



## **1. DIRECTRIZ**

Redllantas S.A. tiene el compromiso de administrar todos sus procesos y sus actividades de comercio, con base en un sistema de administración y gestión de riesgos enfocados en la seguridad de la cadena de suministros internacional, para prevenir y tener planes de contingencia ante la ocurrencia de actividades ilícitas como el contrabando técnico, contrabando abierto, contaminación por tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, lavado de activos, financiación del terrorismo, terrorismo, tráfico de armas, proliferación de armas de destrucción masiva corrupción, soborno, soborno trasnacional; además, de los eventos inesperados con el transporte de la carga como la detención inesperada, hurto o saqueo del contenedor y del vehículo, desvío de la ruta, bloqueo de la vía, accidente de tránsito, falla mecánica y vulneración de sellos y contenedor. Y situaciones que impactan la continuidad del negocio tales como desastre natural, incendio, sabotaje, corte de energía, ciberataques, fallas en las comunicaciones y falla en el transporte. Dando cumplimiento a la normatividad legal aplicable, enfocado los objetivos, metas y programas para el control de estos riesgos identificados en la cadena de suministros.

## **2. OBJETIVO GENERAL**

Definir los conceptos generales y los lineamientos en los que se rige la empresa para la prevención y control de los riesgos enfocados en la seguridad de la cadena de suministros internacional, con el fin de evitar que, en el desarrollo de nuestras operaciones, la empresa sea utilizada directa o indirectamente como instrumento para llevar a cabo actividades ilícitas.

## **3. DEFINICIONES**

### **3.1 Definición de Riesgos**

**Accidente de tránsito:** Incidente vial en la operación del transporte terrestre con un vehículo propio o tercerizado del contenedor y la carga donde se puede presentar avería del vehículo y/o la mercancía.

**Bloqueo de la vía:** Se presenta bloqueo durante la operación de transporte terrestre de los contenedores, por estado de la vía como derrumbe, trabajos de infraestructura, problemas de orden público o grupos delincuenciales.

**Ciberataques:** Ataques de grupos delincuenciales con código malicioso, virus informático, ciberataque, fuga de información, acceso ilegal a la información, infiltración por ingeniería social; que afecta la seguridad de la información contenida en el servidor y en los sistemas de información.



**Contrabando:** Utilización de los vehículos o del contenedor para el transporte de mercancías ilícitas en el territorio nacional y que no presentan documentación de haber sido presentadas o declaradas ante la autoridad aduanera y que no es propiedad de Redllantas.

**Contrabando abierto:** Operación de nacionalización de mercancía diferente o de mercancía no declarada a la autoridad aduanera y que no es propiedad de Redllantas.

**Contrabando técnico:** Operación de gestión documental por parte del proveedor en el exterior donde se relaciona mercancía diferente en las facturas y documentos de la importación.

**Corrupción:** Comportamiento consistente en el ofrecimiento o promesa a otra persona que ostenta cargos públicos, o a personas privadas, a los efectos de obtener ventajas o beneficios contrarios a la legalidad o que sean de naturaleza defraudatoria.

**Corte de energía:** Ausencia de energía eléctrica requerida para el desarrollo de las operaciones de la cadena de suministros en las diferentes sedes de operación.

**Desastre natural:** Eventos naturales como terremoto, sismo, inundación, maremoto, nevadas, tormentas, huracanes, derrumbes o aludes, rayos, tsunamis, fallas geológicas, que puedan afectar la carga en la cadena de suministros internacional o la operación en nuestras instalaciones.

**Desvío de la ruta:** Desvío de la ruta del vehículo que transporta el contenedor, evidenciada por el GPS o por información del conductor de manera forzada por acción de grupos delincuenciales, por motivos de infraestructura vial, por acción de las autoridades de carretera, por problemas de orden público o por condiciones del vehículo.

**Detención inesperada:** Se puede presentar una detención inesperada en tránsito terrestre del vehículo que transporta el contenedor, evidenciada por el GPS o por información del conductor, de manera forzada por acciones de grupos delincuenciales, por problemas de orden público, por las autoridades o motivos de infraestructura vial y fallas del vehículo.

**DTA:** Modalidad de importación donde se autoriza traer una mercancía de cualquier país de origen a una zona franca o un depósito aduanero privado.

