inspecciona y evalúa los contenedores antes de que sean embarcados hacia EEUU. Los contenedores son protegidos desde el inicio en la cadena de suministro, en el puerto de salida.
- La tecnología empleada permite inspeccionar los contenedores para asegurar que la selección puede ser hecha rápidamente sin reducir la velocidad del flujo del comercio. Esta tecnología incluye el rayo X y máquinas de rayo gamma y dispositivos de detección de radiación.

### Los puertos CSI en Centro y Sudamérica

Los puertos panameños de Colón, Manzanillo y Balboa; Freeport (Bahamas), Caucedo (República Dominicana), Kingston (Jamaica), Puerto Cortes (Honduras), Puerto de Cartagena (Colombia), Santos (Brasil), y Buenos Aires (Argentina), son los que cuentan con la implementación del programa CSI.

### What does the CIS do?

- Identify high-risk containers. The US CBP uses automated technology to identify containers posing a potential terrorism risk, which is based on intelligence work.
- Check and assess containers before being shipped to the USA. Containers are protected from the beginning of the supply chain in the port of exit.
- This used technology allows the inspection of containers to guarantee that when being selected, this can be done fast without affecting the commerce flow speed. This technology includes X-ray, Gamma ray machines and radiation detection devices.

### CSI ports in Center and South America

The CSI program has been implemented in Panama ports of Colon, Manzanillo and Balboa Freeport (Bahamas), Caucedo (Dominic Republic), Kingston (Jamaica), Puerto Cortes (Honduras), Puerto de Cartagena (Colombia), Santos (Brazil), and Buenos Aires (Argentina) ports.

Fuente / Source: US CBP

sus importaciones 17.52 millones de TEU's. A nivel global, el 90% del comercio es transportado en contenedores.


Los 255 millones de contenedores TEU's movilizados anualmente implican un flujo diario de más de 700 mil contenedores por los puertos del mundo y cada uno de ellos representa un riesgo para fines de seguridad antiterrorista.

En octubre de 2006 los Estados Unidos, bajo el marco de la Ley de Puerto SAFE (SAFE Port Act), creó el programa de seguridad Container Security Initiative – CSI (Iniciativa de Seguridad de Contenedores) a través del cual la Aduana estadounidense (Custom and Border Protection – CBP) colocó equipos de oficiales en puertos marítimos extranjeros para trabajar junto a sus homólogos del gobierno anfitrión estableciendo criterios de seguridad para identificar contenedores de alto riesgo que podrían transportar armas de destrucción masiva, químicos y otros.

En esos “puertos CSI” las administraciones aduaneras utilizan rayos X y tecnología de detección de radiación para revisar contenedores de alto riesgo antes de que sean enviados a los puertos de los EEUU.

Según el CBP existen en la actualidad 60 puertos CSI que están operativos en 35 países, los cuales logran pre seleccionar aproximadamente el 80% de toda la carga marítima en contenedores importada hacia los Estados Unidos.

El SAFE Port Act exigía desde el inicio que toda la carga en contenedores que entrará a los EEUU se examinará para detectar cualquier radiación ilícita por lo que se estableció el Programa Radiation Portal Monitor (RPM), dispositivos pasivos de detección de radiación que pueden escanear contenedores de carga y vehículos para detectar fuentes de radiación ilícita.

Actualmente más de mil doscientos RPM están desplegados en puertos de entrada estadounidenses, en instalaciones de correo expreso, en puntos de sus fronteras y en ciertas ubicaciones extranjeras. Según el CBP desde el 2006 hasta octubre de 2016 los RPM han escaneado 67 millones de contenedores y medios de transporte. 


transported in containers.

255 million of TEUs containers transported annually involves a daily turnover of more than 700 thousand containers per port in the world, each one represents a risk for anti-terrorism security purposes.

In October 2006, the USA, under the framework of the SAFE Port Act, created a security program, Container Security Initiative – CSI, with which the American Customs (Customs and Border Protection – CBP) assigned officer teams in foreign sea ports in order to work together with their pairs of the host country, as to establish security criteria for identifying high-risk containers which could transport massive destruction weapons, chemicals among others.

In these “CSI ports”, the customs administration departments use X-ray and radiation detection technology to check high-risk containers before being sent to ports in the USA.

According to the CBP, there currently are 60 operational CSI ports working in 35 countries, which are able of selecting 80% of all the containerized sea cargo imported to the USA.

The SAFE Port Act demanded that all containerized cargo entering to the USA from the beginning shall be examined to detect any radiation, thus the RPM - Radiation Portal Monitor was established, which are passive detection devices capable of screening cargo containers and vehicles to detect illegal radiation sources. More than 1,200 RPMs are currently installed in American ports of entry, express courier facilities, and borders spots and in certain foreign locations. A per the CBP, from 2006 to October 2016, RPMs have screened 67 millions of containers and carriers. 

