BUSINESS ALLIANCE FOR SECURE COMMERCE
CAPÍTULO PERÚ

Cargo Security

PUBLICACIÓN ESPECIALIZADA EN SEGURIDAD DE LA CADENA DE SUMINISTRO INTERNACIONAL

AÑO X / 2017 - 30

La nueva era de riesgos

THE NEW AGE OF RISKS

ENTREVISTA / INTERVIEW

El manejo de riesgos en empresas peruanas

RISK MANAGEMENT IN PERUVIAN COMPANIES

ENCUESTA / SURVEY

Gestión de riesgos operacionales en Europa

OPERATIONAL RISK MANAGEMENT IN EUROPE

ENTREVISTA / INTERVIEW

¿Cómo realizar un análisis de riesgos en 5 pasos?

HOW TO PERFORM A FIVE STEP RISK ASSESSMENT PROCESS?

¿Qué sectores pueden contar con la Certificación BASC?

La Certificación BASC está presente en los siguientes sectores:

Cargo Security
PUBLICACIÓN ESPECIALIZADA EN SEGURIDAD DE LA CADENA DE SUMINISTRO INTERNACIONAL

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@bascperu.org

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

BASC
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.bascperu.org

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.

REGISTRO DE MARCA: Certificado Nº 00153963
(Resolución Nº 010346-2009/DSD-INDECOPI)

Contenido
CONTENT

El riesgo en la cadena de suministro

RISK IN THE SUPPLY CHAIN

Bien dicen los expertos, lograr un 100% de seguridad en la cadena de suministro es imposible. Siempre habrá un elemento que genere incertidumbre en el funcionamiento y el rendimiento de este. Pero el objetivo es aproximarse lo más cerca posible a ese 100% y tener la capacidad de manejar los riesgos inevitables.

Además de la implementación de soluciones eficaces de seguridad, lo importante es contar con la información correcta en el momento preciso, antes de que el riesgo se haga visible, para ser alertados tan pronto como sea posible y así tratarlo eficazmente y medir los impactos en las cuentas y la imagen de la empresa. El conocimiento de información útil y pertinente de la situación de la cadena logística en sí, es tan importante como el flujo de los productos a través de esta cadena logística que la empresa maneja.

En esta edición buscamos informar en forma simplificada sobre los criterios y conceptos básicos sobre los cuales descansa la innumerable literatura especializada en el tema de riesgos. Los ejecutivos peruanos deben convencerse de que este asunto cobra cada vez más importancia a nivel mundial por la aparición de nuevas amenazas y el reforzamiento de aquellos ya existentes. De este modo, el terrorismo y las actividades ilegales son solo uno de los muchos riesgos sistémicos que los académicos utilizan para establecer los riesgos globales que pueden afectar al mundo entero y sus elementos (empresas, países y personas).

BASC PERU enriquece permanentemente sus procedimientos y el apoyo que realiza a las empresas asociadas a través de sus auditores y mediante las actividades que organiza a nivel nacional. Nuestra política de manejo del "factor riesgo" no escapa a esta política dirigida a nuestras empresas afiliadas. Por ello ponemos a su disposición especialistas nacionales e internacionales para brindar información relevante y actualizada que cubra las necesidades de cada empresa.

Nosotros partimos de preguntas básicas: ¿Se han identificado las principales fuentes de riesgo y ha medido su impacto? ¿Tiene construida una cadena de suministro capaz de resolver los eventuales inconvenientes? ¿La gestión de riesgos es vista como algo marginal que se aplica sólo cuando sucede algo inesperado o sus empleados contribuyen a mitigar el riesgo en sus actividades diarias? ¿Tiene un plan de contingencia? Ustedes tienen la respuesta y pueden contar con nuestro apoyo.

Experts say that achieving 100% security in the supply chain is impossible. There will always be an element that generates uncertainty in the operation and performance of it. But the goal is to get as close as possible to that 100% and have the ability to handle the inevitable risks.

In addition to the implementation of effective security solutions, the important thing is to have the right information at the right time, before the risk becomes visible, to be alerted as soon as possible and to treat it effectively and measure the impact on the company's image and finances. The knowledge of useful and pertinent information about the situation of the supply chain itself is as important as the flow of products through this supply chain that the company handles.

In this edition we seek to inform in a simplified way about the basic criteria and concepts on which the risk-specialized literature rests. Peruvian executives must be convinced that this issue is becoming more and more important at the global level due to the appearance of new threats and the reinforcement of those that already exist. In this way, terrorism and illegal activities are just one of the many systemic risks that academics use to establish global risks that can affect the entire world and its elements (companies, countries and people).

BASC PERU permanently enriches its procedures and the support given to the associated companies through its auditors and through the activities that it organizes nationwide. Our policy of managing the "risk factor" does not escape this policy addressed to our affiliated companies. That's why we provide national and international specialists to provide relevant and up-to-date information that meets the needs of each company.

We come from basic questions: have the main sources of risk been identified and their impact measured? Do you have a supply chain that can solve any problems? Is risk management viewed as something marginal that applies only when something unexpected happens or your employees contribute to mitigate risk in their daily activities? Do you have a contingency plan? You have the answer and can count on our support.

Raúl Saldías Haettenschweiler
Presidente / President
BASC PERÚ

En qué consiste

El análisis de riesgo de la cadena de suministro internacional

WHAT IS

RISK ANALYSIS IN THE INTERNATIONAL SUPPLY CHAIN?

En el mundo de los negocios existe un sinnúmero de criterios y métodos para realizar el análisis del riesgo en las empresas. El modelo adecuado para cada empresa dependerá, en mayor o menor grado, de la naturaleza de sus operaciones, del tamaño de la organización, del grado de tecnificación de sus operaciones, de su ubicación geográfica, de sus objetivos estratégicos, entre otras. Por ello las empresas deben considerar seguir los lineamientos de profesionales y organizaciones especializadas en un determinado sector.
Los negocios internacionales de bienes implican la interacción de cadenas de suministro que sobrepasan fronteras nacionales, por lo que el rango de zonas de riesgo es extenso, es decir, intervienen elementos o factores que pueden provenir de otros países con mayores grados de amenazas.
Una organización referente a nivel mundial en seguridad de cadena de suministro como es el Customs and Trade Partnership Against Terrorism (C-TPAT), recomienda en este tema que las empresas deben contar con un proceso documentado de "cómo la empresa lleva a cabo su análisis de riesgo de la cadena logística", el cual debe estar basada en la naturaleza única del modelo del negocio que realiza y ajustarse a las necesidades de dicho modelo, evitando adoptar uno genérico.
De esta manera, el programa C-TPAT exige de sus empresas asociadas que "lleven a cabo un análisis de riesgo documentado y verificable por lo menos

In the business world there is an endless number of criteria and methods to carry out risk analysis in companies. The right model for each company will depend, to a greater or lesser degree, on the nature of its operations, the size of the organization, the technology degree of its operations, its geographical location, its strategic objectives, among others. Therefore companies should consider following the guidelines of professionals and organizations specialized in a particular sector.

International goods businesses involve the interaction of supply chains that surpass national borders, so the range of risk areas is extensive. Here interact elements or factors that may come from other countries with higher degrees of threat.

A worldwide organization in supply chain security such as the Customs and Trade Partnership Against Terrorism (C-TPAT), recommends in this issue that companies must have a documented process of "how the company conducts its supply chain risk analysis", which must be based on the unique nature of its business model and must adjust to the needs of such a model, avoiding adopting a generic one.

In this way, the C-TPAT program requires its associated companies to "carry out a documented and verifiable risk analysis at least annually in order to remain in the program." For a company to develop a good risk analysis, it is essential to start by basing the process on clearly established concepts, such as the following:

anualmente para poder permanecer en el programa". Para que una empresa elabore un buen análisis de riesgo es fundamental empezar por basar el proceso en conceptos claramente establecidos, como los siguientes:

- **Análisis:** se refiere al "estudio, mediante técnicas informáticas, de los límites, características y posibles soluciones de un problema al que se aplica un tratamiento por ordenador: análisis informático".
- **Riesgo:** se asume como "Contingencia o proximidad de un daño, o a la teórica posibilidad de daño bajo determinadas circunstancias".
- **Análisis de Riesgo de la Cadena Internacional:** Análisis a todos los actores/empresas que tienen directo contacto con la mercancía de importación/exportación.
- **Auditoria Interna:** proceso que se lleva a cabo dentro de la empresa.
- **Auditoria Externa:** proceso llevado a cabo por una empresa y/o consultor externo.

La auditoría interna

De acuerdo al C-TPAT las auditorías internas se pueden realizar a la misma vez. Cada departamento debe ser involucrado eligiendo a miembros de distintas áreas para realizar auditorías en otras áreas. En este proceso la documentación es esencial, debiendo considerarse los hallazgos, la corrección y el seguimiento como parte del proceso.

¿Dónde se inicia el riesgo?

La regla de oro es que nunca asuma confiadamente que su socio de negocio está "cumpliendo con los requisitos de seguridad". Los expertos dicen: CONFÍA, PERO VERIFICA. Los riesgos están diseminados por todas partes y se pueden clasificar en riesgos mundiales, nacionales, regionales, y locales.
Como se dijo al principio, no exige una técnica específica para llevar a cabo un Análisis del Riesgo, ello depende de varias variables. El C-TPAT recomienda en forma general las siguientes etapas que debería comprender un proceso de análisis de riesgo el cual puede ser modificado según las características de las operaciones del negocio de la empresa.

1. Hacer un mapeo del flujo de embarque e identificar los socios comerciales (contratados directamente o indirectamente).
2. Realizar un análisis de riesgo enfocado en: terrorismo, contrabando de materiales ilícitos, contrabando de humanos, crimen organizado, condiciones en un país/región que puedan aumentar el riesgo de tales amenazas, y clasificar el riesgo en niveles de Alto, Medio, Bajo.
3. Realizar un análisis de vulnerabilidad de acuerdo a los requisitos y clasificar la vulnerabilidad en niveles Alto, Medio, Bajo.
4. Elaborar un plan de acción.
5. **Documentar** el procedimiento de la realización de los análisis del riesgo (política/procedimiento). CS

- **Analysis**: refers to the "study, by computer techniques, of the limits, characteristics and possible solutions of a problem to which a computer treatment is applied: computer analysis".
- **Risk**: is assumed to be "Contingency or proximity of damage, or to the theoretical possibility of damage under certain circumstances".
- **International Chain Risk Analysis**: analysis of all the actors/companies that have direct contact with import/export merchandise.
- **Internal Audit**: process that takes place within the company.
- **External Audit**: process carried out by an external company and/or consultant.

The internal audit

According to the C-TPAT internal audits can be performed at the same time. Each department should be involved by electing members from different areas to conduct audits in other areas. In this process, documentation is essential, and the findings, correction and follow-up should be considered as part of the process.

Where does the risk start?

The golden rule is that you should never confidently assume that your business partner is "meeting the security requirements". Experts say: TRUST, BUT CHECK. Risks are scattered everywhere and can be classified into global, national, regional, and local risks.

As stated at the beginning, there is no specific technique to carry out a Risk Analysis; it depends on several variables. The C-TPAT generally recommends the following stages, that should comprise a process of risk analysis, which can be modified according to the characteristics of the business operations of the company.

1. **Map the shipment flow** and identify the trading partners (hired directly or indirectly).
2. **Conduct a risk analysis** focused on: terrorism, smuggling of illicit materials, human trafficking, organized crime, conditions in a country/region that can increase the risk of such threats, and classify risk at high, medium, low.
3. **Perform a vulnerability analysis** according to the requirements and classify the vulnerability in high, medium and low levels.
4. **Develop an action plan**.
5. **Document** the procedure for conducting the risk analysis (policy/procedure). CS

Fuente/Source: Basado en exposición de Cristóbal Hernández. C-TPAT International Branch, Washington, D.C. Abril 2015. Based on a presentation by Cristóbal Hernández. C-TPAT International Branch, Washington, D.C. April 2015.

Cómo realizar

Un análisis de riesgos en 5 pasos

HOW TO MAKE A

RISK ANALYSIS IN 5 STEPS

Una importante guía de procedimientos que abre el panorama general de un Análisis del Riesgo para una empresa es lo que el Customs and Trade Partnership Against Terrorism (C-TPAT) ofrece en el documento "C-TPAT. Análisis de Riesgos en 5 Pasos. Guía de procedimientos". Esta ayuda muestra la estructura básica de la realización de un análisis de riesgos de la cadena de suministro internacional de acuerdo con los criterios mínimos de esta organización.

La información que se presenta es un resumen de la publicación de 20 páginas por lo que no incluye todo lo que implica un análisis de riesgos de seguridad.

La entidad estadounidense advierte que "algunos miembros del C-TPAT pueden tener una cantidad de cadenas de suministro y que esto puede representar una

An important procedural guide that opens up the general picture of a risk analysis for a company is what the Customs and Trade Partnership Against Terrorism (C-TPAT) offers in the document "C-TPAT. Risk Analysis in 5 Steps. Procedural Guide". This aid shows the basic structure of carrying out an international supply chain risk analysis in accordance with the basic criteria of this organization.

The information presented is a summary of the 20-page publication so it does not include everything that involves a security risk analysis.

The American entity warns that "some C-TPAT members may have a number of supply chains and that this can be a monumental task when conducting a risk analysis of their international chains. Therefore, it

tarea monumental al realizar un análisis de riesgos de sus cadenas internacionales. Por lo tanto, es recomendado que los miembros del C-TPAT identifiquen sus cadenas de suministro de "Alto Riesgo" realizando un análisis de amenazas en el punto de origen o región y donde se transborda/transporta la carga, y después realizar un análisis de la vulnerabilidad de esas cadenas de suministro. Inversamente, si las cadenas de suministro implican un número limitado de socios comerciales o de socios relacionados, su análisis de riesgos de seguridad de su cadena de suministro puede no requerir de estos esfuerzos extraordinarios".

Lo esencial

Se debe entender por 'Análisis de riesgos de seguridad de la cadena de suministro internacional' el proceso de identificar amenazas, vulnerabilidades y debilidades de seguridad en la cadena de suministro internacional y la gestión de acciones correctivas con procedimientos de verificación para asegurar que las debilidades sean corregidas.

Asimismo, el 'Trazado del flujo de participantes involucrados' es el método de identificación de todos los participantes involucrados y sus futuros papeles en los siguientes procesos desde el principio hasta el final de la cadena de suministro internacional: Obtención, Producción, Empaque, Almacenamiento, Embarque / Descarga, Transporte, y Preparación de Documentos de carga al destino.

Todos los socios de negocios involucrados directamente e indirectamente en la exportación / movimiento de mercancía desde el punto de origen hasta el centro de distribución del importador deben ser incluidos. Ejemplo: Fábricas, Granjas, Proveedores, Instalaciones de empaque de exportación, Agencias de compra/venta, Empresas comerciales, Agentes de carga marítima sin nave (NVOCCs), Transportista doméstico, etc., etc.

Otro elemento importante es el 'Grado de riesgo' que consiste en asignar un valor numérico a las amenazas y vulnerabilidades identificadas durante un análisis del riesgo de seguridad de la cadena de suministro (ejm. 1-Bajo, 2-Medio, y 3-Alto).

En el curso del proceso se llegará a un 'Plan de Acción de Seguridad de la Cadena de Suministro' que consiste en la identificación de debilidades y vulnerabilidades de seguridad descubiertas durante el proceso de análisis de riesgo para un socio comercial. El plan asigna responsabilidad por acciones correctivas / estrategias de mitigación (internas y externas), establece plazos / periodo de tiempo, documenta evidencia de medidas tomadas, describe procesos utilizados para verificar qué acciones se han realizado, y delinea el resultado final.

Grado de riesgo de seguridad

Para el C-TPAT cada empresa es responsable en establecer su propio sistema de grado de riesgo de seguridad basado en su modelo comercial. Se entiende que los negocios utilizan diversas metodologías para

is advisable for C-TPAT members to identify their "High Risk" supply chains by conducting a threat analysis at the point of origin or and where the cargo is transshipped/transported, and then perform a vulnerability analysis of these supply chains. Conversely, if supply chains involve a limited number of trading partners or related partners, the analysis of security risks in their supply chain may not require these extraordinary efforts".

The essentials

The International Supply Chain Security Risk Analysis should be understood as the process of identifying threats, vulnerabilities and security weaknesses in the international supply chain and the management of corrective actions with verification procedures to ensure that weaknesses are corrected.

Likewise, the 'Tracing of Participant Flow' is the method of identifying all participants involved and their future roles in the following processes from beginning to end of the international supply chain: Procurement, Production, Packaging, Storage, Loading/Unloading, Transport, and Preparation of Cargo Documents to the destination.

All business partners directly and indirectly involved in the export/movement of merchandise from the point of origin to the importer's distribution center must be included. Example: Factories, Farms, Suppliers, Export packing facilities, Sales agencies, Commercial companies, Non Vessel Operating Common Carrier (NVOCCs), Local carrier, etc.

Another important element is the 'Risk Degree', which consists of assigning a numerical value to the identified threats and vulnerabilities during a supply chain security analysis (e.g. 1-Low, 2-Medium, and 3-High).

In the course of the process, a 'Supply Chain Security Action Plan' will be reached, which consists in identifying weaknesses and security vulnerabilities discovered during the risk analysis process for a business partner. The plan assigns responsibility for corrective actions/mitigation strategies (internal and external), sets deadlines/ time period, documents evidence of actions taken, describes processes used to verify what actions have been taken, and outlines the final outcome.

Security risk degree

For the C-TPAT, each company is responsible for establishing its own security risk level system based on its business model. It is understood that businesses use various methodologies to assess risks within their international supply chains. However, the use of the following "Risk Degrees" is recommended when assessing security threats and vulnerabilities within the international supply chain.

evaluar riesgos dentro de sus cadenas de suministro internacional. Sin embargo, se recomienda el uso de los siguientes "Grados de Riesgo" al evaluar las amenazas y las vulnerabilidades de seguridad dentro de la cadena de suministro internacional.

