|  |  |  |  |
| --- | --- | --- | --- |
| Titulo:  Manual de Procedimientos para Operaciones Seguras del SGCS | | | |
|  | PUESTO | NOMBRE | FECHA |
| ELABORADO POR: | Coordinador de Calidad | Miguel Kikuchi | 12/04/2018 |
| REVISADO POR: | Jefe de Seguridad y Calidad | Ricardo Alarcon | 12/04/2018 |
| APROBADO POR: | Gerente General | Giovanni Klein | 12/04/2018 |

1. **OBJETIVO**

Definir la metodología a seguir para realizar nuestras actividades con la debida evaluación y prevención de los riesgos dentro de nuestro Sistema de Gestión en Control y Seguridad (SGCS), basado en los estándares de seguridad del SGCS BASC, del Programa del Operador Económico Autorizado (OEA) y de las normas Anti Soborno y las de Prevención del Lavado de Activos y Financiamiento al Terrorismo (PLAFT).

1. **ALCANCE**

Es aplicable a todo el personal de la Empresa.

1. **RESPONSABILIDAD**
2. El Coordinador de Calidad es responsable de verificar la adecuada ejecución del presente manual.
3. El Comité de Seguridad del SGCS es responsable del cumplimiento del presente manual.
4. **ABREVIATURAS**

GG Gerente General

GLO Gerente de Logística

SCO Supervisor Comercial

COM Asistente Comercial

JST Jefe de Seguridad, Transporte y Calidad

CCA Coordinador de Calidad

ACA Asistente de Calidad

SSC Supervisor de Servicio al Cliente

ESC Ejecutivo de Servicio al Cliente

UBN Unidad Básica de Negocios

SUP Supervisor de Operaciones

CDE Coordinador de Despachos

JAD Jefe de Administración y Contabilidad

ARH Asistente de RRHH

SSI Supervisor de Sistemas

JLE Jefe Legal

SLE Supervisor Legal

LIQ Liquidador

SEG Jefe de Seguridad

OFI Oficial de Cumplimiento

1. **CONDICIONES GENERALES**
   1. El término Asociado de Negocios incluye a los clientes, proveedores y terceros dentro de la cadena de suministros para CLI.
   2. La cadena de suministros, para los propósitos del SGCS, se inicia en el punto de origen y termina en el punto de distribución.
   3. Los requisitos mínimos de Seguridad C-TPAT que aplican al presente manual son los Estándares de Seguridad para el Agente aduanal, para la prevención de actos ilícitos como el robo, narcotráfico, lavado de activos o terrorismo.
   4. Los requisitos a cumplir son los señalados en la norma BASC, el procedimiento de Certificación OEA, las normas de PLAFT y las Anti Soborno del ISO 37001.
   5. **Exclusión:** El Estándar BASC Agente Aduanal Numeral 6.8.3 indica que los lockers sean controlados y separados de áreas de almacenamiento y manejo de carga, este requisito se excluye del presente Manual; ya que en CLI no contamos con zonas para el almacenamiento y manejo de la carga, puesto que la carga en ningún momento ingresa a nuestras instalaciones.
2. **DESCRIPCIÓN DEL MANUAL DE PROCEDIMIENTOS**