Fuente / Source: World Shipping Council / US CBP





Su situación en la Unión Europea

## La información anticipada para la carga aérea

ITS SITUATION IN THE EUROPEAN UNION

ADVANCE AIR CARGO INFORMATION

**E**n 2016 la Unión Europea pretendía dar inicio al programa “Preloading Consignment Information for Secure Entry (PRECISE)” con lo cual habría sido obligatoria la presentación anticipada de la información de las cargas aéreas a partir del mes de junio de dicho año. Sin embargo, el cumplimiento legal solo ocurrirá una vez que los sistemas electrónicos requeridos estén listos, lo cual ocurrirá como máximo el 31 de diciembre del 2020, fecha límite del proyecto de implementación del programa PRECISE.

Este proyecto europeo inició su proceso de implementación en el 2012 con la ejecución de proyectos piloto. Actualmente, desde mayo 2016, está en periodo de reglamentación y su implementación completa se ha fijado como plazo para el año 2020. La evaluación de riesgos que aplica consta de “7+1” elementos obligatorios y en los proyectos piloto del proceso de reglamentación en marcha están participando las aduanas de 8 países miembros, 4 empresas de carga expresa, 10 aerolíneas y 8 transportadores logísticos, además de 8 operadores postales.

Como se señaló, actualmente la UE está elaborando reglamentos preliminares basados en el requerimiento a los proveedores de servicios de carga aérea el envío anticipado a las aduanas de datos para el análisis de amenazas. En este sentido, PRECISE es un ejercicio de investigación que analiza qué datos deben enviarse con anticipación, cuándo y por quién.

Este programa es similar al programa “Air Cargo Advance Screening (ACAS)” de los Estados Unidos. ACAS, también conocido como “US Importer Security Filing – ISF” o “ISF for Air”, es un programa piloto en curso que trabaja en cooperación con 39 aerolíneas y formará la base para exigir el envío anticipado de datos de carga aérea para los vuelos entrantes.

En el caso del programa europeo PRECISE se sabe que este buscará ocho elementos de datos conocidos como “7+1” en todos los envíos de carga aérea antes de la carga. Habrá siete elementos de datos sin procesar: nombre y dirección del expedidor, nombre y dirección del destinatario, una descripción de los productos, un conteo de piezas y peso del envío, más un identificador de envío y el número de cuenta de la vía aérea domiciliaria (HAWB).

**I**n 2016 the European Union intended to start with the “Preloading Consignment Information for Secure Entry (PRECISE)” program, with which it would have been compulsory to present the advance air cargo information from June of said year. However, the legal compliance will only happen once the required electronic systems are ready. This will happen on December 31, 2020 the latest, which is the limit date for the implementation of PRECISE program project.

This European Project started its implementation process in 2012, executing pilot projects. Nowadays, since May 2016, it is in regulation stage and its full implementation is fixed to be done in 2020. The risk assessment applied comprises “7+1” compulsory elements and during the ongoing pilot projects of regulation process, customs of 8 member countries, 4 express courier companies, 10 airlines and 8 logistic carriers, besides 8 postal carriers are participating.

As stated above, the EU is currently elaborating preliminary regulations based on the advance information required to the air cargo services suppliers by the Customs in order to assess threats. In this way PRECISE is a research exercise that assesses which data must be sent in advance, when and by whom.

This program is similar to the USA Air Cargo Advance Screening (ACAS) program. ACAS, as well known as US Importer Security Filing – ISF” or “ISF for Air”, is one ongoing pilot program which works in cooperation with 39 airlines and will form the base to demand the air cargo information sent in advance for the arriving flights.

In the case of the European program PRECISE, it is understood that this will look for eight data elements known as “7+1” in all the air cargo shipments before loading. There will be seven elements without processing: name, shipper address, consignee name and address, product description, number of pieces, weight, plus a shipment identifier and the account number of the HAWB.

Se espera que la responsabilidad de proporcionar esa información a las aduanas recaiga principalmente en los Agentes de Carga (transitarios) y, en segundo lugar, en los Transportistas. Estudios preliminares han determinado que los agentes de carga son las que tienen acceso a gran parte de los elementos de datos requeridos en un punto anterior del ciclo de envío, una vez que se completa el HAWB.

Las aduanas quieren la mayor cantidad de datos de precarga en un solo mensaje para realizar una primera capa de análisis de riesgos de seguridad. Pero el estudio de la UE reconoció que cierta información necesitaría ser actualizada, tales como la descripción de los productos, por ejemplo, que podría cambiar entre los momentos de la reserva y cuando la carga se registra físicamente.


Una cosa a tener en cuenta es hasta qué punto antes de cargar se requeriría la presentación de datos anticipados. El estudio examinó los intervalos que oscilaron entre ocho horas y menos de dos horas pero no fue concluyente sobre un marco de tiempo necesario y razonable, y señaló que el último tiempo de aceptación para el transporte aéreo varía entre los operadores. Los operadores y transportistas aéreos operan cada vez más en un entorno complejo. Una buena noticia del programa PRECISE es que se coordinará estrechamente con el programa estadounidense ACAS; por lo tanto, si una empresa está en ACAS, estará por delante del juego cuando la UE comience su programa.