Análisis de amenaza

Hay muchas fuentes cuya información puede proporcionar a la empresa una lista de amenazas para su cadena de suministro internacional. Después de realizar una investigación, se recomienda asignar un grado de riesgo de amenaza basado en lo siguiente:

1. **Riesgo Bajo** - Ningún incidente reciente / inteligencia / información.
2. **Riesgo Medio** - Ningún incidente reciente / cierta inteligencia / información sobre la probabilidad de actividad.
3. **Riesgo Alto** - Incidentes e inteligencia / información reciente. Una calificación de 3 en cualquiera de las siguientes áreas pone la cadena de suministro en "Alto Riesgo": 1) Terrorismo, 2) Contrabando de materiales ilícitos, 3) Contrabando Humano, 4) Crimen Organizado.

Análisis de vulnerabilidad

Un método que se puede utilizar para realizar un análisis de vulnerabilidad es enviando encuestas sobre la seguridad de socios comerciales que no son elegibles ni participan en el programa C-TPAT (u otro programa). Las encuestas deben estar basadas en el proceso realizado por el socio en la cadena de suministro internacional (ej. obtención, producción, empaque, almacenaje, cargamento / descarga, transporte, y preparación de documentos).

Las preguntas en la encuesta deben pedir que el socio describa las medidas de seguridad utilizadas, sin aceptar respuestas solo con un "Sí / No". La encuesta debe preguntar si existe un sistema

"Para el C-TPAT cada empresa es responsable en establecer su propio sistema de grado de riesgo de seguridad basado en su modelo comercial."

"For the C-TPAT, each company is responsible for establishing its own security risk level system based on its business model."

Threat analysis

There are many sources whose information can provide the company with a list of threats to its international supply chain. After conducting an investigation, it is recommended to assign a threat risk degree based on the following:

1. **Low Risk** - No recent incident / intelligence / information.
2. **Medium Risk** - No recent incident / certain intelligence / information on the probability of activity.
3. **High Risk** - Incidents and intelligence / recent information. A rating of 3 in any of the following areas puts the supply chain at "High Risk": 1) Terrorism, 2) Smuggling of illicit materials, 3) Human Trafficking, 4) Organized Crime.

Vulnerability analysis

One method that can be used to conduct a vulnerability analysis is sending security surveys about non-eligible business partners that are not participating in the C-TPAT program (or other program). Surveys should be based on the partner process in the international supply chain (e.g. procurement, production, packaging, storage, loading/unloading, transportation, and document preparation).

The questions in the survey should ask the partner to describe the security measures used, without accepting only "Yes/No" answers. The survey should ask whether there is a system of reviews, balances, and accountability, particularly in areas used to secure international traffic instruments, cargo tracking and monitoring, seal security, and partner research (subcontracted).

The following is a recommended vulnerability risk degree (according to the C-TPAT basic

Proceso de análisis de riesgos en 5 pasos

	Proceso	Descripción	Métodos	Recursos
1	Cómo trazar el flujo de carga y de socios	Identificar TODOS los participantes en los siguientes procesos: 1. Obtención 2. Producción 3. Empaque 4. Almacenamiento 5. Embarque/Descarga 6. Transporte 7. Preparación de documentos	1. Exigir información del socio 2. Revisar documentos (BOLs,manifiestos, facturas, etc.) para determinar la ruta 3. Visitas a la instalación, auditorias de la cadena de suministro	Trazo del flujo de carga, identificando socios y procesos
2	Realizar un análisis de riesgos	Identificación y grado de riesgo de amenazas (Alto, Medio, Bajo) por país y región por cada cadena de suministro internacional, utilizando lo siguiente (por lo menos): 1. Terrorismo (político, biológico, agrícola, cyber) 2. Contrabando de materiales ilícitos 3. Contrabando de personas 4. Crimen organizado 5. Condiciones que fomentan las amenazas	1. Fuentes de información vía organizaciones estatales y privadas 2. Representantes/Contactos, presentes en origen 3. Autoridades (extranjero / domestico), local, estatal, federal, nacional 4. Organizaciones de comercio y seguridad 5. personal de C-TPAT asignado	Recursos para hallar amenazas. Consultar webs de Cargo Security Alliance, U.S. Department of Commerce, International Maritime Organization, Global Security Newswire, Customs and Border Protection, etc., etc. Para el análisis de amenazas utilizar como fuentes: Nombre de noticieros o publicaciones, entidad estatal, servicios de inteligencia, etc.
3	Realizar un análisis de vulnerabilidad	Para todos los socios en la cadena de suministro internacional (contratado o subcontratado directamente): 1. Identificar el proceso que realizan 2. Verificar que los socios cumplan con los criterios mínimos de seguridad aplicables 3. Clasifique la conformidad dentro de cada categoría del criterio mínimo que aplica (Alto, Medio, Bajo)	1. Numero de SVI/C-TPAT membresía 2. Membresía en un “Programa Mutuo de Reconocimiento” 3. Encuestas de seguridad 4. Visitas a instalaciones por representantes de la empresa 5. Visitas a instalaciones por personal/agentes extranjeros 6. Reportes de negocio 7. Certificaciones de seguridad quecumplen con el criterio mínimo de C-TPAT 8. Análisis de riesgo realizados por una tercera empresa	Análisis de vulnerabilidad utilizando los criterios mínimos de seguridad de C-TPAT, por ejemplo.
4	Preparar un plan de acción	Establecer un plan de acción corrective para vacíos o vulnerabilidades descubiertas en programas de seguridad de socios.	1. Documento ‘Word’ 2. Hoja de cálculo ‘Excel Spreadsheet’ 3. Software de manejo de proyecto	Plan de acción y seguimiento
5	Documentar el proceso de un análisis de riesgo	Una descripción de dirección, políticas, y procedimientos de compañías sobre cómo realizan un análisis de riesgo interno de su cadena de suministro internacional.	1. Documentar la política de empresas para realizar un análisis de riesgo en la cadena de suministro internacional. 2. Documentar los procedimientos utilizados para realizar un análisis de riesgos en la cadena de suministro internacional.	Documentar procesos, políticas y procedimientos de un análisis de riesgos.

Fuente / Source: Adaptación de documento “C-TPAT. Análisis de Riesgos en 5 Pasos. Guía de procedimientos”

de revisiones, balances, y responsabilidad, particularmente en áreas utilizadas para asegurar los instrumentos de tráfico internacional, el rastreo y supervisión de carga, seguridad de precintos, e investigaciones de socios (subcontratados).

El siguiente es un grado de riesgo de vulnerabilidad recomendado (según los criterios mínimos de seguridad del C-TPAT): Requisitos de socios comerciales, Seguridad de instrumentos de tráfico internacional, Seguridad procesal, Seguridad física, Controles de acceso físico, Seguridad de personal, Capacitación de seguridad y conocimiento de amenazas, y Seguridad de tecnología informática.

1. **Riesgo Bajo** - Cumple con todos los criterios mínimos de seguridad.
2. **Riesgo Medio** - Cumple con los criterios mínimos en áreas críticas (ej. la seguridad de remolques, precintos, rastreo, y el proceso de reclutamiento), pero no ha incorporado todas las medidas de seguridad en otras áreas.
3. **Riesgo Alto** – No cumple con todos los criterios mínimos de seguridad.

Ejemplo de resultados hipotéticos

a. Si todas las secciones que se “deben” tener para cumplir con la seguridad de remolques, precintos, rastreo, y el proceso de reclutamiento están cumplidas, el grado de riesgo para esa categoría sería “1 – Riesgo Bajo.”
b. Si todas las secciones que se “deben” tener para cumplir con la seguridad de remolques, precintos, rastreo, y el proceso de reclutamiento están cumplidas pero las de capacitación de seguridad o de seguridad física no, el grado sería “2 – Riesgo Medio.”
c. Si una sección que se “debe” tener para cumplir con la seguridad de remolques, precintos, rastreo, y el proceso de reclutamiento no están cumplidas, sería clasificado “3 – Riesgo Alto”.

La documentación del proceso de análisis de riesgos

El proceso documentado de análisis de riesgo (ej. las políticas y procedimientos) deben contener, por lo mínimo, la siguiente información: Fecha del proceso; Identificación de personas responsables en mantener el proceso al día, incluyendo personas de respaldo; Cuándo se deben realizar los análisis de riesgo (ej. Proveedor nuevo); El periodo en que se realizarán los análisis (ej. Según las circunstancias o, mínimo, anualmente); La frecuencia requerida de revisiones a procesos /políticas / procedimientos relativo a los análisis de riesgo; Cómo se realizarán los análisis de amenazas (ej. Fuentes utilizadas); Cómo se realizarán los análisis de vulnerabilidad (ej. Enviar encuestas, visitas físicas, participación en un programa de seguridad); Cómo se realizará el seguimiento de esas áreas que requieren ‘acción’ (ej. Visitas físicas en algunos casos, en otros documentación / fotos); Proceso para proveer capacitación a personal clave responsable por el proceso; Supervisión corporativa para asegurar que el proceso se realice consistentemente y eficientemente. CS

safety criteria): Business Partner Requirements, International Traffic Instrument Security, Procedural Security, Physical Security, Physical Access Controls, Personnel Security, Security training and knowledge of threats, and Security of computer technology.

1. **Low Risk** - Meets all basic security criteria.
2. **Medium Risk** - It meets basic criteria in critical areas (e.g. trailer security, seals, tracing, and recruitment process), but has not incorporated all security measures into other areas.
3. **High Risk** - Does not meet all basic security criteria.

Example of hypothetical results

a. If all the sections that one “must” have to comply with trailer security, seals, tracking, and the recruitment process are met; the risk degree for that category would be “1 - Low Risk.”
b. If all the sections that one “must” have to comply with trailer security, seals, tracing, and the recruitment process are met but the security or physical security trainings are not; the degree would be “2 - Medium Risk.”
c. If a section that one “must” have to comply with trailer security, seals, tracking, and the recruitment process are not met, it would be classified as “3 - High Risk”.

Risk analysis process documentation

The documented process of risk analysis (e.g. policies and procedures) should contain, at least, the following information: Date of the process; Identification of responsible people in keeping the process up to date, including back-ups; When to carry out the risk analysis (e.g. New supplier); The period in which the analyzes will be carried out (e.g. depending on the circumstances or at least annually); The required frequency of reviews to processes / policies / procedures related to risk analysis; How threats analysis will be performed (e.g. sources used); How vulnerability analysis will be carried out (e.g. sending surveys, physical visits, participation in a security program); How will the follow-up be carried out in those areas that require ‘action’ (e.g. physical visits in some cases, other documentation / photos); Process to provide training to key personnel responsible for the process; Corporate oversight to ensure the process is performed consistently and efficiently. CS

Fuente / Source: Adaptación de documento “C-TPAT. Análisis de Riesgos en 5 Pasos. Guía de procedimientos”, 2014 / Adaptation of C-TPAT Five Step Risk Assessment Process document, 2014.

Los Sistemas de gestión con enfoque basado en la gestión de riesgos

THE MANAGEMENT SYSTEMS WITH A RISK MANAGEMENT-BASED SCOPE

Escribe/ Write: Kandy Escobar. Gerente de Formación y Capacitación de BASC PERÚ.

La Administración del Riesgo en las organizaciones es un tema que lleva muchos años en el mercado; sin embargo, recién se está tomando conciencia de que la Gestión del Riesgo es la columna vertebral para la implementación, mantenimiento y mejora de los sistemas de gestión en una organización.

En la actualidad, la gestión del riesgo se ha convertido en un deber primordial en las organizaciones que la Alta Dirección debe asumir como parte de los compromisos estratégicos para la prevención del riesgo asociado a su negocio y ante la necesidad de implementación de un sistema de gestión en la empresa.

Para ello se recomienda establecer un Marco General para la gestión del riesgo, el mismo que se ilustra en el cuadro de la siguiente página.

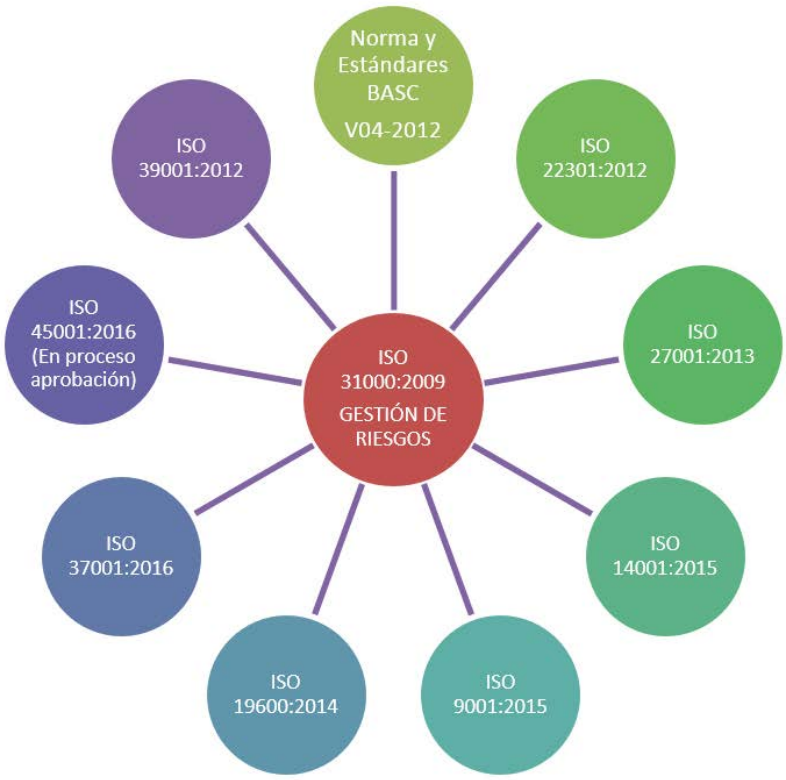
Con este enfoque podemos apreciar que la tendencia en las actualizaciones de los Sistemas de Gestión incluye

For organizations, Risk Management is an issue that has been in the market for many years; however, it is only recently becoming aware that risk management is the backbone for the implementation, maintenance and improvement of management systems in an organization.

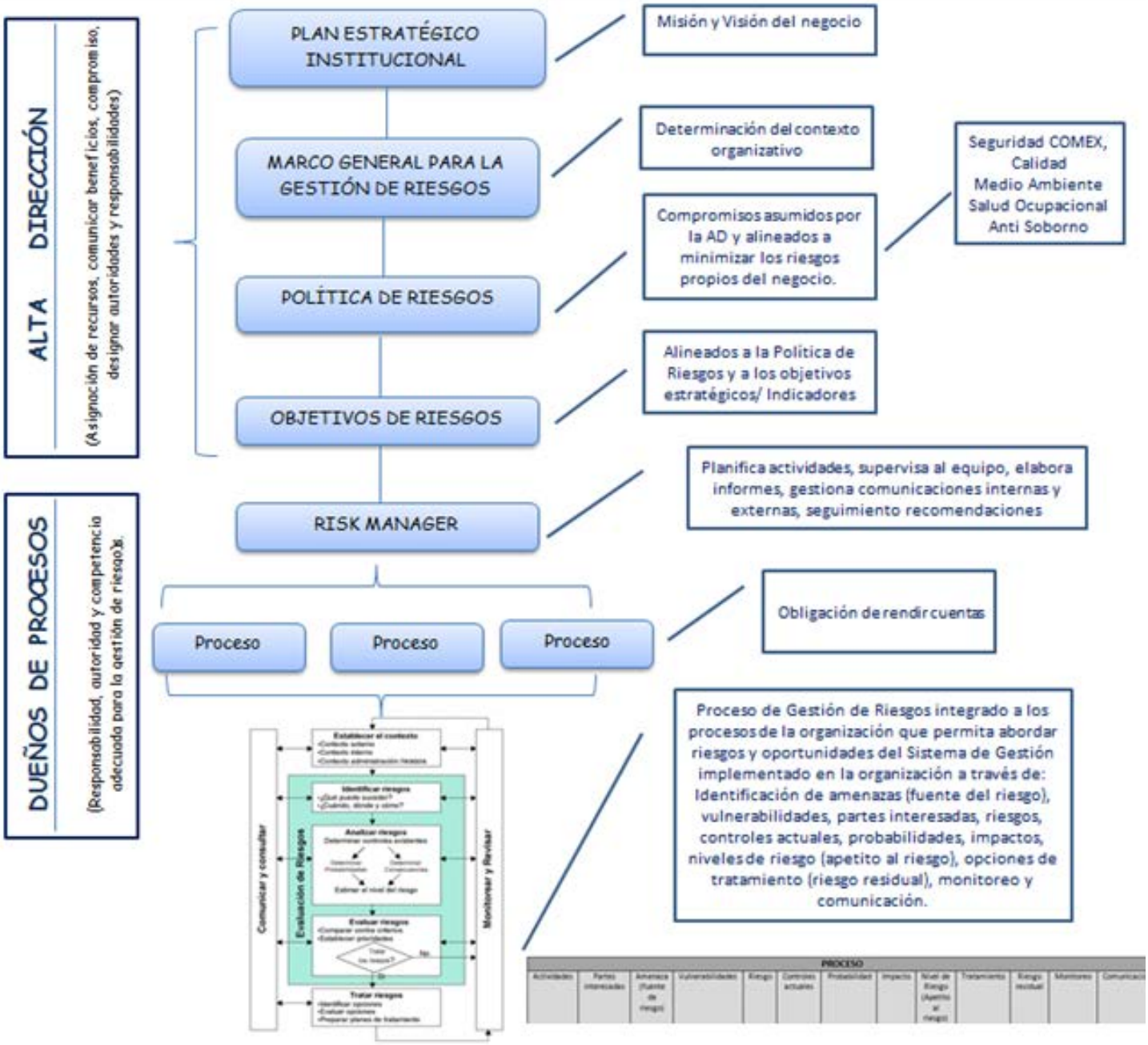
Currently, risk management has become a primary duty in organizations and, due to the need to implement a management system in companies, the Top Management must assume it as part of the strategic commitments for risk prevention associated with its business.