|  |  |
| --- | --- |
| **DESCRIPCIÓN DE LA ACTIVIDAD** | **RESPONSABLE** |
| * 1. **Requisitos de los Asociados de Negocios**      1. Se debe evaluar a los clientes y proveedores, según lo indican los procedimientos de Selección de Clientes PRO-CO-012 y Selección y Evaluación de Proveedores PRO-AD-025, así como el Manual Anti Soborno y de PLAFT MAN-SIG-002.      2. Los files de clientes y proveedores deben contar con documentos que acrediten si tienen certificaciones en programas de seguridad Basc, o de alguna autoridad aduanera nacional o extranjera, de ser el caso.      3. Los criterios de seguridad del SGCS deben encontrarse disponibles para los clientes en el WEBSITE de CLI.      4. Los proveedores críticos que no cuentan con certificación Basc, se deben comprometer a cumplir los requisitos Basc mediante la firma de un acuerdo de seguridad.      5. Se deben realizar visitas a los asociados de negocios no Basc, para confirmar que cuentan con medidas de seguridad.      6. Se debe contar con la información documentada necesaria de clientes, nuevos socios y personal de la empresa, como la DJ de conocimiento del personal, la constitución de la empresa, revisar sus antecedentes legales, penales, financieros y de sus operaciones.      7. También se debe cumplir con lo indicado en el Manual Anti Soborno y de PLAFT MAN-SIG-002, en relación a los Reportes de Operaciones Sospechosas (ROS).   2. **Seguridad del contenedor, furgón y plataforma**      1. Se debe convenir con los asociados de negocios respecto a la seguridad en el lugar de carga, solicitándoles la firma de acuerdos de seguridad que aseguren que se realizan revisiones a los contenedores vacíos, furgones y camiones.      2. Los precintos utilizados en los contenedores llenos deben cumplir con la norma ISO 17712 y ser utilizados por personal especializado.   3. **Control de acceso físico**      1. Se debe controlar el acceso a las oficinas, verificar el buen funcionamiento del marcador electrónico para el personal y los visitantes deben presentar una identificación y registrase en el cuaderno de visitas,      2. Se debe cumplir con portar los Carnés, tanto el personal de CLI como los visitantes, para una mejor identificación del personal que transita en la oficina.      3. El personal de Recepción debe tener la instrucción de revisar la documentación (o paquete) recibida, antes de ser distribuida.      4. El personal debe conocer y aplicar el procedimiento de Retiro de personas no autorizadas PRO-SIG-036.      5. Las visitas al ingresar a las oficinas de CLI deben mostrar el contenido de sus maletines y declarar si tienen una laptop consigo.      * 1. **Seguridad del personal**      1. La verificación al personal debe ser de acuerdo al procedimiento de Gestión Laboral PRO-RH-022.      2. En RRHH deben tener una relación del personal propio y subcontratado.      3. En el file del personal debe archivarse los documentos básicos del trabajador que incluya su foto, antecedentes, registros de visitas domiciliarias, afiliaciones a instituciones de seguridad social y demás registros.      4. Al personal crítico se le deben tomar periódicamente pruebas para detectar consumo de alcohol y drogas y realizar visitas domiciliarias, en un período máximo de 2 años.      5. En los casos de término del vínculo laboral, se tendrá en cuenta lo establecido en el procedimiento de Gestión Laboral PRO-RH-022.   2. **Procedimientos de seguridad**      1. El personal debe cumplir con lo indicado en los procedimientos de Servicio de Operaciones Aduaneras PRO-OP-018 y Liquidación y Revisión de DAMs PRO-SC-017, para garantizar que la información transmitida a las autoridades sea la correcta      2. Se debe cumplir con la política de Firmas y sellos, que indica las autorizaciones correspondientes a los diferentes procesos de la empresa.      3. Se debe remitir previamente a la autoridad correspondiente la información que ésta solicita.      4. Se debe verificar e informar, de ser el caso, de las discrepancias en la carga; según lo indica el procedimiento Detección y reporte de faltantes o sobrantes de carga PRO-OP-016.      5. Se deben tener actualizadas las glosas del despacho, para mantener la trazabilidad de la operación; como lo indica el procedimiento de Servicio de Operaciones Aduaneras PRO-OP-018.      6. Se deben realizar revisiones periódicas para comprobar el cumplimiento de los requisitos del SGCS.      7. Los integrantes del Comité de Seguridad del SGCS, como Funcionarios de Cumplimiento Anti Soborno deben evaluar el Sistema e informar a la Alta Dirección.   3. **Seguridad física**      1. Se debe controlar el acceso al archivo y el personal debe respetar la indicación de acceso restringido, en salvaguarda de los documentos que se guardan en ese lugar.      2. El Jefe de Seguridad debe contar con el nombramiento del Representante de la Gerencia.      3. Se debe inspeccionar las instalaciones y verificar el buen estado de las mismas, según lo indica el Manual Integrado de Seguridad y Salud MAN-SG-003.      4. Se debe tener un control de las llaves de las puertas de las oficinas.      5. El plano con la ubicación de las áreas sensibles debe estar actualizado.      6. El personal debe conocer y poner en práctica el procedimiento de Contingencia y Emergencia PRO-SIG-015, de ser el caso.      7. Se debe contar con los registros de simulacros o ejercicios prácticos de los planes de seguridad.   4. **Seguridad en las tecnologías de información**      1. Se debe cumplir con lo indicado en los procedimientos siguientes:  1. Sistemas Informáticos PRO-TI-027 2. Seguridad del Sistema PRO-TI-030 3. Copia de respaldo informativo – Backup PRO-TI-028    * 1. Deben instalarse software antivirus y anti-espía en los sistemas.      2. Se debe observar el cumplimiento de las normas relativas a protección de la propiedad intelectual.    1. **Capacitaciones**        1. Se debe crear oportunidades para educar a los clientes en las políticas del SGCS Basc.       2. Se debe capacitar en temas relacionados a la seguridad de la carga, seguridad de la información, lavado de activos y temas afines muy en especial al personal de Operaciones, Archivo, Sistemas, Servicio al Cliente y en general a todo el personal de la empresa; para que sepa reconocer y reportar una amenaza       3. Se cuenta con un programa de Incentivos, por la comunicación del personal en casos de detectar operaciones sospechosas o inusuales.    2. **Seguridad en las Operaciones**       1. Se debe cumplir con lo indicado en el Código de Conducta DOC-SIG-001, respecto a los regalos o donaciones a instituciones del estado 4. Asegurar que ningún trabajador de CLI ofrezca regalos o donaciones a una institución del estado o a un funcionario público, a cambio de realizar u omitir un acto inherente a su cargo. 5. Denunciar si algún funcionario solicita un regalo o dádiva a un trabajador de CLI.    * 1. Cuando en una operación se establece que los riesgos de soborno no pueden ser gestionados por los controles anti soborno existentes, se debe terminar, interrumpir o retirarse de ésta lo más pronto posible. | SCO, COM, JAD  COM, CCA  CCA  CCA  SCO, COM, CCA  SCO, COM, OFI  OFI, GG, JAD, GLO  SUP, SSC, GLO, JAD  SUP, CDE, JAD  JAD, SSI, SEG  ARH  JAD  CCA, SEG  JAD  ARH  ARH  ARH  CCA  ARH  JLE, SLE, LIQ, SUP, CDE, SSC, personal de la UBN  Todo el personal  SSC, SUP, JLE, SLE  JLE, ESC, SLE  JLE, SUP, CDE, SSC, personal de la UBN  JST, CCA, ACA  OFI, GLO, JTS  Todo el personal  GG  SEG  CCA, SSI, JAC  JAD, CCA  CCA  CCA  SSI  SSI  SSI  CCA  ARH, CCA, OFI  GG  JTS, CCA, GLO  GG, GLO, JTS |