### Seguridad de la cadena de suministro

La Unión Europea (UE) sigue un enfoque de múltiples niveles basado en el riesgo para la seguridad de las cadenas de suministro, tema que es abordado de dos formas. La primera es observar el flujo de la transacción en el envío de un extremo a otro. Las medidas incluyen la presentación de datos avanzados en formato electrónico, la evaluación de riesgos y la mitigación de riesgos por parte de las aduanas. La segunda forma está basado en el sistema, es decir si las partes involucradas son entidades de confianza (programa OEA o participantes de programas de otras autoridades gubernamentales). La UE considera que la combinación de estos dos enfoques pueden cerrarse en gran medida las brechas de seguridad.

La seguridad incluye todos los modos de transporte que cruzan la frontera hacia la UE. Las medidas para fortalecer la seguridad de las cadenas de suministro tienen en cuenta las particularidades de cada modo de transporte.

Una de las medidas que afecta a todos los modos de transporte fue la introducción de "Entry Summary Declaration – ENS" (Declaración sumaria de entrada) mediante los reglamentos 648/2005 y 1875/2006. Los operadores deben proporcionar información de carga anticipada para sus envíos a la UE presentando una declaración electrónica. Este requisito entró en vigor el 1 de enero de 2011. Para la presentación y el procesamiento de la ENS se implementó el "Import Control System – ICS" (Sistema de Control de Importaciones), un sistema de TI (tecnología informática).

Debido a importantes deficiencias del concepto original de ENS, en particular con respecto a la calidad de los datos y la disponibilidad oportuna, se revisó en el Código aduanero de la Unión y su Ley de aplicación. Los principales cambios (opciones de presentación múltiple, por diferentes actores en la cadena de suministro y en diferentes conjuntos de datos en diferentes momentos) serán implementados cuando estén disponibles todos los sistemas de TI necesarios. 

It is expected that the responsibility, when providing this information to customs departments, relies on the forwarding agent (freight forwarder) and, secondly in the carriers. Preliminary studies have determined that forwarding agents can greatly access this data elements required in a prior step of the shipping cycle, once the HAWB is filled in.

Customs Departments requires as much quantity as possible of pre-shipment information in only one message in order to execute a first stage of security risk assessment. However, the EU study states that certain information would need to be updated, such as product description, which might change when doing the reservation and when the cargo is registered physically.


One thing to keep in mind is to up to what extend before loading; this advance information presentation would be required. The study examined the intervals ranging between eight hours and less than two hours, but it was not conclusive, regarding a time frame necessary and reasonable, and it pointed out that the last acceptance time for air transport varies among the forwarding agents. The forwarding agents and air carriers operate in a more increasing complex environment. The good news about the PRECISE program is that it will be closely coordinated with the American ACAS program, thus if a company is already registered in ACAS, it will be ahead when the EU starts its program.

### Security of the supply chain

The European Union (EU) follows a multiple-level approach based on the risks on supply chain security; this theme is address in two ways. Firstly, to observe the transaction flow of a shipment from one end to the other. The measures include presentation of advance information in electronic format, risk assessment and risk mitigation by Customs. Secondly, this way is based on the system, i.e. if the involved parties are trustworthy entities (OAS program or participants of other governmental authorities programs). The EU considers that these two approaches combined can close the gaps in security to a large extent.

The security includes all the transport means crossing the borders to the EU. The measures to strengthen the supply chain security consider the special features of each transport modality.

One of the measures affecting all the transport modalities was the introduction of the "Entry Summary Declaration – ENS" stated in the regulations 648/2005 and 1875/2006. The forwarding agents must provide all the advance cargo information for their shipments to the EU by presenting an e-filing. This requirement went into effect on January 1, 2011. An "Import Control System" – ICS was implemented for the ENS presentation and processing, this is an IT system.

Due to major deficiencies in the original concept of the ENS, mainly in the quality of information and timely availability, this was revised in the Unions Customs Code and its application Law. The main changes (multiple presentation options, by different parties involved in the supply chain and in different data sets in different moments) will be implemented when all the necessary IT systems are available. 

Fuente / Source: Comisión Europea / Taxation and Customs Union



# TALMA líder en servicios aeroportuarios

## TALMA - LEADER IN AIRPORT SERVICES

**C**on más de 25 años ofreciendo soluciones integrales, Talma brinda servicios aeroportuarios seguros, rápidos y eficientes.

Con más de 5.200 colaboradores altamente capacitados Talma opera en 20 aeropuertos del Perú, 3 ciudades de México y 7 aeropuertos del Ecuador, atendiendo anualmente más de 140 mil vuelos y más de 225 mil toneladas métricas de carga aérea.

Una de las fortalezas de Talma es su moderno sistema de seguridad con tecnología de avanzada, con más de 420 cámaras de video vigilancia que incluye 60 cámaras inteligentes que aseguran la trazabilidad de la carga.

Este sistema permite monitorear todos los procesos operativos y administrativos dentro y fuera del terminal de almacenamiento. Además, Talma cuenta con 9 equipos de rayos X de última generación, acorde con las exigencias de la autoridad aeronáutica y de sus clientes, que se encuentran certificados por la agencia estadounidense Transportation Security Administration (TSA).

Talma tiene el compromiso de ofrecer servicios del más alto nivel, cumpliendo con estándares nacionales e internacionales que le permiten brindar la máxima seguridad en sus procesos.