Therefore, it is recommended to establish a General Framework for risk management, which is exemplified below:

Thus, with this approach, we find that the trend for Management Systems updates includes as the



Fuente / Source: Elaboración propia / Own elaboration.



Fuente / Source: Elaboración propia / Own elaboration.

como principal cambio “las acciones para abordar el riesgo y las oportunidades, la valoración del riesgo, el plan de tratamiento, el monitoreo y la comunicación a las partes interesadas tanto internas como externas”. En el siguiente gráfico se citan algunas de las normas que tienen como referencia este enfoque.

Es preciso mencionar que la norma ISO 31000:2009 y la guía 73 sobre la terminología de la gestión del riesgo, no son una excepción en esta tendencia de cambios y actualizaciones. Es así que desde marzo del 2015 se inició la revisión de esta Norma para discutir los cambios necesarios que deben introducirse y la primera revisión de la norma ISO 31000 Risk Management - Guidelines, en su versión DRAF, se encuentra disponible desde el 17 de Febrero de 2017.

La votación termina el 11 de Mayo de 2017. Mayor información se encuentra disponible en el siguiente link: https://lnkd.in/ebG4-HJ.* CS

main change “actions to address risk and opportunities, risk assessment, treatment plan, monitoring and communication to both internal and external stakeholders”. Below are some of the rules that refer to this approach: It should be mentioned that ISO 31000: 2009 and guide 73 on risk management terminology are no exception in this trend of changes and updates. Thus, since March 2015, the revision of this Standard has been initiated to discuss the necessary changes that need to be introduced, and the first revision of the ISO 31000 Risk Management - Guidelines, in its DRAF version, has been available since February 17, 2017. Voting ends on May 11, 2017. More information is available at the following link: https://lnkd.in/ebG4-HJ.* CS

Fuente / Source: International Organization for Standardization (ISO).

Encuesta a 145 empresas europeas sobre

Gestión de riesgos operacionales de la cadena de suministro

SURVEY FOR 145 EUROPEAN COMPANIES ABOUT SUPPLY CHAIN OPERATIONAL RISK MANAGEMENT

En los meses de Agosto y Septiembre de 2015, la consultora Generix Group, compañía francesa de software y soluciones, realizó una encuesta a 145 empresas con actividades en los sectores de alimentos, bienes de consumo e industrial, para hacer un balance de los riesgos operacionales asociados a la Cadena de Suministro.

Los resultados de esta iniciativa arrojan interesantes aspectos para los ejecutivos de compañías ubicadas en esta parte del mundo, quienes pueden darse una idea de las prioridades, preocupaciones y expectativas de sus pares europeos en este campo, lo cual podría servirles para elaborar estrategias de negocios más asertivas con esa importante zona comercial.

Para Generix Group los problemas de seguridad son algunos de los retos más difíciles de abordar por los gerentes de la cadena de suministro. “Las amenazas son muchas, potencialmente destructivas y a menudo imposibles de predecir. La principal dificultad radica en conseguir una visión de extremo a extremo de la Cadena para controlar. Los tres pilares de una política de seguridad son: anticipar riesgos, reaccionar rápidamente y minimizar los impactos” señala la empresa.

In the months of August and September 2015, Generix Group, a French software and solutions company, surveyed 145 companies with activities in the food, consumer goods and industrial sectors to take stock of the operational risks associated with the Supply Chain.

The results of this initiative give interesting insights to the executives of companies located in this part of the world, who can give an idea of the priorities, concerns and expectations of their European peers in this field, which could serve them to elaborate more assertive business strategies with this important commercial region.

For Generix Group, security issues are some of the most difficult challenges for supply chain managers. “There are many threats, potentially destructive and often impossible to predict. The main difficulty lies in getting an end-to-end view of the Chain to control. The three pillars of a security policy are: anticipate risks, react quickly and minimize impacts”, says the company.

La complejidad de los procesos logísticos, la velocidad de ejecución esperada, la influencia geográfica del comercio y la multiplicidad de actors (transportistas, transitarios, puertos, aeropuertos,

proveedores, contratistas, clientes, aduanas...) no facilitan la tarea de prestar y garantizar un servicio de calidad a los clientes.

Los riesgos abundan y todos implican costos directos e indirectos, deteriorando la imagen corporativa, la pérdida de clientes e incluso la quiebra de la empresa, si no es capaz de retener, de principio a fin, el control operativo de su Cadena de Suministro.

¿Cómo protegerse? El principio básico es lograr visibilidad en toda la Cadena de Suministro: desde el proveedor hasta el cliente final (o cliente a cliente), pasando por todos los interesados. Para ello "es necesario accionar varias palancas" dice Generix Group.

En primer lugar, una palanca organizacional con subidas de información periódica realimentada internamente, por los proveedores y todos los interesados en la Cadena de Suministro. Siguiendo por una palanca de gestión, con la participación de todos los directivos y empleados de la empresa y sus socios, con el fin de aportar planes de continuidad del negocio y gestionar las crisis. Por último, una palanca tecnológica, la puesta en marcha de herramientas y conocimientos adecuados y soluciones de software a medida que ofrecen la visión necesaria de principio a fin a todos los actores de la cadena de suministro.

Los temas más importantes

62%	62% Mejorar el rendimiento
53,8%	53,8% Disminuir los costos
52,4%	52,4% Reducir los riesgos
46,2%	46,2% Conducir el negocio (ventas y planeación de operaciones)
46,2%	46,2% Mejorar la flexibilidad

Fuente: Encuesta Gestión de riesgos operacionales de la Supply Chain. Generix Group 2015.

Los resultados de la encuesta muestran que ocho de cada diez empresas ven los riesgos como una cuestión importante y grave. En concreto, se trata de identificar los problemas, los riesgos operacionales clave más temidos y priorizar los recursos utilizados por las empresas para protegerse a sí mismos.

LOS RETOS DE LOS GERENTES

Mejorar el rendimiento, disminuir costos, medir los riesgos operacionales.

Las empresas encuestadas destacan la necesidad de mejorar el rendimiento de la Cadena de Suministro, reducir los costos y los riesgos operacionales y tener un buen control sobre ella. Para ocho de cada diez empresas, este problema de seguridad se considera importante.

Aumentar niveles de servicio y satisfacción del cliente

La calidad de la Cadena de Suministro se evalúa de principio a fin. Dos indicadores son particularmente críticos para medir esta calidad: la tasa de servicio, que refleja la velocidad de abastecimiento en tiempo y hora, y la satisfacción del cliente. Hoy en día es muy difícil separar estos dos elementos ya que

The complexity of supply chain processes, the expected execution speed, the geographical influence of trade and the multiplicity of actors (carriers, ports, airports, suppliers, contractors, customers, customs...) do not facilitate the task of providing and guaranteeing a quality service to customers.

Risks are plentiful and all involve direct and indirect costs. They deteriorate the corporate image, lose customers and can even bankrupt the company if a company is not able to retain, from beginning to end, the operational control of its Supply Chain.

How to protect yourself? The basic principle is to achieve visibility throughout the Supply Chain: from the supplier to the end customer (or customer to customer), passing by all stakeholders. For this "it is necessary to activate several levers" says Generix Group.

First, there is an organizational lever with periodically updated intern feedback, by suppliers and all stakeholders in the Supply Chain. Then, there is a management lever, with the participation of all managers and employees of the company and its partners, in order to provide business continuity plans and manage crises. Finally, a technological lever, the implementation of appropriate tools and knowledge and software solutions as they provide the necessary vision from start to finish to all actors in the supply chain.

The results of the survey show that eight out of ten companies view risks as a major and serious issue. Specifically, it seeks to identify the most feared key operational problems and risks and prioritize the resources used by companies to protect themselves.

THE MANAGERS CHALLENGES

Improve performance, reduce costs, measure operational risks.

Companies surveyed stress the need to improve Supply Chain performance, reduce costs and operational risks and have good control over it. For eight out of ten companies, this security problem is considered important.

Increase service levels and customer satisfaction

The quality of the Supply Chain is evaluated from start to finish. Two indicators are particularly critical in measuring this quality: the service rate, which reflects the speed of delivery in time and time elapsed, and customer satisfaction. Today it is very difficult to separate these two elements as

la calidad intrínseca de la Cadena de Suministro determina la satisfacción del cliente. Un deterioro en el desempeño aguas arriba tiene repercusiones inevitables sobre el cliente final. Por tanto, se convierte en esencial tener la información correcta para anticipar cualquier anomalía con el fin de ponerle remedio lo antes posible.

Ganar flexibilidad y agilidad

Si bien la agilidad y flexibilidad no son las primeras preocupaciones para los responsables de la Cadena de Suministro, sí son cuestiones preocupantes para ellos. La flexibilidad se refiere a la capacidad de responder rápidamente cuando sea necesario. La agilidad va más allá mediante la integración de una capacidad de anticipación en la Cadena de Suministro. Supone una visibilidad más amplia de ésta y compartir entre todos los actores la información. Por lo tanto, un proveedor puede identificar un retraso en la entrega y buscar soluciones alternativas para proponérselas a su cliente antes de que se vea afectado por un retraso inesperado.

¿CUÁLES SON LOS RIESGOS OPERATIVOS PARA LA SUPPLY CHAIN?

La falta de disponibilidad de los sistemas de información

Estamos en un momento en el que "todo está conectado". Cada vez más información y más servicios están permanentemente disponibles en la web o móvil, por lo que cualquier fallo en los sistemas de información puede tener graves consecuencias para la empresa: costos directos, pérdida de clientes, degradación de la imagen de la empresa. Según CLUSIF (Club de la Seguridad de Sistemas de Información Francesa), muestra que sólo el 1% de las empresas consideran que la dependencia a sus sistemas de información es baja; ocho de cada diez empresas considera que esta dependencia es muy fuerte.

El riesgo asociado a la falta de disponibilidad del sistema de información es grave por lo menos por tres razones: En primer lugar, la cantidad de actores involucrados en la gestión de la Cadena de Suministro se verían afectados (la empresa, sus proveedores, sus transportistas, sus clientes, los clientes de

Cuatro conceptos claves de seguridad

Disponibilidad	Se define como la capacidad de un sistema de información de ser utilizado en cualquier momento, en función del rendimiento esperado. La disponibilidad es tan importante como la integración del sistema de información con aplicaciones de terceros. (vínculos con subcontratistas, socios, etc.)
Integridad	Asegura que la información no sufra modificaciones en el momento del envío y recepción por sus destinatarios. Esto asegura que los datos no se alteran cuando se cobran, almacenan, procesan y devuelven.
Confidencialidad	Asegura que solo los usuarios autorizados tienen acceso a los sistemas y datos, con controles de acceso, encriptación y autentificación.
Trazabilidad	Es la posibilidad de seguir paso a paso todas las operaciones básicas que condujeron al resultado, con el fin de atribuir con certeza a un usuario una acción efectuada en un momento dado.

Fuente: Encuesta Gestión de riesgos operacionales de la Supply Chain. Generix Group 2015.

the intrinsic quality of the Supply Chain determines customer satisfaction. Deterioration in upstream performance has inevitable repercussions on the end customer. Therefore, it becomes essential to have the correct information to anticipate any anomaly in order to correct it as soon as possible.

Increase flexibility and agility

While agility and flexibility are not the primary concerns for Supply Chain managers, they are a matter of concern to them. Flexibility refers to the ability to respond quickly when necessary. Agility goes further by integrating anticipation capacity into the Supply Chain. It implies a broader visibility of this and the sharing of information among all actors. Therefore, a supplier can identify a delay in delivery and look for alternative solutions to propose to its customer before it is affected by an unexpected delay.

WHAT ARE THE OPERATIONAL RISKS FOR THE SUPPLY CHAIN?

The lack of availability of information systems

These days "everything is connected". More information and more services are permanently available on the web or mobile, so any failure in information systems can have serious consequences for the company: direct costs, customer loss, degradation of the company's image. According to CLUSIF (French Information Systems Security Club), only 1% of companies consider that dependence on their information systems is low; eight out of ten companies consider that this dependence is very strong.

The risk associated with unavailability of the information system is serious for at least three reasons: First, the number of actors involved in supply chain management would be affected (the company, its suppliers, its carriers, its customers, its customers' customers). Secondly, due to the

sus clientes). En segundo lugar, debido a la sensibilidad del cliente final en relación a la calidad de la entrega, en particular cuando éste se basa en el JIT (Just in Time).

Si se produce un error en el sistema de información puede conducir a la pérdida de clientes y por lo tanto a pérdidas en el negocio. Y por último, la sensibilidad a la que está expuesta la Cadena de Suministro cuando existen interrupciones del sistema de información de sus principales aplicaciones (APS, WMS o TMS) encargadas del pilotaje de procesos de ejecución en tiempo real donde el fracaso a menudo, implica la incapacidad de disponer de recursos para estar en pleno funcionamiento operacional.

El fallo de los proveedores

Los responsables de la Cadena de Suministro encuestados citan el riesgo de fallo de los proveedores como la segunda amenaza a la que se enfrentan. A menudo es difícil anticipar el riesgo al fallo, sobre todo si las causas están relacionadas con los fenómenos naturales, problemas de liquidez repentinos o roturas en la Cadena de Suministro de sus propios proveedores.

Varios factores contribuyen a agravar los riesgos operacionales y las consecuencias de los fallos de los proveedores. El aumento del uso de la subcontratación aumenta el número de partes interesadas, la globalización aumenta la externalización en los países emergentes dónde los estándares son diferentes, la acentuada dependencia hacia los proveedores estratégicos, la tendencia que privilegia las "cero existencias" y los flujos tensos, y la especialización de las líneas de producción de acuerdo a los productos o componentes.

¿Qué debe incorporar un plan de gestión de crisis eficiente?

Documentar la infraestructura dedicada (sala equipada con conexiones seguras, estaciones de trabajo, documentación, líneas telefónicas de múltiples operadores)
Señalar un responsable de activar el plan de acción de crisis. Listas a los miembros del plan de acción (con números de teléfono).
La descripción del trabajo de cada uno y los medios (presupuesto, recursos humanos, herramientas de software, consultores externos) que tienen.
Definir los escenarios típicos y las consecuencias operacionales de la empresa.
Establecer un plan de comunicación, a nivel interno, a los medios de comunicación y las redes sociales.

Fuente: Encuesta Gestión de riesgos operacionales de la Supply Chain. Generix Group 2015.

La imprevisibilidad de picos de volumen

No ser capaz de hacer frente a los picos de volumen inesperados es el tercer riesgo más temido por los responsables de la Cadena de Suministro. Este riesgo se sitúa incluso en la segunda posición para las empresas del sector de venta al por menor, al por mayor, agroalimentación, bienes de consumo, industria y electrónica.

Pronosticar los picos de volúmenes resulta muy difícil de lograr. Basarse en las tendencias pasadas para anticipar las futuras, es una pista a corto o medio plazo pero es un enfoque que rápidamente encuentra sus límites (mala calidad de datos, efectos estacionales, renovación de productos, especificidades geográficas). Del mismo modo, el análisis predictivo aún no

sensitivity of the final customer in relation to the quality of delivery, particularly when it is based on JIT (Just in Time).

Failure in the information system can lead to loss of customers and therefore to losses in the business. And finally, the sensitivity to which the Supply Chain is exposed when there are interruptions of the information system on its main applications (APS, WMS or TMS) responsible for the piloting of real-time execution processes where failure often implies the inability to have the resources to be fully operational.

Failure of suppliers

The surveyed Supply Chain managers cite the risk of supplier failure as the second threat they face. It is often difficult to anticipate the risk of failure, especially if the causes are related to natural phenomena, sudden liquidity problems or breakages in the Supply Chain of its suppliers.

Several factors contribute to aggravate operational risks and the consequences of supplier failures: increased use of outsourcing increases the number of stakeholders; globalization increases outsourcing in emerging countries where standards are different; strong dependence on strategic suppliers; the trend that favors "zero supplies" and tense flows and the specialization of the production lines according to the products or components.

The unpredictability of volume peaks

Not being able to cope with unexpected volume spikes is the third most feared risk by Supply Chain managers. This risk is even in the second position for companies in the retail, wholesale, food/agriculture, consumer goods, industrial and electronics sectors.

Forecasting peak volumes is very difficult to achieve. Based on past trends to anticipate future ones, it is a short or medium term track but it is an approach that quickly finds its limits (poor data quality, seasonal effects, product renewal, geographic specificities). Likewise, predictive analysis is not yet adapted to the Supply Chain, especially since transactions are normally increasing. Hence the need to focus on real-time information to respond quickly to any change in the expectation of volume processing.

está adaptado a la Cadena de Suministro, sobre todo porque las transacciones están normalmente aumentando. De ahí la necesidad de centrarse en la información en tiempo real para responder rápidamente a cualquier cambio en las expectativas del procesamiento de los volúmenes.

¿CÓMO PROTEGERSE?

Recopilar y compartir buena información

La gestión de riesgos operacionales y su anticipación se basa principalmente en el intercambio de conocimientos e información. Las empresas prefieren sistemas de subida de información y alertas operacionales sobre los acontecimientos que afecten a la Cadena de Suministro, tanto a nivel interno como relacionada con los proveedores externos. Estas alertas internas se han citado como la primera palanca para gestionar los riesgos operacionales que afectan a la Cadena de Suministro.

