



BUSINESS ALLIANCE FOR SECURE COMMERCE

# ESTÁNDAR INTERNACIONAL DE SEGURIDAD BASC

---

## 5.0.3

EMPRESAS QUE DESEEN GESTIONAR  
CONTROLES OPERACIONALES BÁSICOS DE  
SEGURIDAD


Versión 5 – 2017

Fecha de aprobación: 10 de agosto de 2017

Todos los derechos reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación puede ser reproducida, modificada o utilizada en cualquier forma o por cualquier medio, electrónico o mecánico, sin el permiso por escrito de World BASC Organization, Business Alliance for Secure Commerce, BASC.

## TABLA DE CONTENIDO

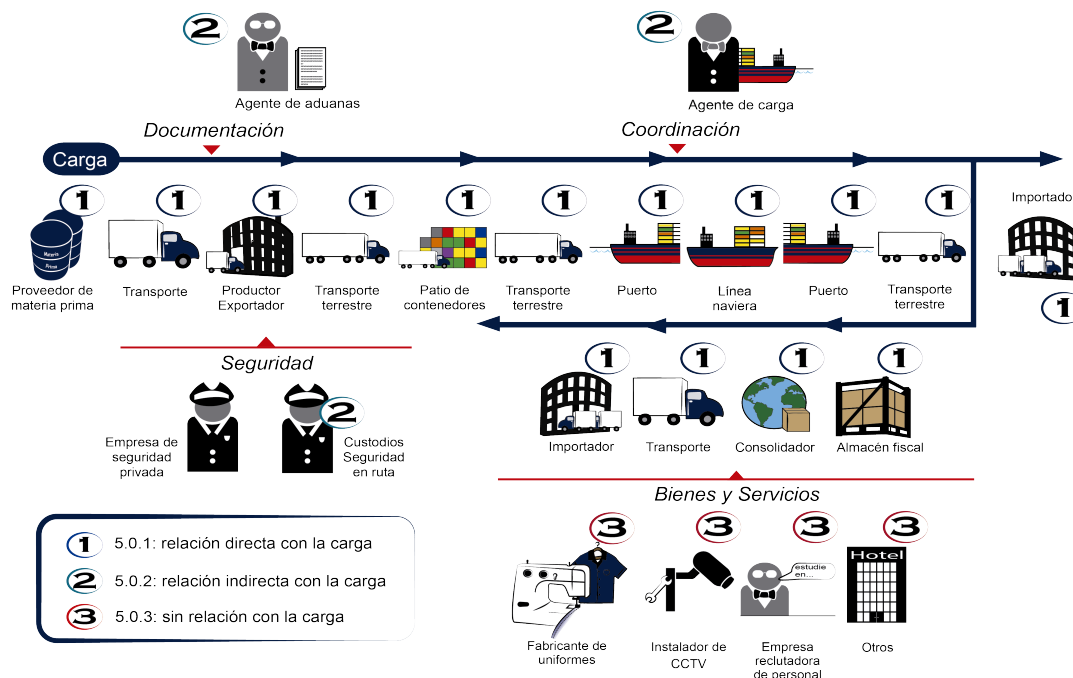
<b>0</b>	<b>INTRODUCCIÓN</b>	<b>3</b>
<b>1</b>	<b>REQUISITOS DE ASOCIADOS DE NEGOCIO</b>	<b>5</b>
1.1	GESTIÓN DE ASOCIADOS DE NEGOCIO	5
1.2	PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO	5
<b>2</b>	<b>SEGURIDAD EN LOS PROCESOS RELACIONADOS CON EL PERSONAL</b>	<b>6</b>
2.1	PROCEDIMIENTO PARA LA GESTIÓN DEL PERSONAL	6
2.2	PROGRAMA DE CAPACITACIÓN	7
<b>3</b>	<b>CONTROL DE ACCESO Y SEGURIDAD FÍSICA</b>	<b>8</b>
3.1	CONTROL DE ACCESO A LAS INSTALACIONES	8
3.2	SEGURIDAD FÍSICA	8
<b>4</b>	<b>SEGURIDAD EN LOS PROCESOS RELACIONADOS CON LA TECNOLOGÍA Y LA INFORMACIÓN</b>	<b>9</b>
4.1	INFORMACIÓN	9
4.2	SEGURIDAD EN TECNOLOGÍA DE LA INFORMACIÓN	9


	<b>World BASC Organization</b> <b>Business Alliance for Secure Commerce</b> <b>Estándar Internacional de Seguridad</b> <b>5.0.3</b>	Versión: 05-2017
		Aprobado: 10-AGO-2017
		Página: Página 3 de 10

## 0 Introducción

El estándar internacional de seguridad BASC, agrupa las medidas de control operacional para los principales elementos que se relacionan con la seguridad de la cadena de suministro. Tiene como objetivo contribuir con las empresas para que sus actividades se desarrollen de forma segura, proteger a sus colaboradores, sus instalaciones, su carga, a sus asociados de negocio y otras partes interesadas.