### Certificaciones:

- ISO 9001
- ISO 14001
- OHSAS 18001
- ISO 28000
- BASC
- ISAGO
- IATA

**W**ith more than 25 years offering integrated solutions, Talma provides secure, quick and efficient airport services.

Having more than 5200 highly skilled employees, Talma operates in 20 airports in Peru, 3 cities in Mexico and 7 airports in Ecuador; attending yearly more than 140 thousand flights and more than 225 thousand metric tons in air cargo.

Owning a modern security system is one of the strengths of Talma, with cutting edge technology of more than 420 video security cameras, including 60 smart cameras that ensure cargo tracking.

This system allows monitoring all the operative and administrative process inside and outside the storage terminal. Moreover, Talma has 9 cutting edge X-ray equipment, complying with the aviation authority regulations and demands of their customers, which are certified by the American agency TSA - Transportation Security Administration.

Talma is committed to provide the highest level services, complying with national and international standard that allows providing the maximum security during its processes.

### Certifications:

- ISO 9001
- ISO 14001
- OHSAS 18001
- ISO 28000
- BASC
- ISAGO
- IATA



### Servicios que ofrece Talma:

- **Asistencia en tierra:** servicios de rampa, servicios al pasajero y operaciones de vuelo a aerolíneas regulares y no regulares.
- **Servicios a la carga:** Servicios de almacenamiento, operaciones de carga, General Handling Agent (GHA) y servicios de frío. Para ello, cuenta con moderna infraestructura y tecnología de punta.
- **Aviación ejecutiva (FBO):** Servicio de Fixed Base Operator (FBO) para vuelos charter y atención de vuelos ejecutivos en los principales aeropuertos del Perú, así como servicios personalizados de primera clase para pasajeros y tripulaciones.
- **Mantenimiento de aeronaves:** Servicios de mantenimiento en línea de aeronaves, para lo cual cuenta con autorizaciones y certificaciones de autoridades aeronáuticas como: DGAC Perú, FAA de los Estados Unidos, DGAC Chile, DAC Ecuador y Aerocivil Colombia.
- **Talma Training School:** Con más de 12 mil horas anuales de instrucción, Talma Training School, es el primer centro de capacitación del sector aerocomercial en el Perú en obtener certificaciones IATA. Además, es el primero en América Latina en constituirse como socio regional de entrenamiento RTP - IATA.

### Nuevos horizontes

Este año Talma inició operaciones en siete (07) de los principales aeropuertos del Ecuador, brindando servicios de rampa, los mismos que se encuentran respaldados por altos estándares internacionales de gestión de la calidad como ISAGO e ISO 9001. Así, suma el tercer país donde se encuentra presente la empresa, posicionándola como referente en el rubro de servicios aeroportuarios en la región.

### Talma provides the following services:

- Ground handling services: ramp services, passenger service and flight operations to regular and non-regular airlines.
- Cargo handling services: storage services, cargo operations, General Handling Agent (GHA) and air cargo services. For this, Talma has modern infrastructure and advanced technology.
- Executive aviation (FBO): Fixed Base Operator (FBO) for charter and executive flights services to the main Peruvian airports. We provide personalized first class services for passengers and crew members.
- Aircraft maintenance: aircraft maintenance services, for which we have authorizations and certifications issued by aeronautical authorities: Peru DGAC, USA FAA, DGAC Chile, DAG Ecuador and Colombia Air civil.
- Talma Training School: With more than 12 thousand annual training hours, Talma Training School is the first training center for the air commercial sector in Peru in obtaining the IATA certifications. Moreover, Talma is the first in Latin America to become a regional partner of training, RTP – IATA.

### New horizons

This year, Talma has started operations in seven (7) of the main airports of Ecuador, providing ramp services, following the highest international standards of quality management, such ISAGO and ISO 9001. In that way, this is the third country where Talma is operating, placing itself as a reference in the airport services sector in the region.



## Organizaciones peruanas pueden certificar en Gestión Anti Soborno

### PERUVIAN COMPANIES CAN CERTIFY IN ANTI BRIBERY MANAGEMENT

Perú fue el primer país latinoamericano en adoptar la Norma ISO 37001 referida al Sistema de Gestión Anti Soborno

Peru was the first Latin American country to embrace the ISO 37001 standard referred to Anti Bribery Management System

**E**n octubre del 2016 la Organización Internacional de Normalización (ISO por sus siglas en inglés) publicó la Norma ISO 37001 Sistema de Gestión Anti-Soborno (SGAS). El pasado 04 de abril del 2017 el Instituto Nacional de Calidad – INACAL del Perú aprobó la adopción internacional de dicha norma a través de la “Norma Técnica Peruana PNTP-ISO 37001 Sistemas de Gestión Anti-Soborno”, convirtiéndose así en el primer país de América Latina en adoptar oficialmente esta Norma.

**I**n October 2016, the International Organization for Standardization (ISO) published the ISO 37001 Anti-Bribery Management System (SGAS). Also, on April 04 of this year, the National Quality Institute - INACAL of Peru approved the international adoption of this standard through the “Peruvian Technical Standard NTP-ISO 37001 Anti-Bribery Management Systems”, becoming the first Latin American country to officially adopt this Standard.