Volcar la información adecuada en tiempo real les permite ser proactivos para detectar lo antes posible fuentes de disfunción y remedios antes de que sea demasiado tarde, antes incluso de impactar negativamente sobre el cliente. La implementación de un proceso de información que presente informes requiere varios requisitos previos:

- La disponibilidad de información de múltiples fuentes
- La calidad de información explotable
- La capacidad de integrar todos los datos para tener una visibilidad completa de los flujos, por ejemplo, con una herramienta tipo “torre de control”
- El desarrollo de indicadores pertinentes.

El reto para construir un sistema de retroalimentación de información eficaz en tiempo real, sigue siendo integrar múltiples tipos de datos representativos de los principales procesos de la Cadena de Suministro: recepción, almacenamiento, flujos procesados, devoluciones, condiciones de envasado, control de conformidad, seguimiento de las preparaciones, trazabilidad de los transportistas, estado de las entregas, gestión de los acontecimientos.

Analizar los riesgos operativos y optimizar los procesos críticos.

Una cadena de suministro puede enfrentarse a dos tipos de riesgos:

- **Los riesgos menores** cuya probabilidad de aparición es relativamente alta, pero cuyo impacto sigue siendo individual (pérdida de un pallet durante un reparto, retraso de una carga)
- **Los riesgos importantes** cuya probabilidad de aparición es pequeña pero con un gran impacto, incluso catastrófico (no disponibilidad de los sistemas de información por un retraso, una catástrofe natural, otros). Los riesgos menores que producidos con demasiada frecuencia pueden tener un impacto significativo para la empresa.

El requisito previo para cualquier política de seguridad

HOW TO PROTECT YOURSELF?

Gather and share good information

The management of operational risks and their anticipation is mainly based on the exchange of knowledge and information. Companies prefer information systems and operational alerts on events affecting the Supply Chain, both internally and related to external suppliers. These internal alerts have been cited as the first lever to manage operational risks affecting the Supply Chain.

Pouring the right information in real time allows them to be proactive to detect as soon as possible sources of dysfunction and solutions before it is too late, before negatively impacting the client. The implementation of an information process that presents reports requires several prerequisites:

- The availability of information from multiple sources
- The quality of exploitable information
- The ability to integrate all the data to have a complete visibility of the flows, for example, with a tool like “control tower”
- The development of relevant indicators.

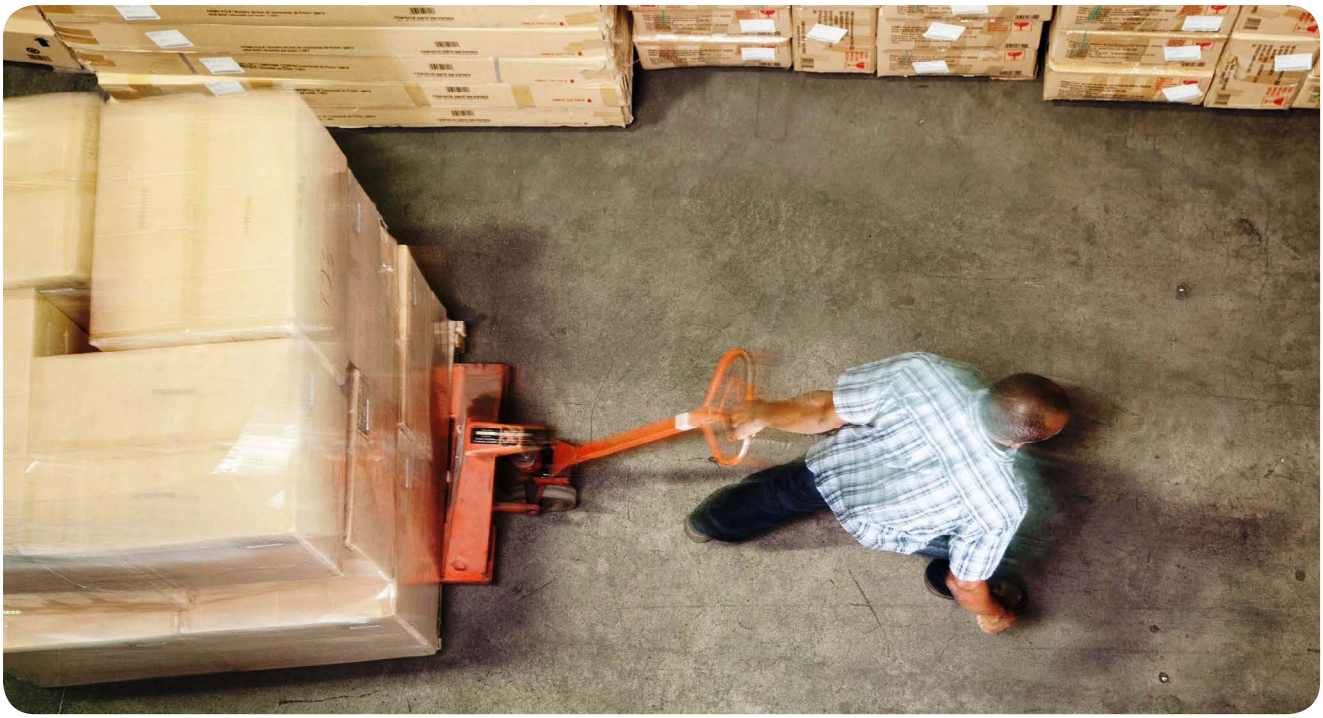
The challenge to build a real-time, effective information feedback system is to integrate multiple types of data representative of the main processes of the Supply Chain: reception, storage, processed flows, returns, packaging conditions, conformity control, follow-up of preparations, traceability of carriers, status of deliveries, management of events.

Analyze operational risks and optimize critical processes.

A supply chain can deal with two types of risks:

- Minor risks whose probability of occurrence is relatively high, but whose impact remains individual (loss of a pallet during distribution, delay of cargo)
- Major risks whose probability of occurrence is small but with a great impact, even catastrophic (unavailability of information systems due to delay, natural catastrophe, others). Minor risks that occur too often can have a significant impact on the company.

The prerequisite for any security policy is the detailed analysis of the operational risks to which a Supply Chain may be confronted. This implies a work threat of impact analysis (direct and indirect), the assessment of potential threats



es el análisis detallado de los riesgos operativos a los que una Cadena de Suministro puede enfrentarse. Esto supone una amenaza de trabajo de análisis de impactos (directos e indirectos), la evaluación de amenazas potenciales y la definición de escenarios de riesgo en función de su gravedad. Conocer sus riesgos no es suficiente, sin embargo, tenemos que ser capaces de hacerlos frente cuando éstos se producen.

Es interesante tener un proceso de gestión de crisis y toda la información necesaria, en caso de que aparezca una crisis, pero también aguas arriba (antecedentes o previos) para prevenir su aparición y proliferación.

Desarrollar un plan de continuidad del negocio

Además del análisis de amenazas y el desarrollo de un plan de gestión de crisis eficaz, la gestión del riesgo operacional deberá garantizar la continuidad de la Cadena de Suministro. Tal como se sabe, no es posible soportar una indisponibilidad prolongada de los sistemas de información, de hecho, es el primer riesgo percibido por las empresas en sus actividades logísticas.

La tarea de un responsable de la Cadena de Suministro es reducir al mínimo el tiempo de inactividad de los flujos logísticos. En ausencia de un plan de continuidad, esta misión parece difícilmente concebible.

Para ser eficaz, un plan de continuidad de negocio debe incluir varios elementos, en particular, las condiciones operacionales en los procedimientos de recuperación en la Cadena de Suministro, soluciones de emergencia para diversos componentes (copias de seguridad, redes de telecomunicaciones, sistemas de información), los recursos disponibles, las distintas responsabilidades, el plan de crisis.

La encuesta revela que en este punto las empresas europeas necesitan avanzar. Por ejemplo, de cada diez empresas, menos de una presenta la integración de la Cadena de Suministro en el plan general de continuidad del negocio de la empresa, siendo el elemento esencial para evitar perder el control de la situación. CS

and the definition of risk scenarios according to their severity. Knowing their risks is not enough, however, we have to be able to face them when they occur.

It is interesting to have a crisis management process and all the necessary information, in case of a crisis, but also upstream (background or previous) to prevent their emergence and proliferation.

Develop a Business Continuity Plan

In addition to threat analysis and the development of an effective crisis management plan, operational risk management must ensure the continuity of the Supply Chain. As it is known, it is not possible to support a prolonged unavailability of information systems, in fact, it is the first risk perceived by companies in their **supply chain activities.**

The task of a Supply Chain Manager is to minimize the downtime of supply chain flows. Without a continuity plan, this mission seems difficult to conceive.

In order to be effective, a business continuity plan should include several elements, in particular, the operational conditions in the Supply Chain recovery procedures, emergency solutions for various components (backups, telecommunications networks, information systems), The resources available, the different responsibilities, the crisis plan.

The survey reveals that at this point European companies need to move forward. For example, out of every ten companies, less than one presents the integration of the Supply Chain into the general business continuity plan of the company, being the essential element to avoid losing control of the situation. CS

Fuente / Source: "Gestión de riesgos operacionales de la cadena de suministro" Generix Group, 2015.

El manejo del riesgo en empresas peruanas

RISK MANAGEMENT IN PERUVIAN COMPANIES

Debido a la influencia de la política y de hechos sociales, económicos y culturales, así como de la naturaleza, las empresas enfrentan grados de incertidumbre en su entorno operativo y estos, a su vez, generan necesidades de reacción para la alta dirección y los ejecutivos de línea.

La incertidumbre respecto a un asunto puntual puede impactar en algún momento del avance del logro de los objetivos de la empresa, posibilidad que se conoce como 'riesgo'. ¿Las empresas conocen y manejan adecuadamente el riesgo que encaran?

Respecto a este tema hemos hecho algunas preguntas a los ejecutivos de cuatro importantes empresas del comercio exterior peruano, cuyas respuestas podrían ser representativas de la situación del nivel de concienciación y del manejo que realizan el promedio de empresas en el país. Estas empresas y sus respectivos ejecutivos son:

Due to the influence of politics and social, economic, cultural and natural events, companies face degrees of uncertainty in their operating environment and these, in turn, generate needs for reaction from the senior management and line executives.

Uncertainty about a specific issue may impact at some point in the progress of achieving the company goals, a possibility that is known as 'risk'. Do companies know and properly manage the risk they face?

Regarding to this issue, we have asked the executives of four important Peruvian foreign trade companies, whose answers could be representative of the awareness level and the management that the average companies in the country perform. These companies and their respective executives are:

Erick Hein Dupont, Gerente General de TRABAJOS MARITIMOS S.A. – TRAMARSA.

Wilson Gómez Barrios, Gerente General de SECURITAS S.A.C.

Oscar Guido Echegaray Rengifo, Apoderado Legal de SOCIEDAD AGRÍCOLA VIRÚ S.A.

Gabriel Monge Aguirre, Gerente General de TERMINAL INTERNACIONAL DEL SUR S.A. – TISUR.

¿Podría hacer una breve descripción de cada uno de los tres principales riesgos que su empresa considera de atención prioritaria como parte de su política de Manejo de Riesgos?

(TRAMARSA): Riesgos Económicos, Operacionales y de seguridad.

(SECURITAS): SECURITAS entiende que, dado su giro de negocio, los riesgos más significativos de su organización están asociados al factor humano. Para ello, fundamentamos nuestra gestión en nuestros tres valores (Integridad, Eficacia y Servicio) mediante diversas herramientas.

En primer lugar, los riesgos asociados a la integridad de nuestro personal, los cuales son contemplados desde un estricto proceso de selección, hasta la gestión de nuestro Comité de Ética, pasando por procesos de capacitación en nuestro Código de Valores y Ética y el reforzamiento de estos principios mediante supervisión.

En segundo lugar, los riesgos asociados a la calidad de servicio y su implicancia en los controles de seguridad que brindamos a nuestros clientes, que son gestionados mediante capacitaciones virtuales y presenciales facilitadas por nuestra plataforma global de capacitación virtual SECURITAS ONLINE ACADEMY y nuestro CENTRO DE DESARROLLO DE COMPETENCIAS, en los cuales se refuerzan los conocimientos técnicos y legales de nuestro personal en materia de seguridad, lo cuales son posteriormente reforzados en campo mediante una Supervisión efectiva; todo esto con un trasfondo ético siempre presente y potenciado por aplicaciones tecnológicas que se incluyen dentro de nuestros Servicios de Protección.

Por último, los riesgos asociados a la predisposición del personal a una correcta ejecución de sus funciones y los medios que se requieren para ese propósito; para lo cual se ejecutan constantemente actividades de concientización y sensibilización en materia de seguridad, las cuales procuramos que se extiendan a nuestros clientes, así como que generen en nuestro personal una actitud proactiva, advirtiendo riesgos más allá de sus funciones rutinarias, agregando valor al servicio brindado al cliente.

Todo esto es potenciado mediante nuestro PREMIO VALORES SECURITAS y el PREMIO LÍDER EN

Could you give a brief description of each of the three main risks that your company considers of critical attention as part of its Risk Management policy?

(TRAMARSA): Economic, Operational and Security Risks.

(SECURITAS): SECURITAS understands that, given its type of business, the most significant risks of its organization are associated with the human factor. For this, we base our management on our three values (Integrity, Efficiency and Service) through various tools.

First, the risks associated with the integrity of our personnel, which are considered from the strict selection process, to the management of our Ethics Committee, going through training processes in our Code of Values and Ethics and the reinforcement of these principles through supervision.

Secondly, the risks associated with quality of service and its implication in the security controls we provide to our clients, which are managed through virtual and face-to-face training provided by our global virtual training platform SECURITAS ONLINE ACADEMY and our COMPETENCY DEVELOPMENT CENTER, which reinforce the technical and legal knowledge of our security personnel, which is later reinforced in the field through effective supervision; all with an ever-present ethical background and enhanced by technological applications that are included in our Protection Services.

Finally, the risks associated with the predisposition of the personnel to a correct execution of their functions and the means that are required for that purpose; for which activities of awareness raising and security awareness are constantly carried out, which we seek to extend to our clients, as well as to generate in our staff a proactive attitude, warning risks beyond their routine functions, adding value to the service provided to the client.

All of this is boosted through our SECURITAS VALUES PRIZE and the LEADER AWARD FOR SECURITY KNOWLEDGE, which seek to recognize the outstanding work of our staff and their high degree of commitment to the values of our organization.

CONOCIMIENTOS DE SEGURIDAD, los cuales buscan reconocer la labor sobresaliente de nuestro personal y su alto grado de compromiso con los valores de nuestra organización.

(VIRÚ): Los puntos que consideramos como prioritarios y de riesgos críticos que vienen siendo controlados por la empresa son: Contaminación de la carga: Virú realiza un seguimiento continuo y permanente a los controles de seguridad en toda la cadena de suministro, se inicia con la identificación y control de los puestos y proveedores críticos; control satelital a las unidades de transporte asegurándonos que éstas cumplan con exigencias de nuestro sistema de gestión integrado de seguridad.

Lavado de activos: Evaluamos a todos nuestros proveedores y clientes con los criterios máximos de seguridad (rastreo, antecedentes, lista Clinton) asegurando la custodia, así como mitigar y minimizar el riesgo que la empresa sea utilizada para actividades ilícitas.

Siniestros al sistema informático: Se realiza la verificación permanente en la Seguridad de la Información, con back ups a los equipos, control de acceso y seguridad a la información crítica, rastreo del uso de la información al personal crítico y se realizan auditorías inopinadas en forma externas.

Todos estos procesos son auditados a través de la trazabilidad de la cadena de suministro en forma inopinada, esta puede ser en cualquier momento y forma programada trimestralmente evaluándose la efectividad del sistema de seguridad integral implementado, la cual está empoderado con la participación de la alta gerencia, llevando así una supervisión continua y permanente.

(TISUR): Uno de los principales riesgos de nuestra actividad está relacionado a la seguridad en las operaciones en cuanto al manejo de carga. En relación a esto es vital contar con personal de confianza e íntegro identificado con la empresa y sensibilizado en la importancia de aplicar los controles y procedimientos establecidos para minimizar la probabilidad de alguna ocurrencia.

El segundo riesgo está relacionado a la importancia de mantener buenas relaciones con el entorno, tanto interno como externo, evitando cualquier situación que conlleve a un escenario de conflictividad que pueda impactar las operaciones.

Un tercer riesgo a considerar es el factor climático. Al ser un puerto y al encontrarnos en una zona sísmica, estamos expuestos a diferentes desastres naturales que requieren de un tratamiento adecuado a nivel de planes de contingencia, evacuación y cobertura.

¿Cuál es su comentario sobre el aporte de BASC Perú en el manejo de la gestión de riesgos al interior de su empresa?

(TRAMARSA): La Certificación BASC nos permite estandarizar procesos y controles mitigando riesgos en la cadena logística del comercio exterior.

(SECURITAS): En la amplia diversidad de iniciativas y herramientas existentes para la gestión de Riesgos, el contar con una norma tan completa como guía y que, al

(VIRÚ): The issues we consider as priority and critical risks that are being controlled by the company are:

Cargo contamination: Virú continuously and permanently monitors security controls throughout the supply chain. It starts with the identification and control of critical positions and suppliers; satellite control to the transport units ensuring that they comply with the requirements of our integrated security management system.

Money Laundering: We evaluate all our suppliers and clients with the maximum-security criteria (tracking, background, Clinton list) ensuring custody, as well as mitigating and minimizing the risk that the company is used for illicit activities.

Computer system damage: Permanent verification in Information Security, with equipment back-ups, access and security control for critical information, use of information tracking of critical personnel and external unexpected audits.

All these processes are audited through the supply chain traceability in an unexpected way, this can be at any time and form, scheduled quarterly and evaluating the effectiveness of the integrated security system implemented, which is empowered with the participation of senior management, thus providing continuous and permanent supervision.

(TISUR): One of the main risks of our activity is related to operational security in terms of cargo handling. Regarding to this, it is vital to have reliable and honest personnel identified with the company and aware of the importance of applying the established controls and procedures to minimize the probability of any occurrence.