1. **CONTROL DE CAMBIOS**
2. Se han agregado como Objetivos del presente manual y como requisitos de nuestro Sistema de Gestión en Control y Seguridad (SGCS), las normas Anti Soborno y las de Prevención del Lavado de Activos y Financiamiento al Terrorismo (PLAFT) en el ítem 1
3. Se modifica el ítem 3.2 indicando que el Comité de Seguridad del SGCS es responsable del cumplimiento del presente manual
4. Se ha actualizado las abreviaturas de los responsables, de las actividades principales a realizar, en el ítem 4.
5. Se incluye el ítem 5.4 que señala que los requisitos a cumplir son los señalados en la norma BASC, el procedimiento de Certificación OEA, las normas de PLAFT y las Anti Soborno del ISO 37001.
6. Se ha agregado el ítem 6.3.5 que indica que las visitas al ingresar a las oficinas de CLI deben mostrar el contenido de sus maletines y declarar si tienen una laptop consigo.
7. Se deben realizar revisiones periódicas para comprobar el cumplimiento de los requisitos del SGCS, como lo señala el ítem 6.5.6.
8. Los integrantes del Comité de Seguridad del SGCS, como Funcionarios de Cumplimiento Anti Soborno deben evaluar el Sistema e informar a la Alta Dirección, según se indica en el ítem 6.5.7.
9. Se ha incluido el ítem 6.9.1 indicando que se debe cumplir con lo indicado en el Código de Conducta DOC-SIG-001, respecto a los regalos o donaciones a instituciones del estado
10. Asegurar que ningún trabajador de CLI ofrezca regalos o donaciones a una institución del estado o a un funcionario público, a cambio de realizar u omitir un acto inherente a su cargo.
11. Denunciar si algún funcionario solicita un regalo o dádiva a un trabajador de CLI.
12. Se adiciona el ítem 6.9.2 señalando que cuando en una operación se establece que los riesgos de soborno no pueden ser gestionados por los controles anti soborno existentes, se debe terminar, interrumpir o retirarse de ésta lo más pronto posible.