Se emitieron tres documentos con la intención de consolidar los requisitos correspondientes a la interacción con la carga definida en el alcance del SGCS. El Estándar Internacional de Seguridad BASC 5.0.1 aplica a las empresas que tienen contacto directo con la carga o con las unidades de transporte de carga, tales como fabricantes, productores, exportadores, importadores, comercializadores, operadores logísticos, transportadores (ej.: terrestres, marítimos, aéreos, etc.), empresas que almacenan carga, instalaciones portuarias, entre otros. El Estándar Internacional de Seguridad BASC 5.0.2 aplica a las empresas que tienen una relación indirecta con la carga o con las unidades de transporte de carga. Y el Estándar Internacional de Seguridad BASC 5.0.3 es aplicable a todo tipo de empresas que deseen gestionar los controles operacionales básicos que les permitan una operación segura. La siguiente figura ilustra ejemplos de la aplicación de este criterio:




	<p align="center"><b>World BASC Organization</b>  <b>Business Alliance for Secure Commerce</b>  <b>Estándar Internacional de Seguridad</b>  <b>5.0.3</b></p>	<p align="right">Versión: 05-2017</p>
		<p align="right">Aprobado: 10-AGO-2017</p>
		<p align="right">Página:  Página <b>4</b> de <b>10</b></p>

Este documento es el resultado de la gestión de:

Consejo Directivo 2015-2017: Álvaro Alpízar, Presidente; José Nelton, Vicepresidente; Maricela Valenzuela, Secretaria; Juan Toruño, Tesorero y; Raúl Saldías, Vocal.

Consejo Directivo 2017-2019: Álvaro Alpízar, Presidente; Juan David Osorio, Vicepresidente; Armando Rivas, Secretario; Salvador Mónico, Tesorero y; Emilio Aguiar, Vocal.

Comité Técnico de WBO: Omar Castellanos, Director Ejecutivo Capítulo BASC Dominicana; Diego Castillo, Director Ejecutivo Capítulo BASC Pichincha; Jorge Hütt, Auditor Internacional BASC Costa Rica; Jorge Jiménez, Director Ejecutivo Capítulo BASC Colombia; Jorge Wellmann, Director Ejecutivo Capítulo BASC Guatemala.

	<p align="center"><b>World BASC Organization</b>  <b>Business Alliance for Secure Commerce</b>  <b>Estándar Internacional de Seguridad</b>  <b>5.0.3</b></p>	Versión: 05-2017
		Aprobado: 10-AGO-2017
		Página: Página 5 de 10

## **1 REQUISITOS DE ASOCIADOS DE NEGOCIO**

### **1.1 Gestión de asociados de negocio**

*Orientaciones: Los asociados de negocio constituyen partes interesadas de la empresa, representan clientes, proveedores y terceros que se consideran con algún nivel de criticidad de acuerdo a la gestión de riesgos de la empresa.*

La empresa debe establecer un procedimiento documentado para implementar y verificar periódicamente controles operacionales a sus asociados de negocio. La extensión, detalle y enfoque de los mismos, debería estar alineado con el impacto de cada asociado de negocio en la gestión de riesgos. La empresa debe mantener un listado actualizado de sus asociados de negocio.

### **1.2 Prevención del lavado de activos y financiación del terrorismo**


1.2.1 El procedimiento para la selección de los asociados de negocio, debería incluir criterios de prevención tales como:

- a) Conocimiento de sus asociados de negocio, identidad y legalidad de la empresa y sus socios.
- b) Antecedentes legales, penales y financieros.
- c) Monitoreo de sus operaciones (actividad económica, origen de sus ingresos, características de sus operaciones, otros clientes, cumplimiento de contratos y antigüedad en el mercado).
- d) Reporte oportuno a las autoridades competentes cuando se identifiquen operaciones sospechosas.
- e) Verificación de pertenencia a gremios o asociaciones.

1.2.2 Debería contemplar como mínimo los siguientes factores para la identificación de operaciones sospechosas:

- a) Origen y destino de la operación de comercio.
- b) Frecuencia de las operaciones.
- c) Valor y tipo de mercancías.
- d) Modalidad de la operación de transporte.
- e) Forma de pago de la transacción.
- f) Inconsistencias en la información proporcionada por los asociados de negocio.
- g) Requerimientos que salen de lo establecido.