#### LEGISLACIÓN ANTICORRUPCIÓN

La Ley N°30424 que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho (delito que consiste en sobornar a una autoridad mediante la solicitud de una dádiva a cambio de realizar un acto inherente a su cargo) establece que, el modelo de prevención Anti Soborno puede ser certificable por terceros debidamente registrados y acreditados, como lo es PERÚ CERTIFICATION.

La Persona Jurídica está exenta de la responsabilidad administrativa si adopta o implementa con anterioridad al delito un modelo de prevención, de acuerdo a su riesgo con medidas de vigilancia y controles para prevenir el delito o reducir el riesgo. El modelo de prevención debe contener:

#### ANTICORRUPTION LEGISLATION

Law No. 30424 regulating the administrative liability of legal persons for the crime of bribery (an offense of bribing an authority by requesting a donation in exchange for performing an act inherent to its position) establishes that the Anti-bribery prevention model can be certifiable by duly registered and accredited third parties.

BASC PERÚ trained in February of this year a group of international auditors as “Leading Auditors of ISO 37001: 2016” before the Professional Evaluation and Certification Board (PECB) of Canada.

The Legal Entity is exempt from administrative responsibility if it adopts or implements prior to the crime a model of prevention, according to its risk with surveillance measures and controls to prevent crime or reduce risk. The prevention model must contain:

- Función de Auditoría interna de prevención
- Medidas preventivas frente a actividades que generen o incrementen riesgos
- Establecer procedimientos
- Sistemas de denuncia
- Difusión y supervisión del modelo de prevención

## REQUISITOS PARA LA CERTIFICACIÓN

Esta Norma Técnica Peruana (NTP) es aplicable a las organizaciones pequeñas, medianas y grandes, ya sean del sector público o privado, para que puedan identificar los canales o procesos de riesgo dentro de su organización, y así establecer mecanismos de control para prevenir y tener trazabilidad, por ejemplo, de los recursos de una obra específica y estos no se destinen a otra. A continuación un resumen de los requisitos para poder certificar:

**Objeto de la Norma.** El documento especifica los requisitos y proporciona una guía para establecer, implementar, mantener, revisar y mejorar un Sistema de Gestión Anti Soborno. El sistema puede ser independiente o puede estar integrado en un Sistema de Gestión Global.

**Contexto de la organización:** La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los objetivos previstos de su Sistema de Gestión Anti Soborno.

**Liderazgo:** La organización debe contemplar el liderazgo y compromiso, la política anti soborno y los roles, responsabilidades y autoridades en la organización. Es importante enfatizar que cuando la organización cuente con un órgano de gobierno, este debe demostrar su liderazgo y compromiso con respecto al sistema de gestión anti soborno por ejemplo a través de:

- Aprobar la política anti sobornos de la organización.
- Asegurar que la estrategia de la organización y la política anti soborno se encuentran alineadas.

**Planificación:** Al planificar el sistema de gestión anti soborno, la organización debe considerar: Acciones para tratar riesgos y oportunidades y objetivos anti sobornos y planificación para lograrlos.

**Apoyo:** La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión anti soborno. Además, debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecte el desempeño anti soborno, enfocándose en los procesos de contratación. Este capítulo también contempla la toma de conciencia y formación, la comunicación y la información documentada.

**Operación:** La organización debe planificar, implementar, revisar y controlar los procesos necesarios para cumplir los requisitos del Sistema de Gestión Anti Soborno y para implementar acciones. Para tal efecto la organización debe contemplar lo siguiente:

- Planificación y control operacional.
- La debida diligencia, la organización debe evaluar

- Internal Audit Prevention function
- Preventive measures against activities that generate or increase risks
- Establish procedures
- Reporting systems
- Dissemination and supervision of the prevention model

## REQUIREMENTS FOR CERTIFICATION

This Peruvian Technical Standard (NTP) is applicable to small, medium and large organizations, whether in the public or private sector, so that they can identify the risk channels or processes within their organization, and thus establish control mechanisms to prevent and have traceability, for example, of the resources of a specific work that are not intended for another. Below is a summary of the requirements to be able to certify:

**Object of the Standard:** The document specifies requirements and provides guidance for establishing, implementing, maintaining, reviewing and improving an Anti-Bribery Management System. The system can be independent or can be integrated into a Global Management System.

**Context of the organization:** The organization must determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended objectives of its Anti-Bribery Management System.

**Leadership:** The organization should consider leadership and commitment, anti-bribery policy and the roles, responsibilities and authorities in the organization. It is important to emphasize that when the organization has a governing body, it must demonstrate its leadership and commitment to the anti-bribery management system, for example through:

- Approval the organization's anti-bribery policy.
- Ensuring that the organization's strategy and anti-bribery policy are aligned.

**Planning:** In planning the anti-bribery management system, the organization should consider: Actions to address risks and opportunities and anti-bribery objectives and planning to achieve them.