The second risk is related to the importance of maintaining good relations in the work environment, both internal and external, avoiding any situation that leads to a conflict scenario that may impact operations.

A third risk to consider is the environmental factor. Being a port and being in a seismic zone, we are exposed to different natural disasters that require the adequate treatment in terms of contingency plans, evacuation and coverage.

What is your comment on the contribution of BASC Peru in the handling of risk management within your company?

(TRAMARSA): BASC Certification allows us to standardize processes and controls mitigating risks in the foreign trade supply chain.

(SECURITAS): In the wide diversity of existing initiatives and tools for risk management, having a standard as complete as a guide and, at the same time, a common reference for the large number of companies involved in international trade, is priceless.

In addition, BASC Peru's participation in the development of our organization through its various

mismo tiempo, constituye una referencia común para el amplio número de empresas involucradas en el comercio internacional, resulta de un valor incalculable.

Adicionalmente, la participación de BASC Perú dentro del desarrollo de nuestra organización por sus diversos canales, nos ha permitido, no solo ampliar nuestros conocimientos sobre los aspectos técnicos más relevantes de la seguridad en el comercio internacional, sino también entender mejor las necesidades y expectativas de nuestros clientes, así como beneficiar a clientes fuera de la cadena de comercio internacional al generalizar muchas de estas buenas prácticas en todas nuestras operaciones.

(VIRÚ): BASC es nuestro socio estratégicos y nos viene acompañado en el crecimiento organizacional liderando el sector agroexportador, para ello, dentro de sus objetivos estratégicos está priorizar el control de riesgos de la cadena de suministro de manera que la certificación anual sea una consecuencia y proceso natural de nuestra gestión.

(TISUR): Los estándares BASC aportan a la organización la mejora en el control de las operaciones, de la información, del personal y de las empresas asociadas a nuestra operatividad. Así como tomar acciones anticipadas y tener personal capacitado para responder ante cualquier contingencia

¿Qué planes tiene en su agenda del presente año para avanzar en la prevención y mitigación de riesgos en el campo de seguridad de la cadena de suministro de su empresa?

(TRAMARSA): Básicamente , reforzar nuestros controles a fin de mitigar al máximo los riesgos que se presentan en el despliegue de nuestras operaciones tanto dentro del terminal de almacenamiento como durante el transporte de mercancías de nuestros clientes.

(SECURITAS): Dentro del marco de nuestra nueva visión corporativa para el año 2020, la gestión del riesgo se extiende más allá de nuestras prácticas habituales, tanto dentro como fuera de nuestra organización, con un enfoque predictivo.

Al interno, la gestión de los riesgos corporativos será reforzada con un equipo especializado multidisciplinario, cuya función será extender el cumplimiento de las políticas de seguridad hasta la más pequeña actividad de los procesos críticos asociándolas a indicadores clave, así como reforzar el compromiso de la seguridad en cada miembro de la organización desde su ingreso.

Al externo, en primer lugar, se estarán implementando modelos de gestión de proveedores más participativos, reforzando las buenas prácticas en gestión del riesgo, así como estableciendo controles más detallados; posteriormente, el enfoque predictivo se insertará en nuestros servicios, basados en un sólido Análisis y Evaluación de los Riesgos, hasta el lograr un Servicio de Protección personalizado a las necesidades de nuestros clientes.

channels has allowed us not only to expand our knowledge of the most relevant technical aspects of security in international trade, but also to better understand the needs and expectations of our clients, as well as to benefit clients outside the international trade chain by wide spreading many of these good practices in all our operations.

(VIRÚ): BASC is our strategic partner and is with us in the organizational growth, leading the agro-export sector, for it, within its strategic objectives is to prioritize the control of risks in the supply chain so that the annual certification is a consequence and natural process of our management.

(TISUR): BASC standards provide the organization with improved control of operations, information, personnel and companies associated with our operations. As well as taking anticipated actions and having personnel trained to respond to any contingency.

What plans do you have in this year's agenda to progress in the prevention and mitigation of risks in the security field of your company's supply chain?

(TRAMARSA): Basically, to reinforce our controls in order to completely mitigate the risks that arise in the development of our operations both inside the storage terminal and during the transport of our clients' goods.

(SECURITAS): Within the framework of our new corporate vision for the year 2020, risk management extends beyond our usual practices, both inside and outside our organization, with a predictive approach.

Internally, corporate risk management will be reinforced with a specialized multidisciplinary team whose role will be to extend compliance with security policies down to the smallest activity of critical processes by associating them with key indicators as well as reinforcing the security commitment in each member of the organization since its entry.

Externally, first, more participatory supplier management models will be implemented, reinforcing good practices in risk management, as well as setting up more detailed controls; subsequently, the predictive approach will be inserted in our services, based on a solid Risk Analysis and Assessment, until achieving a Protection Service customized to our clients' needs.

(VIRÚ): Virú plans to continue with the effectiveness verification of the internal Security Agreements and involving the suppliers in the system, specialized trainings in supply chain security for critical personnel, security audits of second party to our stakeholders, as well as continue with

(VIRÚ): Virú tiene planificado continuar con la verificación de la eficacia de los Acuerdos de Seguridad al interno y con los proveedores involucrándolos cada día más en el sistema, capacitaciones especializadas en la seguridad de la cadena de suministro al personal crítico, auditorías de seguridad de segunda parte a nuestros stakeholders, así como continuar con las mejoras al interior de la organización, es parte de nuestra cultura y política.

(TISUR): Inversión en tecnología que soporta el control de las operaciones en tiempo real mejorando nuestro sistema de Circuito Cerrado de Televisión (CCTV).

Planes de capacitación y sensibilización continuo al personal según el nivel de especialización requerido.

La consultora EY (Ernst & Young) reveló en el 2015 que en el Perú el 70% de los directores de empresas tienen en agenda la gestión del riesgo, pero que solo el 9% tienen un comité del riesgo que se encarga de evaluar esta gestión. ¿Cuál es la situación de su empresa en este aspecto?

(TRAMARSA): Tenemos un Comité de Auditoría donde se evalúan y gestionan los principales riesgos según su materialidad. Asimismo, recientemente se ha creado la Gerencia de Sistemas Integrados de Gestión que tiene como misión, optimizar los procesos internos y minimizar el riesgo.

(SECURITAS): El grado de compromiso alcanzado dentro de nuestra organización nos ha llevado involucrar en esta gestión a colaboradores del más alto nivel. En este contexto, las funciones del Comité de Gestión del Riesgo son ejecutadas por los Directores y cuatro gerencias estratégicas que se reúnen con una alta frecuencia para la revisión de los puntos más críticos de nuestro SGCS y periódicamente para la revisión general del mismo; todo esto con el soporte de nuestras áreas administrativas y el SOC (SECURITAS OPERATION CENTER).

(VIRÚ): Tenemos como prioridad número uno el control efectivo del Sistema de Seguridad en la Cadena de Suministro para disminuir y mitigar los riesgos inherentes al negocio. Por ello contamos con un Comité de Seguridad y Control del Riesgo que evalúa permanentemente el desempeño del Sistema BASC en nuestra empresa.

Este Comité está liderado y empoderado por la Gerencia General y representado por el Gerente de RRHH quien la convoca mensualmente, en cual evaluamos y hacemos seguimiento minuciosos a los controles implementados y se proponen mejoras al sistema, además de la trazabilidad trimestral mencionada en la que evaluamos en forma integral el sistema en toda la empresa, tanto interna como externamente.

(TISUR): TISUR cuenta con un Comité del Riesgo que evalúa de forma periódica la gestión del riesgo de la empresa a nivel de directorio. Dicho comité recibe la información del tratamiento de estos riesgos mediante los canales independientes de auditoría.

improvements within the organization. It is part of our culture and policy.

(TISUR): Investment in technology that supports the control of operations in real time improving our Closed Circuit Television (CCTV) system.

Continuous training and awareness plans for staff according to the level of specialization required.

La consultora EY (Ernst & Young) reveló en el 2015 que en el Perú el 70% de los directores de empresas tienen en agenda la gestión del riesgo, pero que solo el 9% tienen un comité del riesgo que se encarga de evaluar esta gestión. ¿Cuál es la situación de su empresa en este aspecto?

(TRAMARSA): We have an Audit Committee where the main risks are evaluated and managed according to their nature. Also, the Integrated Management Systems Administration was recently created, whose mission is to optimize internal processes and minimize risk.

(SECURITAS): The degree of commitment reached within our organization has led us to involve collaborators of the highest level in this management. In this context, the functions of the Risk Management Committee are carried out by the Directors and four strategic managers who meet with high frequency for the review of the most critical points of our SGCS and meet periodically for a general review of the same; all this with the support of our administrative areas and the SOC (SECURITAS OPERATION CENTER).

(VIRÚ): We have as the number one priority the effective control of the Supply Chain Security System to reduce and mitigate the inherent risks of the business. That is why we have a on Security and Risk Control Committee that permanently evaluates the performance of the BASC System in our company.

This Committee is led and empowered by the General Management and represented by the HR Manager who convenes monthly. In it, we evaluate and closely monitor the implemented controls and propose improvements to the system, in addition to the aforementioned quarterly traceability in which we evaluate the system in the whole company, both internally and externally.

(TISUR): TISUR has a Risk Committee that periodically evaluates the risk management of the company at the board level. This committee receives information on the management of these risks through independent audit channels.

Situación de la gestión de riesgos en el Perú

RISK MANAGEMENT SITUATION IN PERU

La consultora EY (Ernst & Young) lanzó a finales de 2015 su publicación "Sin riesgo no hay recompensa – Encuesta sobre Gobierno, Riesgo y Cumplimiento 2015" documento basado en una encuesta a cerca de 1,200 empresas a nivel mundial, incluyendo a 33 empresas en el Perú.

Sus resultados para la situación peruana mostraron que el 45% de empresas identifican, evalúan y desarrollan planes para gestionar el riesgo; mientras que un 24% los identifican y solo un 21% discuten los riesgos.

Asimismo, el 70% de los directores de empresas peruanas consideran como parte de su agenda la evaluación de riesgos, pero solo el 9% de las empresas cuentan con un Comité de Riesgo.

En relación al uso de herramientas tecnológicas de la gestión del riesgo para facilitar respuestas rápidas, el informe encontró que en el 64% de gerencias de alto nivel consultadas no utiliza tecnologías del riesgo y solo un 18% cuenta con múltiples tecnologías y cumplimiento para la organización.

At the end of 2015, EY (Ernst & Young) launched the publication "No Risk No Reward – 2015 Government, Risk and Compliance Survey", document based on a survey of nearly 1,200 companies worldwide, including 33 companies in Peru.

The results for Peru showed that 45% of companies identify, evaluate and develop plans to manage risks, while 24% identify them and only 21% discuss the risks.

Likewise, 70% of Peruvian company managers consider risk assessment as part of their agenda, but only 9% of companies have a Risk Committee.

Regarding the use of technological tools of risk management to facilitate rapid responses, the report found that 64% of high-level managers consulted do not use risk technologies and only 18% have multiple technologies and compliance for the organization.

Según el Foro Económico Mundial

Los riesgos globales en el 2017

ACCORDING TO THE WORLD ECONOMIC FORUM

GLOBAL RISKS IN 2017

El Foro Económico Mundial – FEM (World Economic Forum), conocido también como Foro de Davos, elabora desde hace 12 años su documento 'Informe de Riesgos Globales' en el que evalúa los riesgos que se consideran de potenciales efectos globales para las industrias y que pueden causar daños económicos por más de US$10 000 millones y además provocar gran sufrimiento humano por lo que requieren un enfoque multidisciplinario para poder prevenir y ser mitigado.

El FEM es una fundación mundial sin fines de lucro con sede en Ginebra, Suiza, y reúne en su asamblea anual a los principales líderes empresariales, políticos, académicos e intelectuales y personalidades con reconocimiento mundial para analizar los problemas más apremiantes que afronta el mundo.

En su más reciente documento "Informe de Riesgos Globales 2017" el Foro Económico Mundial evalúa 30 riesgos globales, así como 13 tendencias subyacentes que podrían agravarlos o alterar las interconexiones entre ellos, los cuales se basan en encuestas y entrevistas a 750 expertos en todo el mundo.

De todos los riesgos globales analizados, los analistas consideran a cinco principales aquellos que se consignan en los cuadros respectivos del presente artículo. En estos cuadros se pueden diferenciar dos tipos de riesgos: probables e impactantes, así como su importancia actual comparado con el de hace 10 años.

De modo general, la desigualdad económica, la polarización social y los crecientes peligros

The World Economic Forum (WEF), also known as the Davos Forum, has been developing its Global Risk Report document for 12 years, assessing the risks that are considered to have global effects on industries and can cause economic damage for more than US $ 10 billion and also cause great human suffering and it requires a multidisciplinary approach to prevent and be mitigated.

The WEF is a global non-profit foundation based in Geneva, Switzerland, and brings together at its annual assembly top business leaders, politicians, academics, intellectuals and public figures with global recognition to analyze the most pressing problems the world faces.

In its most recent "Global Risk Report 2017" the World Economic Forum assesses 30 global risks as well as 13 underlying trends that could aggravate them or alter interconnections between them, which are based on surveys and interviews with 750 experts across the globe.

Of all the global risks analyzed, the analysts consider five main ones that are listed in the charts of this article. In these charts two types of risks can be distinguished: probable and shocking, as well as their current importance compared to that of 10 years ago.

Overall, economic inequality, social polarization and increasing environmental

medioambientales son las tres principales tendencias de riesgos que determinarán los avances globales en los próximos 10 años, según el documento. Con una creciente desafección política y la disrupción global como telón de fondo, el informe pone de manifiesto tres conclusiones claves:

1. **Los patrones persisten.** La desigualdad económica y de la distribución de la riqueza, y la creciente polarización de las sociedades, ocupan el primer y tercer lugar respectivamente entre las tendencias subyacentes que determinarán los avances globales en los próximos diez años. Asimismo, los riesgos más interconectados son el elevado nivel desempleo estructural (subempleo) y una profunda inestabilidad social.
2. **El medio ambiente domina el panorama** de riesgos globales. El cambio climático ha sido la tendencia subyacente número dos este año. Y por primera vez, los cinco riesgos medioambientales de la encuesta se han clasificado como de alto riesgo y de alta probabilidad, con los fenómenos meteorológicos extremos emergiendo como principal riesgo global.
3. **La sociedad no sigue el ritmo del cambio tecnológico**. De las 12 tecnologías emergentes analizadas en el informe, los expertos han detectado que la inteligencia artificial y la robótica tienen el mayor potencial para ofrecer beneficios, pero también para provocar efectos negativos, por lo que se hace imprescindible una mejor regulación al respecto.

5 riesgos top en términos de probabilidad
Top 5 Global Risks in Terms of Likelihood

	2007	2017
1	Averías de infraestructura de información critica Breakdown of critical information Infrastructure	Eventos climáticos extremos Extreme weather Events
2	Enfermedades crónicas en países desarrollados Chronic disease in developed countries	Involuntaria migración a gran escala Large-scale involuntary migration
3	Impacto del precio del petróleo Oil price shock	Grandes desastres naturales Major natural disasters
4	Fuerte aterrizaje de la economía china China economic hard landing	Ataques terroristas a gran escala Large-scale terrorist attacks
5	Colapso del precio de activos Asset price collapse	Incidentes masivos de robo y fraude de datos Massive incident of data fraud/theft

Fuente: "Informe de Riesgos Globales 2017", Foro Económico Mundial.

En el caso específico de Latinoamérica, los principales riesgos para los negocios en 2017 y en adelante, siguen la tendencia de años anteriores, si bien el impacto del precio de la energía baja algunas posiciones, quedando de la siguiente manera:

1- Fallos en la gobernabilidad
2- Alto índice de desempleo
3- Crisis fiscales
4- Inestabilidad social
5- Impacto de los precios de la energía

Con la finalidad de evitar fracturas sociales el documento sugiere poner en agenda reformar el capitalismo de mercado, más aun luego de las sorpresas

hazards are the three major risk trends that will determine global progress over the next 10 years, according to the document. With increasing political disaffection and global disruption as a backdrop, the report highlights three key findings:

1. Patterns persist. Economic inequality and wealth distribution, and the increasing polarization of societies, rank first and third respectively among the underlying trends that will determine global progress over the next ten years. Also, the most interconnected risks are the high level of structural unemployment (underemployment) and deep social instability.
2. The environment dominates the global risk landscape. Climate change has been the number two underlying trend this year. And for the first time, the five environmental risks of the survey have been classified as high risk and high probability, with extreme weather phenomena emerging as the main global risk.
3. Society does not keep pace with technological change. Of the 12 emerging technologies analyzed in the report, experts have found that artificial intelligence and robotics have the greatest potential to offer benefits, but also to cause negative effects, which makes it necessary to better regulate them.

In the specific case of Latin America, the main risks for business in 2017 and beyond, follow the trend of previous years, although the impact of energy prices drops some positions, being as follows:

1- Failures in governance
2- High unemployment rate
3- Fiscal Crises
4- Social Instability
5- Impact of energy prices

In order to avoid social fractures, the document suggests reforming market capitalism, especially after the electoral surprises of 2016 and the rise of previously minority parties that prioritize national sovereignty and traditional values (Europe, the United States).

electorales de 2016 y el ascenso de partidos anteriormente considerados como minoritarios que priorizan la soberanía nacional y los valores tradicionales (Europa, Estados Unidos).

La creciente polarización y los sentimientos nacionalistas en auge se cuentan entre los principales riesgos. De ahí el siguiente reto: abordar la importancia de la identidad y la comunidad. Los cismas culturales resultantes están poniendo a prueba la cohesión social y política, y podrían ahondar muchos otros riesgos si no se abordan.