*Nota: Para el reporte de la operación sospechosa no se requiere tener certeza de que se trata de una actividad delictiva, ni identificar el tipo penal o que los recursos*

	<p align="center"><b>World BASC Organization</b>  <b>Business Alliance for Secure Commerce</b>  <b>Estándar Internacional de Seguridad</b>  <b>5.0.3</b></p>	<p align="right">Versión: 05-2017</p>
		<p align="right">Aprobado: 10-AGO-2017</p>
		<p align="right">Página:  <b>Página 6 de 10</b></p>

*involucrados provienen de tales actividades. Este reporte debe hacerse ante las autoridades competentes de cada país.*

## **2 SEGURIDAD EN LOS PROCESOS RELACIONADOS CON EL PERSONAL**

*Orientaciones: Se entiende como personal a los colaboradores directos, el personal subcontratado y el personal temporal.*

### **2.1 Procedimiento para la gestión del personal**

La empresa debe contar con un procedimiento documentado, conforme a la legislación, que regule las siguientes actividades:

#### **2.1.1 Verificación antes de la contratación:**

- a) Información suministrada por el candidato.
- b) Referencias laborales y personales.
- c) Antecedentes.

#### **2.1.2 Selección y contratación:**

La empresa debe:

- a) Verificar las competencias.
- b) Aplicar pruebas para detectar el consumo de alcohol y drogas ilícitas al personal que ocupará cargos críticos.
- c) Mantener un archivo fotográfico actualizado del personal e incluir un registro de huellas dactilares y firma.
- d) Controlar la entrega, uso y devolución de elementos de trabajo, identificación y uniformes cuando tengan distintivos de la empresa.
- e) Considerar en el proceso de inducción los elementos descritos en el apartado 2.2.


La empresa debería:

- f) Realizar una visita domiciliaria al personal que ocupará cargos críticos basado en la gestión de riesgos y las regulaciones locales.

#### **2.1.3 Mantenimiento del personal:**

La empresa debe:

- a) Actualizar los datos del personal al menos una vez al año.

	<p align="center"><b>World BASC Organization</b>  <b>Business Alliance for Secure Commerce</b>  <b>Estándar Internacional de Seguridad</b>  <b>5.0.3</b></p>	<p align="right">Versión: 05-2017</p>
		<p align="right">Aprobado: 10-AGO-2017</p>
		<p align="right">Página:  Página 7 de 10</p>

- b) Verificar los antecedentes del personal que ocupa cargos críticos como mínimo una vez al año.
- c) Aplicar pruebas para detectar el consumo de alcohol y drogas ilícitas en forma aleatoria, como máximo cada dos años y cuando se presente sospechas.
- d) Mantener un programa de prevención de adicciones.
- e) Mantener un programa de prevención del riesgo de corrupción y soborno.

La empresa debería:

- f) Realizar una visita domiciliaria al personal que ocupa cargos críticos, basado en la gestión de riesgos y las regulaciones locales, máximo cada dos años.

#### 2.1.4 Terminación de la vinculación laboral:

La empresa debe:

- a) Retirar la identificación, uniformes y activos con base en los registros generados por la entrega de los mismos.
- b) Eliminar el acceso a los sistemas informáticos y a las instalaciones.

La empresa debería, de conformidad con la gestión de riesgos:


- c) Comunicar a las partes interesadas la desvinculación del colaborador.

*Nota: Cuando se presente un cambio en el cargo de un colaborador, se debe tener en cuenta los elementos descritos en el proceso de contratación.*

## 2.2 Programa de capacitación

La empresa debe contar con un programa anual de capacitación que incluya como mínimo:

- a) Políticas del SGCS BASC (ver norma BASC 4.2), manejo de información (ver 4.1.), etc.
- b) Gestión de riesgos, controles operacionales, preparación y respuesta a eventos.
- c) Cumplimiento de los requisitos legales relacionados con sus funciones.
- d) Impacto de las actividades individuales sobre el cumplimiento de los indicadores de eficacia de los procesos.
- e) Aplicación de los procedimientos del SGCS BASC.
- f) Prevención de adicciones al alcohol, drogas, juegos y otros, que incluya avisos visibles y material de lectura.
- g) Prácticas de prevención de corrupción y soborno.
- h) Lavado de activos y financiación del terrorismo.
- i) Prácticas de prevención de conspiraciones internas y actividades sospechosas.

	<p align="center"><b>World BASC Organization</b>  <b>Business Alliance for Secure Commerce</b>  <b>Estándar Internacional de Seguridad</b>  <b>5.0.3</b></p>	<p align="right">Versión: 05-2017</p>
		<p align="right">Aprobado: 10-AGO-2017</p>
		<p align="right">Página:  Página 8 de 10</p>

### **3 CONTROL DE ACCESO Y SEGURIDAD FÍSICA**

#### **3.1 Control de acceso a las instalaciones**

*Orientaciones: El control de acceso a las instalaciones impide la entrada no autorizada, mantiene control de los colaboradores, visitantes y protege los bienes de la empresa.*

La empresa debe contar con un procedimiento documentado que incluya las siguientes actividades:

##### **3.1.1 Acceso de colaboradores:**

- a) Identificar a sus colaboradores.
- b) Controlar su ingreso a las instalaciones.
- c) Limitar acceso a las áreas asignadas.