**Support:** The organization must determine and provide the necessary resources for the establishment, implementation, maintenance and continuous improvement of the anti-bribery management system. In addition, it must determine the necessary competence of the people who perform, under its control, a work that affects the anti-bribery performance, focusing on the hiring processes. This chapter also addresses awareness and training, communication and documented information.

**Operations:** The organization must plan, implement, review and control the processes necessary to comply with the requirements of the Anti-Bribery Management System and to implement actions. For this purpose, the organization should consider the following:

- Operational Planning and Control.

la naturaleza y el alcance del riesgo de soborno en operaciones, proyectos, actividades, socios de negocios y personal pertinente.

- Los controles financieros y no financieros.
- La implementación de controles Anti Soborno por organizaciones controladas y por socios de negocio.
- Los compromisos Anti Soborno.
- Los regalos, atenciones, donaciones y beneficios similares.

#### **Evaluación del desempeño: La organización debe establecer:**

- El seguimiento, medición, análisis y evaluación.
- La auditoría interna, asegurándose que los resultados de las auditorías se informan a la dirección pertinente.

Además, para asegurar la objetividad e imparcialidad de esos programas de auditoría, la organización debe asegurarse que se efectúan por una función independiente o una tercera parte apropiada.

- La revisión por la Dirección, y
- La revisión por la función de cumplimiento anti soborno

**Mejora:** La organización debe reaccionar ante la no conformidad e implementar acciones correctivas apropiadas a los efectos de las no conformidades encontradas. Además, debe mejorar continuamente la idoneidad, adecuación y eficacia del Sistema de Gestión Anti Soborno (SGAS).

#### **BENEFICIOS DE LA CERTIFICACIÓN:**

Para la organización

- Genera confianza en sus stakeholders ya que se implementan controles internacionales.
- Sirve como herramienta de defensa frente a los fiscales y/o tribunales en caso de investigación, mostrando evidencia de que la organización ha tomado medidas para prevenir el soborno.
- Aporte al "Compliance" de la organización.
- Estandarización y mejor gestión de los procesos.

Para los clientes

- Permite identificar a aquellas organizaciones que buscan desarrollar sus actividades en un escenario en contra el soborno.
- Trabajar con proveedores no expuestos a riesgos que puedan comprometer su imagen de marca.
- Menores riesgos al operar en mercados extranjeros ya que son reglas aceptadas internacionalmente.

Para el mercado

- Organizaciones más comprometidas y transparentes.
- Establecer reglas internacionales que impidan el incremento de costos de hacer negocios.
- Genera confianza en las instituciones.
- Las auditorías externas permiten evidenciar el cumplimiento.

- Due diligence, the organization should evaluate the nature and extent of the risk of bribery in operations, projects, activities, business partners and relevant personnel.
- Financial and non-financial controls.
- The implementation of Anti-bribery controls by supervised organizations and business partners.
- Anti-bribery commitments.
- Gifts, courtesies, donations and similar benefits.

#### **Performance evaluation: The organization must establish:**

- Monitoring, measurement, analysis and evaluation.
- The internal audit, ensuring that the results of the audits are reported to the relevant address.

In addition, to ensure the objectivity and impartiality of such audit programs, the organization must ensure that they are performed by an independent function or an appropriate third party.

- Review by Management, and
- Review by anti-bribery compliance function

**Improvement:** The organization must react to non-compliance and implement appropriate corrective actions for the purposes of nonconformities encountered. In addition, it must continuously improve the suitability, adequacy and effectiveness of the anti-bribery management system.

#### **CERTIFICATION BENEFITS:**

To the organization

- Generates trust in its stakeholders as international controls are implemented.
- It serves as a defense tool against prosecutors and/or courts in case of investigation, showing evidence that the organization has taken steps to prevent bribery.
- Contribution to the Compliance of the organization.
- Standardization and better management of processes.

To the clients

- It identifies those organizations that seek to develop their activities in a scenario against bribery.
- Work with suppliers not exposed to risks that may compromise their brand image.
- Lower risks when operating in foreign markets as they are internationally accepted rules.

To the market

- More committed and transparent organizations.
- Establish international rules that prevent increased costs of doing business.
- Generates trust in institutions.
- External audits make it possible to demonstrate compliance.

# Corporación SEALERS inaugura nuevo laboratorio mecánico para sus precintos

## SEALERS CORPORATION INAUGURATES NEW MECHANICAL LABORATORY FOR ITS SECURITY SEALS

Según la norma NTP-ISO 17712: 2015 los precintos deben pasar por diversos ensayos, el laboratorio permite desarrollar pruebas de tensión, corte, torsión, impacto y en breve se desarrollarán pruebas de baja temperatura con una nueva cámara frigorífica.

El tener un laboratorio propio permite complementar las pruebas de una producción diaria y control de calidad rápidamente, así mismo se puede evaluar que los productos superen los requisitos mínimos, también podemos proporcionar al usuario un estándar que le garantiza la compra de un mejor producto.