Pese a que las corrientes políticas anti establecidos tienden a culpar a la globalización del deterioro de las perspectivas laborales a nivel nacional, algunos indicios sugieren que la gestión del cambio tecnológico es un reto aún más importante para los mercados laborales.

Si bien históricamente la innovación ha creado nuevos tipos de trabajos además de destruir aquellos que han quedado obsoletos, este proceso podría estar ralentizándose. No es casualidad que las amenazas a la cohesión social y el cuestionamiento de la legitimidad de la clase política coincidan con una fase altamente disruptiva de cambio tecnológico.

Gestionar la Cuarta Revolución Industrial

La última parte del Informe explora la relación entre los riesgos globales y las tecnologías emergentes de la Cuarta Revolución Industrial. Nos enfrentamos a un apremiante problema de gestión si hemos de crear las reglas, normas, estándares, incentivos, instituciones y otros mecanismos necesarios para definir el desarrollo e implementación de dichas tecnologías.

Cómo manejar las nuevas tecnologías es una cuestión compleja: una regulación demasiado estricta y a la carrera puede frenar el progreso, pero la falta de regulación adecuada puede agravar los riesgos y crear incertidumbres que ahuyenten a potenciales inversores e innovadores.

Actualmente, la regulación de las tecnologías emergentes es irregular: algunas están altamente reguladas mientras que otras no lo están en absoluto ya que no dependen de ningún órgano regulador.

El Informe valora los riesgos asociados con la forma en que la tecnología está redefiniendo las infraestructuras físicas: una mayor interdependencia entre distintas redes de infraestructuras está aumentando el alcance de posibles fallos sistémicos (ya sea a causa de ciberataques, fallos técnicos de software, desastres naturales u otras causas) en cascada entre redes, algo que afectaría a la sociedad entera de forma imprevisible.

5 riesgos top en términos de impacto
Top 5 Global Risks in Terms of Impact

	2007	2017
1	Colapso del precio de activos Asset Price collapse	Armas de destrucción masiva Weapons of mass destruction
2	Restricción de la globalización Retrenchment from globalization	Eventos climáticos extremos Extreme weather events
3	Guerras civiles y entre estados Interstate and civil wars	Crisis del agua Water crises
4	Pandemias Pandemics	Serios desastres naturales Major natural disasters
5	Impacto del precio del petróleo Oil price shock	Fracaso en la mitigación y adaptación del cambio climático Failure of climate change mitigation and adaptation

Fuente: "Informe de Riesgos Globales 2017", Foro Económico Mundial.

Rising polarization and rising nationalist sentiments are among the main risks. Hence the following challenge: to address the importance of identity and community. The resulting cultural schisms are testing social and political cohesion, and could deepen many other risks if they are not addressed.

While anti-established political trends tend to blame globalization for the deteriorating labor prospects at the national level, some evidence suggests that managing technological change is an even greater challenge for labor markets.

While innovation has historically created new types of jobs as well as destroying those that have become obsolete, this process could be slowing down. It is no coincidence that the threats to social cohesion and the questioning of the political class legitimacy coincide with a highly disruptive phase of technological change.

Managing the Fourth Industrial Revolution

The last part of the Report explores the relationship between global risks and emerging technologies of the Fourth Industrial Revolution. We face a pressing management problem if we are to create the rules, norms, standards, incentives, institutions and other mechanisms necessary to define the development and implementation of these technologies.

Managing new technologies is a complex issue: overly strict regulation can slow down progress, but lack of adequate regulation can aggravate risks and create uncertainties that may discourage potential investors and innovators.

Currently, the regulation of emerging technologies is inconsistent: some are highly regulated while others are not regulated at all because they do not depend on any regulatory body.

The Report assesses the risks associated with how technology is redefining physical infrastructures: a greater interdependence between different infrastructure networks is increasing the scope of possible systemic failures (whether due to cyber attacks, technical software failures, natural disasters or other causes) between networks, something that would affect the whole society in an unforeseeable way.

Fuente / Source: World Economic Forum , "The Global Risks Report 2017
World Economic Forum, "The Global Risks Report 2017""

El avance del compliance

THE PROGRESS OF COMPLIANCE

El **Compliance** (sistema de cumplimiento) es una tendencia fuerte dentro del mundo legal y empresarial que ha dado origen a una nueva profesión (compliance officer). Sin embargo, aún existen numerosos profesionales que no conocen exactamente en qué consiste el compliance, y piensan que es algo que sólo puede interesar a las grandes empresas.

El Compliance nace en el mundo empresarial anglosajón, más concretamente en el sector financiero, que tradicionalmente ha estado sometido a una regulación bastante rigurosa. En las entidades financieras surge la necesidad de asegurarse el cumplimiento con toda la normativa, bastante compleja en ocasiones, y con sanciones muy altas en caso de incumplimiento, por lo que comienzan a emplear a departamentos dedicados en exclusiva a asegurar el cumplimiento, deslindándolos del área de asesoría legal que hasta entonces era la encargada de esa función.

Actualmente la regulación cada vez más profusa y exigente no se limita al sector financiero, sino que se extiende a otros sectores de la economía, que también empiezan a interesarse en implementar sus propios planes de compliance.

La llegada a otros países de este moderno concepto sigue una ruta más o menos común: En un comienzo, son las empresas con matrices situadas en el extranjero las que prestan atención a esta nueva figura por ser algo prácticamente intrínseco a su cultura corporativa. Otras empresas, nacionales pero con importantes conexiones internacionales, también deben implementarlo para proporcionar seguridad a sus socios extranjeros.

Según el desarrollo de este tema en cada país, el compliance ha sido objeto de legislación, llegando a normas que obligan a las empresas a adaptarse a unos estándares de cumplimiento. De ahí que existan empresas certificadoras en esta área. Sin embargo, estas empresas también requieren ser reglamentadas, tarea nada fácil. Ejemplo, en Chile existen 26 empresas

Compliance is a strong trend within the legal and business world that has given rise to a new profession: compliance officer. However, there are still many professionals who do not know exactly what compliance is, and they think it is something that can only interest large companies.

Compliance is born in the Anglo-Saxon business world, more specifically in the financial sector, which has traditionally been subject to fairly rigorous regulation. In financial institutions, there is a need to ensure compliance with all the regulations, which are quite complex at times, and with very high penalties in case of non-compliance, so that they begin to employ departments dedicated exclusively to ensuring compliance, removing them from the legal advice area, which was in charge of that function.

Currently, the increasingly profuse and demanding regulation is not limited to the financial sector, but extends to other sectors of the economy, which also begin to be interested in implementing their own compliance plans.

The arrival of this modern concept to other countries follows a more or less common route: in the beginning, the companies with headquarters located abroad are the ones who pay attention to this new figure because it is almost intrinsic to its corporate culture. Other national companies, but with important international connections, must also implement it to provide security to their foreign partners.

According to the development of this issue in each country, compliance has been the subject of legislation, reaching standards that force companies to adapt to compliance standards. Hence, there are certification companies in this area. However, these companies also need to be regulated, not an easy task. Example, in Chile there are 26 certification companies for compliance, but only 5 are active because there is no regulation that guarantees their activity. In Peru, the institution that oversees this system is the Superintendence of the Securities Market (SMV).

certificadoras en compliance, pero sólo 5 están activas por no haber reglamentación que dé garantía a su actividad. En Perú, la institución que supervisa este sistema es la Superintendencia del Mercado de Valores (SMV).

La legislación en el Perú relacionada al compliance ha iniciado una etapa de desarrollo por los recientes casos de corrupción en el caso Odebrecht. Con la finalidad de perseguir con eficacia a los responsables, en enero de 2017 el Gobierno publicó un decreto legislativo que amplía la responsabilidad administrativa de personas jurídicas; se amplió a más delitos tipificados en el Código Penal, delitos de lavado de activos y otros relacionados a minería ilegal y crimen organizado.

Con estos antecedentes, no solo más empresas grandes deberían encaminarse a contar con un área de compliance, puesto que una pequeña empresa, desde sus inicios, puede establecer qué cosas no se puede hacer y desarrollar este procedimiento junto a su crecimiento.

Implementación

El **compliance** o cumplimiento normativo consiste en establecer las políticas y los procedimientos pertinentes para garantizar que una empresa, incluidos sus directivos, empleados y agentes vinculados, cumplan con el marco normativo aplicable. Sin embargo, además del marco normativo deberían incluirse también las políticas internas, los compromisos con clientes, proveedores o terceros, y especialmente los códigos éticos que la empresa se comprometa a respetar. Esta función puede realizarse mediante cinco acciones:

1. **Identificación:** se han de identificar los riesgos a los que se enfrenta la empresa, teniendo en cuenta su severidad e impacto y la probabilidad de que se den.
2. **Prevención:** conociendo los riesgos, se debe diseñar e implementar procedimientos de control que protejan a la empresa.
3. **Monitorización y detección:** la efectividad de los controles implementados debe ser supervisada, informando a la dirección de la exposición de la empresa a los riesgos, y realizando las auditorías periódicas que sean precisas.
4. **Resolución:** cuando pese a todo surge algún problema de cumplimiento, debe trabajarse para su solución.
5. **Asesoramiento:** los directivos y trabajadores deben recibir toda la información necesaria para llevar a cabo su trabajo de acuerdo con la normativa vigente.

Tradicionalmente, y de modo general, estas funciones recaían en los departamentos de asesoría jurídica, pero debido a la mayor complejidad regulatoria han surgido personas que se especializan en esta función, ya sea desde dentro de la empresa como asesor in-house, o bien como parte de compañías especializadas en compliance.

A su vez, dentro del organigrama de la empresa, los encargados de compliance pueden trabajar de forma centralizada, diseñando y controlando las actividades de toda la organización; o de forma descentralizada, integrándose en las distintas áreas de la empresa de una forma más autónoma, sin perjuicio de que exista una persona supervisora a nivel general. CS

In Peru, legislation related to compliance has begun a development stage due to the recent cases of corruption in the Odebrecht case. In order to effectively prosecute those responsible, in January 2017 the Government issued a legislative decree that extends the administrative responsibility of legal persons; it was extended to more crimes classified in the Penal Code, money-laundering offenses and others related to illegal mining and organized crime.

With this background, not only more large companies should aim to have a compliance area, since a small company, from its inception, can establish what things can not be done and develop this procedure together with its growth.

Implementation

Compliance or regulatory compliance is to establish the relevant policies and procedures to ensure that a company, including its managers, employees and related agents, complies with the applicable regulatory framework. However, in addition to the regulatory framework, internal policies, commitments to clients, suppliers or third parties should also be included, especially the ethical codes that the company undertakes to respect. This function can be performed through five actions:

1. **Identification**: the risks faced by the company must be identified, taking into account their severity and impact and the likelihood of their occurrence.
2. **Prevention**: knowing the risks, it is necessary to design and implement control procedures that protect the company.
3. **Monitoring and detection**: the effectiveness of the implemented controls should be monitored, informing the management of the company's exposure to the risks, and carrying out periodic accurate audits.
4. **Resolution**: when in spite of everything there is a problem of compliance, you must work for its solution.
5. **Advising**: managers and workers must receive all the information necessary to carry out their work in accordance with current regulations.

Traditionally and generally, the legal advisory departments handled these functions, but because of the greater regulatory complexity, people who specialize in this function have emerged, either from within the company as an in-house advisor, or as part of companies specialized in compliance.

In turn, within the organization's organizational chart, compliance officers can work in a centralized way, designing and controlling the activities of the entire organization; or in a decentralized way, integrating in the different areas of the company in a more autonomous way, without preventing a supervisor at a general level. CS

Fuente / Source: Sánchez y Sánchez Abogados, España / El Comercio / Diario Gestión

El INSIDER. El peligro más cerca que nunca

THE INSIDER. DANGER CLOSER THAN EVER

Escribe / Write: Kalim Schiantarelli, Gerente General de CLOVER PRO.

Edimburgo, Escocia. Domingo, 6 de noviembre 2016. Entre fantasmas que recorren sus oscuros y estrechos callejones, en "Auld Reekie" o "Vieja Chimenea", como la suelen llamar sus amables ciudadanos, una historia más de misterio se va tejiendo en la capital. Miles de celulares vibran al recibir un mensaje de texto inesperado: "Ayer nuestro sistema de prevención de fraude identificó actividad sospechosa en un número de cuentas de nuestros clientes incluyendo la suya (…)" (*)

TESCO, el primer supermercado del Reino Unido, había enviado este mensaje a sus clientes, quienes detrás del reflejo de sus equipos móviles lucirían pálidos de preocupación y no era para menos. La noche anterior ciber-atacantes habían penetrado el sistema bancario de la compañía, succionando dinero de 20,000 cuentas de sus clientes. Los delincuentes robaron en total la gran suma de 2.5 millones de euros.

Hoy la investigación continúa y aunque TESCO señala que debe haber sido un ataque externo sofisticado, varios expertos en seguridad informática opinan que el caso tuvo que empezar desde el interior. Para acceder, pues, a 20,000 cuentas personales con nombres de usuarios y contraseñas se necesitaría una "llave" por dentro, alguien quien deje las "puertas del castillo" abiertas.

EL INSIDER: Persona que opera desde dentro de la empresa, puede ser un empleado o contratista, quien tiene llegada a los sistemas informáticos y accede a estos para delinquir solo o en modalidad de crimen organizado.

El Insider es un agente peligroso para la empresa; opera desde la confianza que se le brinda y los daños que ocasiona son contundentes y –a menudo- irreparables. Este insidioso actor puede manipular, contaminar y hasta destruir sus sistemas. Este "enemigo interno" está al acecho de los "secretos, planes estratégicos, cuentas,

Edinburgh, Scotland. Sunday, November 6, 2016. Between ghosts that run through their dark, narrow alleys, in "Auld Reekie" or "Old Chimney", as it is usually called by their friendly citizens, another mysterious story is developing in the capital. Thousands of cellphones vibrate when receiving an unexpected text message: "Yesterday our fraud prevention system identified suspicious activity on a number of accounts of our clients including your own (…)" (*)

TESCO, the UK's first supermarket, had sent this message to its customers, who, behind their reflection on their mobile equipment, would look pale with concern and with good reason. The previous night cyber-attackers had penetrated the company's banking system, sucking money from 20,000 accounts of its customers. The criminals stole in total the large sum of 2.5 million euros.

Today the investigation continues and although TESCO points out that it must have been a sophisticated external attack, several computer security experts say the case had to start from the inside. To access 20,000 personal accounts with usernames and passwords would require a "key" from de inside, someone who leaves the "castle doors" open.

THE INSIDER: Person operating from within the company; can be an employee or contractor who has access to computer systems and accesses these to commit crimes alone or as part of organized crime.

The Insider is a dangerous agent for the company; operates from the trust he is given and the damages he causes are severe and often irreparable. This insidious character can manipulate, contaminate and even destroy your systems. This "internal enemy" is on the lookout for "your company's secrets, strategic plans, accounts,

finanzas, datos bancarios" de su empresa y más, dice Andrés Velázquez- Presidente de la empresa especializada en seguridad digital MATTICA. Así mismo, informa que en general 80% de los fraudes se originan desde el interior, un dato esclarecedor (MATTICA.COM.)

¿Sabía usted que en Perú el 90% de las empresas considera que los ataques tienen más probabilidad de ser perpetrados por los mismos empleados? Esto es lo que reveló precisamente una encuesta mundial sobre seguridad del 2014 de la renombrada Ernest and Young (Diario Gestión). Lo que es alarmante también es que empresarios notaron que la cantidad de amenazas en 2016 se incrementó, mientras que sus capacidades de detectar los ataques –admiten- son muy bajas.

¿Qué acciones puede tomar para combatir el riesgo de ser víctimas del Insider?

- Realice procesos estrictos a la hora de la contratación, reforzando revisión de background, crédito y contactando referencias.
- Implemente políticas de seguridad, asegurando que sus empleados las lean, firmen y estén informados sobre las fuertes consecuencias de actuar en contra de estas.
- Esté atento a los cambios de conducta y hábitos de trabajo de sus empleados.
- Minimice el acceso a la información según rangos de responsabilidad.
- Disminuya la rotación de empleados.
- Tenga cuidado con el uso de celulares, USBs y correo electrónico; son las herramientas para el robo de la información.
- Integre sistemas de seguridad y control en los canales de comunicación que se manejan.
- Efectúe software de detección temprana de actividad sospechosa y manténgalo actualizado.

Lo que NO DEBE hacer en caso de hallar sus sistemas vulnerados:

1. Apagar las computadoras
2. Encender un equipo apagado
3. Ejecutar cualquier aplicación
4. Realizar búsquedas
5. Desconectar dispositivos de almacenamiento
6. Abrir archivos

Adicionalmente, contacte a un especialista en cómputo forense para que maneje la escena. De esta manera evitará contaminar o perder la evidencia necesaria para hallar poder defenderse dentro de esta delicada situación. El peligro está más cerca que nunca y cada vez se siente más el calor de posibles futuros ataques, como aquel día en la "Vieja Chimenea". Que no sea usted quien tenga que enviar el siguiente mensaje. Cuidado con el INSIDER. CS

finances, bank details" and more, says Andrés Velázquez - President of the company specialized in digital security MATTICA. Likewise, he informs that in general 80% of the frauds originate from the interior, an eye-opening fact (MATTICA.COM.).

Did you know that in Peru 90% of companies consider that the attacks are more likely to be perpetrated by their own employees? This is precisely what a global security survey of the renowned Ernest and Young revealed in 2014 (Diario Gestión). What is also alarming is that businessmen noticed that the number of threats increased in 2016, while their capabilities to detect the attacks are very low, they admit.

What actions can you take to reduce the risk of falling victim to the Insider?