##### **3.1.2 Acceso a los visitantes, contratistas y terceros:**

- a) Presentar una identificación oficial vigente con fotografía.
- b) Mantener un registro del ingreso y salida.
- c) Solicitar autorización para su ingreso.
- d) Entregar una identificación temporal controlada.
- e) Asegurar que estén acompañados o controlados por personal de la empresa.
- a) Limitar acceso a las áreas asignadas.

##### **3.1.3 Inspeccionar el correo y paquetes recibidos antes de distribuirlos, manteniendo un registro que incluya la identificación de quién recibe y a quién está destinado.**

##### **3.1.4 Control operacional en las instalaciones que incluya:**

- a) Debe exhibir el carné o identificación temporal en un lugar visible, bajo las normas de seguridad industrial aplicables.
- b) Identificar y retirar a personas no autorizadas.


#### **3.2 Seguridad física**

*Orientaciones: Seguridad física hace referencia a las medidas de protección de las instalaciones en donde se llevan a cabo procesos críticos.*

##### **3.2.1 La empresa debe implementar y mantener:**

- a) Estructuras y barreras perimetrales que impidan el acceso no autorizado.



	<b>World BASC Organization</b> <b>Business Alliance for Secure Commerce</b> <b>Estándar Internacional de Seguridad</b> <b>5.0.3</b>	Versión: 05-2017
		Aprobado: 10-AGO-2017
		Página: Página 9 de 10

- b) Cerraduras en puertas y ventanas.
- c) Sistemas de alarma que identifiquen acceso no autorizado.

#### 3.2.2 La empresa debe establecer y documentar:

- a) Inspecciones y reparaciones periódicas para mantener la integridad de las barreras perimetrales y estructura de los edificios.
- b) Control de llaves, dispositivos y claves de acceso.
- c) Inspecciones y reparaciones periódicas a los sistemas de emergencia.

#### 3.2.3 La empresa debería implementar y mantener de conformidad con su gestión de riesgos:

- a) Sistemas de circuito cerrado de televisión monitoreado por personal competente durante las 24 horas.
- b) Sistemas de respaldo de imágenes y video (grabación) con la capacidad de almacenamiento suficiente para responder a posibles eventos.

*Nota: Los elementos de seguridad física deben ser conforme con la gestión de riesgos.*

#### 3.2.4 La empresa debería tener un servicio de seguridad competente de conformidad con los requisitos legales y que garantice una acción de respuesta oportuna.

### 4 SEGURIDAD EN LOS PROCESOS RELACIONADOS CON LA TECNOLOGÍA Y LA INFORMACIÓN

*Orientaciones: Se considera seguridad de la información a las medidas y controles establecidos por la empresa para mantener la integridad, confidencialidad y disponibilidad de la documentación, registros y evidencias relacionadas con el SGCS.*

#### 4.1 Información


La empresa debe establecer e implementar:

- a) Una política para impedir que se revele información confidencial.
- b) Una política de uso de los recursos informáticos.

#### 4.2 Seguridad en tecnología de la información

La empresa debe:

- a) Establecer una política o procedimiento documentado para gestionar la seguridad informática que permita identificar, proteger y recuperar la información.

	<p align="center"><b>World BASC Organization</b>  <b>Business Alliance for Secure Commerce</b>  <b>Estándar Internacional de Seguridad</b>  <b>5.0.3</b></p>	Versión: 05-2017
		Aprobado: 10-AGO-2017
		Página: Página <b>10</b> de <b>10</b>

- b) Utilizar cuentas asignadas de forma individual y cada usuario que acceda al sistema debe tener sus propias credenciales de acceso y mantener contraseñas; estas deben cambiarse periódicamente.
- c) Revisar periódicamente los accesos asignados a los usuarios.
- d) Impedir la instalación de *software* no autorizado.
- e) Implementar y mantener *software* y *hardware* que proteja la información de amenazas informáticas (virus, accesos no autorizados y similares).
- f) Contar con copias de seguridad de la información sensible y una copia debe almacenarse fuera de las instalaciones de forma segura con base a la gestión de riesgos.
- g) Eliminar el acceso a la información a todos los colaboradores y usuarios externos al terminar su contrato o acuerdo.
- h) Mantener un registro actualizado de los usuarios y claves de acceso.
- i) Cerrar/bloquear la sesión en equipos desatendidos.

La empresa debería:

- j) Prohibir la conexión de dispositivos periféricos personales (teléfonos inteligentes, reproductores MP3, memorias USB, etc.) a cualquier dispositivo que esté conectado a la red informática. Los puertos USB deberían ser desactivados por defecto.