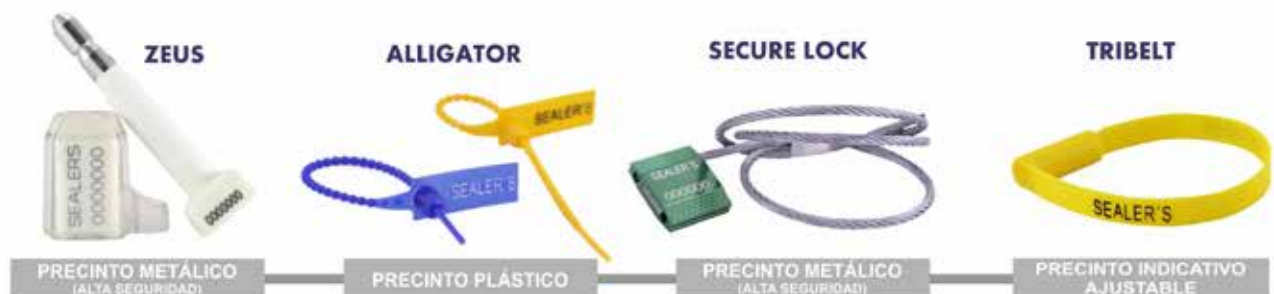
According to the NTP-ISO 17712:2015 standard, security seals must pass different tests. The laboratory allows conducting tension, cut, torsion and impact tests, and soon, low temperature tests will be developed in a new cooling room.

Having a own laboratory allows complementing daily production tests and quality control quickly, as well as assessing that products are not exceeding the minimal requirements and we can likewise provide the user with a standard that guarantees a better product acquisition.



## CORPORACIÓN SEALER'S S.A

Fabricantes y Exportadores de Precintos de Seguridad



**EXCLUSIVO**

**PRECINTO TITÁN**



**Nuestras Certificaciones**



**Somos la Solución a la Seguridad de sus Productos**

Calle Rene Descartes N° 155 Sta Raquel, Ate - Lima - Perú

(511) 713 - 8800  
994-069-815  
998-338-030

ventas@sealers.com.pe  
comercial@sealers.com.pe  
www.sealers.com.pe

Síguenos en:





## ANAB realiza Auditoría Testificada a la auditoría de BASC PERÚ a TALMA SERVICIOS AEROPORTUARIOS S.A.

ANAB CONDUCTS A WITNESS AUDIT TO THE AUDIT CARRIED OUT BY BASC PERU TO TALMA SERVICIOS AEROPORTUARIOS S.A.

Entre los días 13 y 18 de noviembre se realizó la Auditoría Testificada (llamada también auditoría testigo, que es cuando una entidad acreditadora observa in-situ la auditoría que la entidad certificadora realiza a una empresa certificada) de ANAB (Ansi-ASQ National Accreditation Board) a BASC PERÚ durante la auditoría en la Norma ISO 37001:2016 (Sistema de Gestión Anti Soborno) que este último desarrolló a TALMA SERVICIOS AEROPORTUARIOS S.A., empresa que cuenta con la certificación BASC y que a la vez se encuentra en proceso de certificación en dicha norma anti-soborno mediante PERÚ CERTIFICATION.

La auditoría estuvo a cargo de Carlos Reyes, Gerente de Operaciones y Auditor Líder en la Norma ISO 37001, con la participación, en calidad de observadora, de Kandy Escobar, Gerente de Capacitaciones y Auditor Líder en la Norma ISO 37001, ambos de BASC PERÚ.



Between the 13 and 18 of November, ANAB (ANSI-ASQ National Accreditation Board) carried out a Witness Audit (also known as testified audit, which is when the accrediting body conducts an in-situ observation to the audit that the certifying body is conducting to a certifying company) to BASC PERU during the audit of the ISO 37001:2016 (Anti-Bribery System) Standard, which BASC conducted to TALMA SERVICIOS AEROPORTUARIOS S.A., company BASC certified and that at the same time is in process of obtaining the anti-bribery certification through PERU CERTIFICATION.

The audit was in charge of Carlos Reyes, Operations Manager and Lead Auditor of the ISO 37001 Standard, with the participation of Kandy Escobar, Training Manager and Lead Auditor of the ISO 37001 Standard, as observer, both from BASC PERU.

## BASC PERÚ ponente principal en el “Taller de la NTP ISO 37001”, organizado por la Comisión de alto nivel Anti Corrupción (CAN)

BASC PERÚ main presenter at the “Workshop of the NTP ISO 37001”, organized by the High Level Anti-Corruption Commission (CAN)

BASC PERÚ estuvo presente en el “Taller de Intercambio de Experiencias en la Implementación de la Norma Técnica Peruana ISO 37001” realizado el pasado 27 de octubre. El taller fue organizado por la Comisión de Alto Nivel Anti Corrupción (CAN), entidad que presentó en dicha ocasión la Política Nacional de Integridad y Lucha Contra la Corrupción.

La ponencia principal estuvo a cargo de César Venegas Núñez, Gerente General del BASC PERÚ, quien expuso el tema “La Corrupción en el Perú, la NTP 37001:2016, sus beneficios y el proceso de certificación”. La CAN está integrada por instituciones públicas, privadas y la sociedad civil con el objetivo de articular esfuerzos, coordinar acciones y proponer políticas dirigidas a prevenir y combatir la corrupción en el Perú.