- Perform strict processes when hiring, reinforcing background check, credit review and contacting personal referrals.
- Implement security policies, ensuring that your employees read and sign them and be informed about the severe consequences of acting against them.
- Be aware of behavioral changes and work habits of your employees.
- Minimize access to information according to ranges of responsibility.
- Reduce employee rotation.
- Be aware of the use of cell phones, USBs and email; these are the tools for information theft.
- Integrate security and control systems into the communication channels in use.
- Run early detection software for suspicious activity and keep it updated.

What you should NOT do if you find your systems compromised:

1. Shut down the computers
2. Turn on equipment that is off
3. Execute any application
4. Conduct searches
5. Disconnect storage devices
6. Open files

Additionally, contact a computer forensics specialist to handle the scene. In this way you will avoid contaminating or losing the necessary evidence to be able to defend yourself in this delicate situation. Danger is closer than ever and the heat of possible future attacks is felt more and more, like that day in the "Old Chimney". Do not let yourself be the one who has to send the next message. Beware of the INSIDER. CS

(*) http://www.telegraph.co.uk/business/2016/11/07/ tesco-bank-to-free-ze-customer-transactions-after- hacking-attack/

Encuestas revelan una realidad poco esperada

Las interrupciones en la cadena de suministro

SURVEYS REVEAL AN UNEXPECTED REALITY

DISRUPTIONS AND RISK MANAGEMENT IN THE SUPPLY CHAIN

Operar bajo el principio “esperar lo inesperado” es la mejor defensa contra la interrupción de la cadena de suministro, y puede evitar grandes pérdidas y disfrutar de una ventaja competitiva en los exigentes mercados. Sin embargo, las empresas no lo llevan a la práctica.

Operating under the “expect the unexpected” principle is the best defense against supply chain disruption, and you can avoid big losses and enjoy a competitive edge in demanding markets. However, companies do not put it into practice.

A inicios de 2016 la empresa DHL divulgó el informe “Insight On: Risk and Resilience” (Percepción: Riesgo y Resiliencia) sobre la gestión del riesgo y de la resiliencia en la cadena de suministro. El estudio encontró que el riesgo en las cadenas de suministro ha sido la consecuencia no deseada de las dos principales tendencias más importantes de las últimas décadas: la globalización y la producción ajustada.

Muchas interrupciones y mucho dinero perdido

El documento revela que el 74% de las empresas encuestadas sufrió interrupciones en su cadena de suministro durante el 2015 debido a varios acontecimientos sucedidos, tales como el conflicto en Oriente Medio, el incendio en el puerto de Tianjin, las huelgas en los puertos de Estados Unidos.

También revela que en el periodo 2000 – 2010 las pérdidas causadas por la ruptura de la cadena de suministro ascendieron a una media de 115.000 millones de dólares al año, aumentando a 380.000 millones de dólares en el 2011. Se estima que el costo en el 2015 sea mayor, ya que sólo el retraso en los puertos estadounidenses costó a los minoritas de ese país 7.000 millones de dólares.

“La economía moderna opera con cadenas de suministro globales interconectadas, pero la distancia y la complejidad vienen acompañadas de nuevos riesgos, como desastres naturales o provocados por el hombre, el cambio climático y los factores socio-políticos y económicos de la guerra, huelgas y delincuencia”, señala el documento.

El informe concluye diciendo que hay demasiadas empresas que siguen centradas en la eficiencia y en la reducción de costos, haciendo caso omiso a los riesgos inherentes de este tipo de enfoque. Por ejemplo, muchas empresas de varios sectores mantienen inventarios y existencias de reserva bajo mínimos con el objetivo de reducir gastos generales. Todo ello, a pesar de que la más mínima interrupción de la cadena de suministro,

In early 2016, DHL released the “Insight On: Risk and Resilience” report on risk management and supply chain resilience. The study found that supply chain risk has been the undesired consequence of the two most important major trends of recent decades: globalization and lean manufacturing.

Many disruptions and lots of lost money

The document reveals that 74% of the companies surveyed suffered disruptions in their supply chain during 2015 due to several events, such as the conflict in the Middle East, the fire in the port of Tianjin, strikes in US ports.

It also reveals that in the 2000-2010 period, the losses caused by supply chain disruption amounted to an average of 115 billion dollars a year, increasing to 380 billion dollars in 2011. It is estimated that the cost in 2015 will be greater, since only the delay in the US ports cost 7 billion dollars to the retailers of that country.

“The modern economy operates with interconnected global supply chains, but distance and complexity are accompanied by new risks, such as natural or man-made disasters, climate change and socio-political and economic factors of war, strikes and crime”, the document states.

The report concludes that too many companies remain focused on efficiency and cost reduction, ignoring the inherent risks of such an approach. For example, many companies in various industries maintain inventories and reserve stocks under minimums in order to reduce overheads. All this, despite the fact that the slightest disruption of the supply chain, such as a fire in a single component

como un incendio en una sola fábrica de componentes, podría llevar a la paralización de la producción mundial.

Una cadena de suministro flexible, sin embargo, podría mantener con seguridad hasta un 14% menos de reservas de mercancía y continuar, aún así, bajo cualquier circunstancia. Asimismo, los problemas de calidad son los más difíciles de detectar en la cadena de suministro y los más rápidos en derivar a un riesgo para la reputación. El rápido crecimiento de la comunicación digital y la naturaleza cada vez más interconectada de las empresas, productos y cadenas de suministro también están aumentando los riesgos cibernéticos.

Las soluciones para aumentar la resiliencia pasan por tener un enfoque de los costos totales; la visibilidad en tiempo real de los datos; ideas para predecir futuros cambios; y la colaboración, incluyendo a los clientes.

Muchas cadenas de suministro globales complejas carecen de transparencia; las empresas no saben dónde se encuentran los riesgos, o la forma de gestionarlos y mitigarlos. Según el informe, la visibilidad en toda la cadena es de vital importancia para que las empresas entiendan su exposición crítica y sean capaces de actuar con rapidez en caso de crisis. Como resultado, DHL ha desarrollado 'Resilience360', una herramienta de plataforma basada en la nube con tres pilares, que pueden responder a los incidentes y gestionar la continuidad del negocio.

Las empresas no gestionan sus riesgos…

En Noviembre de 2014 la transnacional logística UPS y el Instituto de Cadena de Suministro Global de la Universidad de Tenessee publicaron el estudio "Gestión del riesgo en la cadena de suministro global" (Managing Risk in the global supply chain) el cual se basó en una encuesta realizada a 150 compañías líderes.

El estudio concluyó, entre otras, que los responsables de la cadena de suministro de todos los sectores son cada vez más conscientes de los riesgos a los que estas se enfrentan y sus temidas consecuencias, pero no obstante, "muchos de ellos aún no desarrollan ni ejecutan estrategias para gestionar adecuadamente estos peligros". Otra de los resultados del estudio fue que "el 90% de las empresas no cuantifican formalmente los riesgos de la cadena de suministro cuando subcontratan la producción".

Asimismo, ninguno de los participantes en el estudio utilizaba su experiencia para evaluar los riesgos de la cadena de suministro, lo que "sorprende la falta de estrategias para minimizar el riesgo" señalaba el documento.

La cadena de suministro es un área de las compañías en la que sus responsables se enfrentan a la eficiencia operacional sin tener un control directo de muchas de las fases, por tanto, las estrategias que reduzcan el riesgo resultan esenciales en las operaciones. Así pues, cualquier negocio que no disponga de algún plan para aminorar el riesgo, está jugando con la supervivencia de su empresa.

Otras conclusiones relevantes fueron que la mayoría de las compañías encuestadas disponen de responsables del riesgo en algún lugar de la compañía, habitualmente dentro de los departamentos legales y financieros. Sin embargo, la mayoría de ellos no están alineados con los riesgos de la cadena de suministro, lo que da lugar a fallos significativos en las estrategias globales de mitigación del riesgo de las compañías.

factory, could lead to stoppage of world production.

A flexible supply chain, however, could safely maintain up to 14% less merchandise reserves and continue under any circumstances. Also, quality problems are the most difficult to detect in the supply chain and the fastest to derive a reputation risk. The rapid growth of digital communication and the increasingly interconnected nature of businesses increase the products and supply chains cyber risk.

Solutions to increase resilience should have a total cost approach, real-time data availability, ideas for predicting future changes and collaboration, including customers.

Many complex global supply chains lack transparency; companies do not know where the risks are, or how to manage and mitigate them. According to the report, visibility throughout the chain is vital for companies to understand their critical exposure and be able to act quickly in case of crisis. As a result, DHL has developed 'Resilience360', a three-pillar, cloud-based platform tool that can respond to incidents and manage business continuity.

Companies do not manage their risks…

In November 2014, the transnational company UPS and the Global Supply Chain Institute of the University of Tennessee published the "Risk Management in the Global Supply Chain" study, which was based on a survey performed on 150 leading companies.

The study concluded that supply chain managers in all sectors are increasingly aware of the risks they face and their feared consequences, but nonetheless, "many of them do not yet Implement strategies to properly manage these hazards". Another conclusion of the study was that "90% of companies do not formally quantify supply chain risks when they outsource production."

Likewise, none of the study participants used their experience to assess supply chain risks. "The lack of strategies to minimize risk is surprising", the document stated.

The supply chain is a company area in which the managers face operational efficiency without having direct control of many of the stages; therefore, the strategies that reduce risk are essential in the operations. Thus, the company that does not have a plan to mitigate the risk is playing with its own survival.

Other relevant findings were that most of the companies surveyed have risk managers somewhere in the company, usually within the legal and financial departments. However, most of them are not aligned with supply chain risks, leading to significant failures in the companies' global risk mitigation strategies.

Fuente/ Source: DHL, "InsightOn: Riesgo y Resiliencia" 2016 / UPS, "Managing Risk in the global supply chain" 2014

BASC permite tener procesos ordenados y orientados al aseguramiento del comercio internacional

BASC ALLOWS FOR ORGANIZED PROCESSES ORIENTED TOWARDS FOREIGN TRADE ASSURANCE

Para Eduardo Freundt Delta, gerente comercial de ISCO, la certificación BASC ayudó a su empresa lograr ser un Operador Económico Autorizado (OEA) reconocido ante la SUNAT, gracias a que sus empleados trabajan siguiendo los requisitos establecidos por BASC.

For Eduardo Freundt Delta, commercial manager at ISCO, BASC certification helped his company to be recognized as an Authorized Economic Operator (AEO) by SUNAT thanks to the work his employees do, following the requirements established by BASC.

Haga una breve reseña de su empresa. Describa los servicios que ISCO ofrece.

Interamerican Service Co S.A.C. se crea en el año 1947 como agencia de aduana, hoy como grupo logístico, ofrecemos Agenciamiento de Aduanas, Transporte, Almacenaje y Distribución, manteniendo siempre la misma vocación de servicio hacia los importadores y exportadores.

Mediante un equipo humano especializado y un proceso eficiente y seguro, ISCO ofrece un servicio integral en toda la cadena logística. Nuestro servicio comprende desde el Seguimiento Pre-Embarque, Transporte Internacional, Agenciamiento de Aduanas, Transporte Local y Nacional mediante distribución. Todo ello adaptando nuestras operaciones o los requerimientos de nuestros clientes.

¿Cuáles son las buenas prácticas de seguridad que ha implementado por ser asociado BASC?

La aplicación de la certificación BASC nos ha permitido identificar, valorar y administrar los riesgos a los que estamos expuestos en el ámbito del comercio internacional.

Dentro de las buenas prácticas que nos han traído resultados positivos están los siguientes: garantizar la trazabilidad de nuestros servicios de inicio a término, la adecuada evaluación de nuestros Clientes y Proveedores Críticos, la homologación y constante capacitación de nuestros asociados de transporte de carga.

Asimismo, un correcto proceso de selección y evaluación periódica de nuestro personal, y su constante formación en relación a temas técnicos aduaneros y de prevención de riesgos nos ha permitido fortalecer nuestro sistema de gestión.

Briefly summarize your company. Describe services offered by ISCO.

Interamerican Service Co S.A.C. was founded in the year 1947 as a customs broker. Nowadays, as a logistics group, we offer Customs Clearance, Transport, Warehousing and Distribution, always keeping the same calling to serve both importers and exporters.

With a specialized team and a secure, efficient process, ISCO offers a comprehensive service throughout the supply chain. Our service includes Preloading Monitoring, International Transport, Customs Clearance, and National and Local Transport through distribution. We adapt all our operations to our customers' requirements.

What security best practices have you implemented as BASC associate?

The implementation of BASC certification has allowed us to identify, value and manage the risks we are exposed to in international trade.

Among the best practices that have had positive results are the following: guarantee the traceability of our services from beginning to end, the appropriate assessment of our Critical Providers and Clients, the standardization and constant training of our cargo transport associates.

Likewise, our management system has been strengthened by the right process of selection and periodic assessment of our staff, as well as their constant training in technical issues on customs and risk prevention.

De acuerdo a su política de seguridad basada en el Sistema de Gestión y Control de Seguridad BASC, ¿Qué procedimientos se aplican en su empresa en casos de sospechas de actividades ilícitas o de conspiraciones internas?

Actualmente contamos con canales de comunicación a todo nivel, los cuales permiten a nuestros colaboradores identificar algún incidente y puedan comunicarlo de manera inmediata y de forma confidencial al área de Calidad.

Nuestra área de Calidad es responsable de activar las diversas alertas y controles, así como hacer que las áreas responsables se involucren en el tratamiento de los incidentes, de ser el caso.

Así también, tenemos la consigna de trabajar de manera preventiva en los incidentes reportados a fin de evitar vuelvan a ocurrir, esto lo trabajamos a través de círculos de calidad.

¿Cree usted que la Certificación BASC, como plataforma, ayudó a su empresa implementar el programa OEA?

Sin duda el contar con la certificación BASC nos ayudó en gran medida para llegar a ser un Operador Económico Autorizado. Nos permitió tener nuestros procesos ordenados y orientados al aseguramiento del comercio internacional, así como la base documental para el cumplimiento de los requisitos para la aplicación de la certificación OEA.

Asimismo, gracias a que nuestro capital humano viene desarrollando sus actividades en base a los requisitos de la certificación BASC, tuvimos la facilidad de obtener el reconocimiento del programa OEA ante la SUNAT.

¿Cuál es su opinión respecto a las nuevas Certificaciones ISO 9001 E ISO 28000 que está ofreciendo BASC?

Nos parece una buena iniciativa por parte de BASC Perú el ampliar sus servicios de certificación, sobre todo consideramos que es una buena alternativa para empresas que participan de la cadena del comercio internacional ya que permite gestionar los riesgo de manera integral y reforzar los controles de los diversos procesos de la empresa. CS

According to your security policy based on the BASC Management and Security Control System, what procedures are applied in your company in case of suspicion of illegal activities or internal conspiracies?

Currently we have communication channels at all levels, which allow our collaborators to identify an incident and communicate it immediately and confidentially to the Quality department.

Our Quality department is responsible for activating the various alerts and controls, as well as making the responsible areas involved in the handling of incidents.

Also we have the instruction of working preventively in the reported incidents in order to avoid recurrence. We work with quality circles.

Do you believe that BASC Certification, as a platform, helped your company implement the AEO program?

Without a doubt the BASC certification helped us to a great extent to become an Authorized Economic Operator. It allowed us to have our processes organized and oriented to international trade assurance. It gave us the documentary basis to comply with the requirements for the AEO certification application.

Likewise, thanks to the fact that our human capital has been carrying out its activities based on BASC certification requirements, we have been able to obtain recognition of the AEO program from SUNAT.

What is your opinion regarding the new ISO 9001 and ISO 28000 Certifications offered by BASC?

We believe that it is a good initiative on the part of BASC Peru to expand its certification services, especially considering that it is a good alternative for companies that participate in the international trade chain. Certification allows you to manage risks in a comprehensive manner and strengthen the controls of various company processes. CS

Tecnología de Punta Aplicada a la Seguridad Industrial

CUTTING-EDGE TECHNOLOGY APPLIED TO INDUSTRIAL SECURITY

Hoy en día es posible proteger nuestros productos o valores aplicando la tecnología láser. Ésta tecnología nos permite tener un mejor orden y/o control en producciones a gran escala.

Sus beneficios son: Un grabado nítido y marcado sin desgaste, la impresión es correlativa sin duplicidad y grabado oculto (tinta ultra violeta).

Puede personalizarse de acuerdo a las necesidades del usuario con numeración, código de barras y logotipo de la empresa, que -de la mano de un diseño gráfico- se obtienen las muestras previas. Finalmente, recibimos la conformidad del cliente con la cual iniciaremos una producción eficaz y segura.

Hoy tú decides cómo proteger tu producto.

¡ PERSONALIZA!

Today it is possible to protect our products or values by applying laser technology. This technology allows us to have a better order and/or control in large-scale productions.

Its benefits are: a clear and marked engraving without wear, printing is correlative without duplicity and hidden engraving (ultra violet ink).

It can be customized according to the needs of the user with numbering, bar code and company logo, which – along with a design – is used to make samples. Finally, we receive the customer confirmation and we will start an efficient and safe production.

Today you decide how to protect your product.

CUSTOMIZE!

Nuevo plazo para la publicación de la ISO 45001

NEW DEADLINES FOR PUBLISHING ISO 45001

La gestión de la seguridad y salud en el trabajo adquirirá pronto una nueva estructura cuando la ISO 45001 sea publicada. Por su magnitud y alcance el lanzamiento oficial de esta nueva norma aún es incierto, aunque se estima que no sea más allá de Marzo de 2018.

Occupational health and safety management will soon acquire a new structure when ISO 45001 is published. Due to its magnitude and scope, the official launch of this new standard is still uncertain, though it is estimated to be in March 2018 at the most.

Los accidentes y las enfermedades relacionados a las actividades laborales representan un rubro preocupante en el mundo por sus dimensiones y repercusiones en la economía de las personas, empresas y países. De acuerdo a David Smith, presidente del comité que viene desarrollando la 'Norma ISO 45001 de Seguridad y Salud en el Trabajo', a nivel mundial cada 15 segundos un trabajador muere a causa de un accidente o enfermedad y 153 personas sufren una lesión, todos relacionados con el trabajo. Esto supone más de 2,3 millones de muertes al año y más de 300 millones de accidentes no mortales, según datos de la Organización Internacional del Trabajo (OIT).