BASC PERU was present at the “Sharing Experiences on the Peruvian Technical Standard ISO 37001 Workshop”, which was held last October 27. The workshop was organized by the High Level Commission of Anti-Corruption (CAN in Spanish), which in said event presented the National Integrity and Anti-Corruption Policy.

The main presentation was in charge of Cesar Venegas Nuñez, General Manager of BASC PERU, who talk about “Corruption in Peru, the Peruvian Technical Standard - NTP 37001:2016, its benefits and certification process”. The CAN is composed of public and private institutions and civil society with the aim of coordinating efforts, coordinating actions and proposing policies aimed at preventing and combating corruption in Peru.

## Foro “Lavado de Activos”

### FORUM ON MONEY LAUNDERING

El 17 de noviembre pasado BASC PERÚ realizó el foro Lavado de Activos en la Cámara de Comercio Americana del Perú (AMCHAM) con el objetivo de informar y dar a conocer las medidas preventivas que deben tomar las organizaciones para evitar ser víctimas de esta actividad ilícita.

BASC PERÚ agradece a la Unidad de Inteligencia Financiera (UIF) de la Superintendencia de Banca, Seguros y AFP por la participación de Fernanda García-Yrigoyen, Intendente del Departamento de Prevención, Enlace y Cooperación de dicha Unidad, mediante su exposición “Prevención del lavado de activos y del financiamiento del terrorismo, exigencias regulatorias y estrategias”.



Last November 17th, BASC PERU conducted the Forum on Money Laundering at the American Chamber of Commerce of Peru (AMCHAM) with the purpose of informing and discussing about the preventive measures that organizations shall take to avoid being victims of this illegal activity.

BASC PERU expresses its gratitude to the Unit of Financial Intelligence (UIF) of the Banking, Insurance and Retirement Funds Superintendence (SBS in Spanish) for the participation of Fernanda Garcia-Yrigoyen, Intendant of the Department of Prevention, Relation and Cooperation of said Unit for her presentation “Prevention of Money Laundering and Terrorism Financing, Regulatory Requirements and Strategies”.



## CAPACITE A SUS CLIENTES Y PROVEEDORES EN EL SGCS BASC



### Dirigido a:

Clientes y proveedores de empresas asociadas a BASC.

### Cantidad de participantes

Las charlas se llevarán a cabo con una cantidad mínima de 20 participantes.

### Objetivo

Fomentar una cultura de seguridad en los asociados de negocio de las empresas certificadas BASC a fin de fortalecer las operaciones de comercio exterior.

### Contenido

- Amenazas al Comercio Internacional
- Iniciativas de Seguridad en el Comercio Internacional
- Sistema de Gestión en Control y Seguridad BASC
- Controles para minimizar los riesgos en las operaciones.

### Lugar

Instalaciones de la empresa asociada BASC.

### Duración

90 minutos

### Mayor Información

[paula.lopez@bascperu.org](mailto:paula.lopez@bascperu.org) // [afiliaciones2@bascperu.org](mailto:afiliaciones2@bascperu.org)  
Fijo: 6128300 anexo 2232 / 2230 Celular: 946454057 - 98147\*6514



## CERTIFIQUESE CON NOSOTROS



En:

ISO 28000:2007

ISO 9001:2015



BASC PERÚ es casa matriz acreditada ante ANAB (ANSI-ASQ National Accreditation Board) desde el 23 de marzo del 2016, lo cual nos permite otorgar localmente con validez mundial, la certificación de Sistemas de Gestión para las siguientes Normas:

**ISO 9001:2015 - Sistema de Gestión de la Calidad**

**ISO 28000:2007 - Sistema de Gestión de la Seguridad en la Cadena de Suministro**

### BENEFICIOS

- BASC PERÚ cuenta con una vasta experiencia en sistemas de gestión de seguridad en la cadena de suministro ofreciendo valor agregado en cada actividad.
- Ahorro en la inversión con auditorías integradas BASC-ISO de menor costo, disminuyendo horas de auditoría.
- Menor tiempo en la entrega del certificado debido a que BASC PERÚ es casa matriz que se relaciona directamente con ANAB.
- Capacitaciones, talleres y seminarios gratuitos.
- Auditores acreditados por una entidad certificadora tercera que valida competencia (Professional Evaluation and Certification Board – PECB de Canadá)

Mayor información: [certificaciones.iso@bascperu.org](mailto:certificaciones.iso@bascperu.org)

Tel. (51-1) 612-8300 Anexo: 2230



BUSINESS ALLIANCE FOR SECURE COMMERCE

# Promoviendo Empresas Seguras



## Certificación BASC

- Capacitación para la implementación del Sistema SGCS BASC ■
- Control y Trazabilidad en la Cadena de Suministro BASC ■
- Cursos y Talleres Especializados BASC ■

## Nuevas Certificaciones

Certificación ISO 9001 

Certificación ISO 28000 

Acreditado por 

Jr. Francisco Graña 335, Magdalena del Mar, Lima - Perú  
Tel. +511-612-8300 Ext: 2230 E-mail: paula.lopez@bascperu.org  
[www.bascperu.org](http://www.bascperu.org)