Estos indicadores negativos pueden revertirse con el establecimiento de procesos adecuados al interior de las empresas y organizaciones. Precisamente la norma ISO 45001 busca este objetivo. Su diseño final ayudará a las organizaciones de cualquier tamaño y sector a poner en marcha un entorno de trabajo seguro para sus empleados, reduciendo los accidentes y las enfermedades de trabajo en todo el mundo.

Accidents and diseases related to occupational activities are a concerning issue in the world due to their dimensions and repercussions in the economy of people, companies and countries. According to David Smith, chairman of the committee developing the ISO 45001 Standard: Occupational Health and Safety Management Systems, worldwide a worker dies every 15 seconds caused by an accident or disease and 153 people suffer an injury, all of them work related. This involves over 2,3 million deaths a year and over 300 million mortal accidents according to the data provided by the International Labour Organization (ILO).

These negative indicators can be reverted if appropriate processes are implemented within companies and organizations. Actually, ISO 45001 Standard aims at that. Its final design will help organizations of all sizes and sectors to put in place a safe work environment for their employees, reducing occupational accidents and diseases around the world.

Teniendo en cuenta que esta nueva norma de sistemas de gestión pasará a formar parte de las normas empresariales, independientemente de si las organizaciones deciden adoptarla o no, es importante para las empresas mantenerse al tanto de los últimos desarrollos.

Antecedentes

Los sistemas de gestión de seguridad y salud en el trabajo no son nuevos, y a pesar de que un buen número de países tienen sus propias normas, como Estados Unidos y Australia, los únicos documentos internacionales son las Directrices ILO-OSH 2001, de la Organización Internacional del Trabajo, y OHSAS 18001, desarrollado por la British Standards Institution (organismo de normalización británico).

El desarrollo de ISO 45001 reúne información de todos estos grupos que han desarrollado normas en todo el mundo, así como de instituciones dedicadas a la seguridad como la Institución de Seguridad y Salud en el Trabajo (IOSH), la Sociedad Americana de Ingenieros de Seguridad (ASSE) y la Asociación Americana de Higiene Industrial (AIHA).

Con mucha experiencia en este campo, la OIT ha proporcionado información sobre aquellos aspectos de sus normas que son relevantes y esenciales para la gestión eficaz de la SST: la importancia de la participación de la alta dirección y el papel esencial de los trabajadores al participar en el desarrollo y la operación del sistema de gestión de la Seguridad y Salud en el Trabajo (SST). Los desarrolladores señalan que siempre que ha sido posible, se ha procurado que no exista conflicto con normas que ya existen y que son ampliamente adoptadas.

En este sentido, se espera que los usuarios del estándar OHSAS 18001 y las Directrices ILO-OSH adopten la ISO 45001, ya que no entra en conflicto con estos documentos y aumenta la posibilidad de integrar la gestión de la SST en los procesos de negocio globales.

Los beneficios de la adopción de la Norma ISO 45001, aparte de ser una nueva norma surgida del consenso, es que, naturalmente, se alinea a los enfoques de gestión adoptados para otros riesgos empresariales en el conjunto de normas de sistemas de gestión de ISO. Esto debería beneficiar a las pyme cuando se trata de gestionar distintas normas de requisitos. A diferencia de las Normas ISO 9001 e ISO 14001, no existe un proceso formal de transición, pero se están haciendo esfuerzos para ayudar a las organizaciones con la transición de la OHSAS 18001 a la Norma ISO 45001.

La publicación de la Norma ISO 45001 debería dar mayor credibilidad a la gestión de la SST. Es de esperar que reciba el respaldo dado a las Normas ISO 9001 e ISO 14001 por la comunidad empresarial.

Las grandes organizaciones querrán estar seguras de que las organizaciones que operan bajo su control tienen buenos sistemas de gestión de SST establecidos, mucho más cuando se busca el aseguramiento de la calidad en el mundo actual. Si éste es el caso, la adopción de la norma debería superar los 100.000 usuarios, pasados tres años de su publicación, según David Smith. El éxito de este desarrollo se debe al duro trabajo realizado en el comité ISO/PC 283 por los cerca de 100 expertos de todo el mundo.

Taking into account that this new standard on Management Systems will be part of business standards, regardless of the decisions made by organizations to adopt it or not, it is important for companies to keep up to date of the latest developments.

Background

Occupational Health and Safety Management Systems are not new and, even though a good number of countries has their own standards, such as United States and Australia, the only international documents are the ILO-OSH 2001 Guidelines of the International Labour Organization (ILO), as well as the OHSAS 18001, developed by the British Standards Institution.

The ISO 45001 gathers information from all of these groups that have developed standards around the world, and from institutions dedicated to safety, such as the Institution of Occupational Safety and Health (IOSH), the American Society of Safety Engineers (ASSE) and the American Industrial Hygiene Association (AIHA).

Having a lot of experience in this field, ILO has provided information about those aspects from its standards that are relevant and essential for efficient Occupational Safety and Health (OSH) management: the importance of the involvement of senior management, and the essential role workers have in the development and operations of the OSH management system. The developers point out that, whenever possible, they have tried not to disagree with the already existing standards that are already extensively adopted.

In this sense, users of the OHSAS 18001 standard and ILO-OSH Guidelines are expected to adopt the ISO 45001, since it does not go against these documents and increases the possibility to integrate OSH management in global business processes.

Besides being a new standard that came up in consensus, the benefit of adopting the ISO 45001 Standard is that it naturally aligns to the management approaches adopted for other business risks within the group of ISO standards on management systems. This should benefit SMBs when managing different requirement standards. Unlike the ISO 9001 and ISO 14001 Standards, there is no formal process of transition, but efforts are being made to help organizations with the transition from OHSAS 18001 to ISO 45001 Standard.

Publishing the ISO 45001 Standard should give more credibility to OSH management. The business community is expected to support it just as ISO 9001 and ISO 14001 Standards.

Big organizations will want to make sure organizations operating under their control have good OSH management systems in place, and even more so when the world is currently seeking quality assurance. If this is the case, over 100,000 users would adopt the standard after three years of its publication, according to David Smith, The success of this development is thanks to the hard work the ISO/PC 283 committee put with around 100 experts from around the world.

El lanzamiento

Se esperaba que la publicación del ISO 45001 se realice a finales de 2016 o principios del presente 2017. Sin embargo, de acuerdo a los resultados del encuentro en Febrero último en Viena (Austria) de los miembros del Comité ISO/PC 283 que está trabajando la futura ISO 45001, el lanzamiento podría ser a finales de este año o principios del 2018.

Como se sabe, dicho Comité está compuesto por numerosos observadores de hasta 14 países distintos y de alrededor de 20 organismos de enlace, los cuales cuentan con el conocimiento y la experiencia práctica en cuestiones de salud y seguridad ocupacional, así como en los desafíos a los que este proyecto se enfrenta.

La reunión tuvo por objetivo continuar con el trabajo sobre el texto DIS 2 de la futura ISO 45001. El DIS es un Borrador de Norma Internacional y, en este caso, es el segundo sobre la ISO 45001. Como se recuerda, se espera que esta nueva norma sustituya a la OHSAS 18001, estándar internacional sobre Sistemas de Gestión de Seguridad y Salud en el Trabajo. Esta reunión en Austria tuvo lugar luego de la reunión realizada en el mes de Noviembre pasado en Lituania.

Asimismo, se sabe que en la reciente reunión se dio a conocer el siguiente cronograma sobre los posibles plazos de trabajo y publicación de la futura ISO 45001:

- Desde Febrero hasta Marzo del 2017 tendrán lugar los preparativos y el desarrollo del documento DIS 2.
- A partir de Marzo de 2017 hasta Mayo del 2017estará disponible el DIS2 para su traducción.
- Desde Mayo hasta Julio del 2017 tendrá lugar la elección.
- En Julio de 2017 se conocerán los resultados de la votación del DIS 2, así como los posibles comentarios.
- En Septiembre de 2017 se reunirá el Comité ISO/PC 283 para verificar los resultados de la votación DIS 2.

Según trascendió, la siguiente reunión del Comité elaborador de la norma ISO 45001 tendría lugar del 18 al 23 de septiembre de este año en Malaca (Malasia) donde se revisaría los resultados de la votación así como los comentarios del mismo para así poder establecer un nuevo calendario de trabajo en el proceso de desarrollo de la ISO 45001.

Si finalmente el borrador DIS 2 es aprobado y no se requiere FDIS (proyecto final de la norma internacional), se prevé que la publicación de la futura ISO 45001 pueda ser durante los meses de Octubre / Noviembre de 2017. Si el FDIS fuese necesario, la publicación de la norma podría demorarse hasta el mes de marzo del próximo año 2018.

"... a nivel mundial cada 15 segundos un trabajador muere a causa de un accidente o enfermedad y 153 personas sufren una lesión, todos relacionados con el trabajo."

"... worldwide a worker dies every 15 seconds caused by an accident or disease and 153 people suffer an injury, all of them work related."

The launch

The publication of ISO 45001 was expected to take place in late 2016 or early 2017. However, launch could be late this year or early 2018, according to the conclusions of the ISO/PC 283 Committee meeting in Vienna (Austria) last February. This Committee is working on the future ISO 45001.

As is known, this Committee is composed of numerous observers from up to 14 different countries and about 20 liaison agencies, which have the knowledge and practical experience in occupational health and safety issues to deal with the challenges that this project is facing.

The purpose of the meeting was to continue the work on DIS 2 text of the future ISO 45001. The DIS is an International Standard Draft and, in this case, it is the second on ISO 45001. As is recalled, this new standard is expected to replace the OHSAS 18001, international standard on Occupational Health and Safety Management Systems. This meeting in Austria took place after the meeting held last November in Lithuania.

Likewise, it is known that in the recent meeting the next schedule was made known the possible work deadlines and the publication of the future ISO 45001:

- From February to March 2017, preparation and development of the document DIS 2 will take place.
- From March 2017 the DIS2 will be available for translation.
- From May to July 2017 the election will take place.
- In July 2017 the results of the DIS 2 vote will be announced, as well as possible comments.
- In September 2017, the ISO/PC 283 Committee will meet to verify the results of the DIS 2 vote.

The next meeting of the ISO 45001 Committee was scheduled to take place from September 18 to 23 this year in Malacca (Malaysia), where the results of the vote and its comments would be reviewed in order to establish a new work calendar for the ISO 45001 development process.

If the draft DIS 2 is finally approved and FDIS (final draft of the International Standard) is not required, it is expected that the publication of the future ISO 45001 may be during the months of October/November 2017. If FDIS is necessary, the publication of the standard could be delayed until March 2018.

Fuente/ Source: Revista AENOR Enero 2016 / ISOTools excellence
AENOR magazine January 2016 / ISOTools excellence

Foro sobre figura legal "Tercero Civilmente Responsable"

FORUM ON THE LEGAL FIGURE "THIRD-PARTY LIABILITY"

Con el objetivo de concientizar a los colaboradores de las empresas sobre los riesgos, alcances y las responsabilidades respecto a la figura legal "Tercero Civilmente Responsable", así como sugerir los procedimientos a seguir ante una posible responsabilidad penal de los empleados y directivos en casos de hallazgo de sustancias ilícitas dentro de la carga; el 10 de febrero pasado se BASC PERÚ realizó un foro gratuito sobre este tema en las instalaciones de la Cámara de Comercio Americana del Perú (AMCHAM).

Alrededor de un centenar de participantes pertenecientes a diversas empresas asociadas BASC, tuvieron la oportunidad de informase y actualizar los detalles técnicos acerca de este importante tema legal relacionada a la seguridad de la cadena de suministro. La exposición estuvo a cargo de un reconocido fiscal del Ministerio Público – Fiscalía de la Nación.

In order to raise awareness among companies' employees about the risks, scope and responsibilities regarding the legal figure "Third-Party Liability", as well as to suggest the procedures to be followed for possible criminal liability of employees and managers in case of finding of illicit substances within the cargo; on February 10 BASC PERU held a free forum on this subject at the premises of the American Chamber of Commerce of Peru (AMCHAM).

About a hundred participants from various BASC partner companies had the opportunity to inform and update the technical details about this important legal issue related to supply chain security. The presentation was in charge of a recognized prosecutor from the Attorney General's Office.

Existen 49 empresas certificadas con el programa OEA

THERE ARE 49 COMPANIES CERTIFIED WITH THE AEO PROGRAM

Con la incorporación a principios del presente año de 11 empresas a la lista de poseedores de la certificación del programa Operador Económico Autorizado (OEA), la SUNAT registra actualmente a un total de 49 empresas con esta certificación de seguridad de la cadena de suministros de la Organización Mundial de Aduanas (OMA).

Entre las nuevas empresas OEA se encuentran las siguientes: AGENCIA AFIANZADA DE ADUANA J.K.M. S.A.C; AUSA OPERACIONES LOGISTICAS S.A.; INCALPACA TEXTILES PERUANOS DE EXPORT S.A.; ADUANLINK SAC; ANTARES ADUANAS S.A.C; INKABOR S.A.C.; TERMINAL INTERNACIONAL DEL SUR S.A. - TISUR; FUNDO SACRAMENTO S.A.C; EXSA S.A.; CREDITEX S.A.A; y CAMPOSOL S.A.

En esta relación figuran empresas que también cuentan con la certificación BASC por lo que estos se encuentran en una situación inmejorable en su capacidad de realizar una eficiente gestión de seguridad de sus cadenas de suministro internacional para el beneficio del comercio exterior peruano.

With the inclusion of 11 companies to the list of those holding a certification of the Authorized Economic Operator (AEO) program in the beginning of this year, SUNAT currently has a total of 49 companies with this supply chain certification of the World Customs Organization (WCO).

Among the new AEO companies, the following can be found: AGENCIA AFIANZADA DE ADUANA J.K.M. S.A.C; AUSA OPERACIONES LOGISTICAS S.A.; INCALPACA TEXTILES PERUANOS DE EXPORT S.A.; ADUANLINK SAC; ANTARES ADUANAS S.A.C; INKABOR S.A.C.; TERMINAL INTERNACIONAL DEL SUR S.A. – TISUR; FUNDO SACRAMENTO S.A.C; EXSA S.A.; CREDITEX S.A.A; and CAMPOSOL S.A.

In this list, there are companies that also have the BASC certification, so they are in an unbeatable situation in terms of their ability to efficiently manage their international supply chains for the benefit of the Peruvian foreign trade.

Fuente/Source: SUNAT

Auditores BASC se capacitan en ISO 37001: 2016 (Sistema de Gestión Anti – Soborno)

BASC AUDITORS ARE TRAINED IN ISO 37001: 2016 (ANTI-BRIBERY MANAGEMENT SYSTEM)

Como parte de su política de mejora continua BASC PERÚ se realizó los días 14, 15 y 16 de febrero pasado el curso internacional Auditor Líder en ISO 37001: 2016 (Sistema de Gestión Anti – Soborno).

Este curso es acreditado por la Professional Evaluation and Certification Board (PECB) de Canadá y estuvo dirigido a los auditores internacionales de BASC PERÚ con la finalidad de darles a conocer las mejores prácticas para implementar y administrar los componentes esenciales del Sistema de Gestión Anti- Soborno, tal como se especifica en la norma ISO 37001. El curso fue liderado por el Sr. Miller Romero, Auditor Líder e Implementador de la ISO 37001 (SGAS).

As part of its policy of continuous improvement, BASC PERU held on February 14, 15 and 16, the international course Lead Auditor in ISO 37001: 2016 (Anti-Bribery Management System).

This course is accredited by Canada's Professional Evaluation and Certification Board (PECB) and was addressed to BASC PERU's international auditors in order to inform them about best practices for implementing and managing the essential components of the Anti-Bribery Management System, as specified in ISO 37001. The course was led by Mr. Miller Romero, Lead Auditor and Implementer of ISO 37001 (SGAS).

BASC PERÚ otorga Certificación ISO 9001:2015 a empresa de seguridad

BASC PERU AWARDS ISO 9001: 2015 CERTIFICATION TO SECURITY COMPANY

La empresa NATIONAL ENTERPRISE OF SECURITY S.A. obtuvo recientemente la certificación ISO 9001: 2015 de parte de BASC PERÚ CERTIFICATION, una división del capítulo peruano de la Alianza Empresarial para un Comercio Seguro (BASC por sus siglas en inglés). Dicha empresa recibió la certificación ISO para sus oficinas de Lima, Callao, Piura, La Libertad, Ancash e Ica; la cual se suma a la Certificación BASC obtenida en el año 2008.

Gerente general de BASC PERÚ con el equipo de National Enterprise of Security S.A

BASC PERU General manager with the National Enterprise of Security S.A. team

NATIONAL ENTERPRISE OF SECURITY S.A., recently obtained the ISO 9001: 2015 certification from BASC PERU CERTIFICATION, a division of the Peruvian chapter of the Business Alliance for a Secure Commerce (BASC). This company was ISO certified for its offices in Lima, Callao, Piura, La Libertad, Ancash and Ica; which is added to the BASC Certification obtained in 2008.

CAPACITE A SUS CLIENTES Y PROVEEDORES EN EL SGCS BASC

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.

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.

Lugar

Instalaciones de la empresa asociada BASC.

Duración

90 minutos

Mayor Información

paula.lopez@bascperu.org // afiliaciones2@bascperu.org
Fijo: 6128300 anexo 2232 / 2230 Celular: 946454057 - 98147*6514

BASC
Business Alliance for Secure Commerce

CERTIFÍQUESE CON NOSOTROS

BASC PERÚ CERTIFICATION

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 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 ANAB

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