**Fallas en el transporte:** Eventos e incidentes de seguridad que se presentan durante el transporte del contenedor y la carga en la cadena de suministros internacional o durante el transporte terrestre de puerto hasta los centros de distribución o las instalaciones del cliente.

**Fallas en las comunicaciones:** Intermittencia o interrupción de los servicios de telecomunicaciones causada por ataques direccionados a los sistemas de comunicación,



por daño en equipos o por la caída de los servicios por parte del proveedor de telecomunicaciones.

**Falla mecánica:** Varada en carretera durante la operación del transporte terrestre del contenedor y la carga desde el puerto a los centros de distribución o el cliente, con un vehículo tercerizado donde se puede presentar un evento de cambio de vehículo o trasbordo o un accidente de tránsito con averías en el contenedor y la carga.

**Faltantes y Sobrantes:** Cantidad verificada durante inspección física o en el descargue del contenedor diferente a la relacionada en los documentos soporte de la importación.

**Financiación del terrorismo:** En Colombia es un delito definido como “el que directamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos armados al margen de la ley o terroristas nacionales o extranjeros”. Ver Código Penal Art. 345.

**Hurto o saqueo del vehículo:** Perdida de la mercancía o del contenedor en la cadena de suministros por organizaciones delincuenciales, piratas marítimos o terrestres, suplantación de identidad de un funcionario de la empresa de transporte o un empleado del cliente.

**Incendio:** Acción ajena con fines destructivos u ocasionado en las sedes de operación por equipos o instalaciones defectuosas, manipulación de elementos de fácil combustión, chispas, fricción.

**LA/FT:** Tener relaciones comerciales con personas naturales o Jurídicas con capitales de origen ilícito cuyo domicilio sea de países considerados no cooperantes o que sean empresa fachada, o sea están legalmente constituidas pero sus operaciones sean ficticias, o que estén reportadas en listas restrictivas vinculantes para Colombia.

**Lavado de activos:** En Colombia es un delito definido como “el que adquiera, resguarde, invierta, transporte, transforme, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes.

**Pandemia:** La propagación mundial de una nueva enfermedad (OMS). Se da cuando un virus se extiende por varios países o continentes y afecta a un gran número de personas. Se refiere a enfermedades infecciosas, aunque a veces se hace referencia a enfermedades no transmisibles.



**Proliferación de armas de destrucción masiva:** Las armas de destrucción masiva son armas diseñadas para matar a una gran cantidad de personas, dirigidas tanto a civiles como a militares. Estas armas no se utilizan generalmente en un objetivo muy específico, sino más bien sobre un área extendida más allá del radio de una milla, con efectos devastadores en las personas, infraestructura y medio ambiente.

**Sabotaje:** Daños o destrucción intencional en nuestra operación de la cadena de suministros, a los procesos, a la información o a las instalaciones, por factores externos como grupos delincuenciales o internos por ocasión de algún tercero o empleado vinculado con la organización.

**Soborno:** El soborno es un delito que se define como el acto de ofrecer, prometer, entregar, aceptar o solicitar una ventaja indebida para influir en las acciones o decisiones de una persona. La ventaja puede ser tangible o intangible, financiera o no, y puede tomar muchas formas, como dinero, regalos, favores, o incluso beneficios no monetarios.

**Soborno Transnacional:** El soborno transnacional es un acto en el que una persona jurídica o sus empleados, administradores, contratistas, asociados o vinculados, ofrecen, prometen o dan dinero u objetos de valor a un servidor público extranjero. El objetivo es que el servidor público realice, omita o retarde un acto relacionado con sus funciones y con una transacción o negocio internacional.


**Terrorismo:** Actos o actividades de grupos terroristas u organizaciones delincuenciales, durante el trayecto en la cadena de suministros internacional de la carga, o en las sedes de operación, donde puede haber pérdidas humanas o de la mercancía por volcamiento, incendio y explosión.

**Tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, tráfico de armas, contaminación:** Introducción de sustancias durante el trayecto en la cadena de suministros internacional de la carga, que pueden ser estupefacientes o sustancias para el procesamiento de narcóticos, armas u otros elementos diferentes a la mercancía de Redllantas.

**Vulneración de sellos y del contenedor:** Los sellos de seguridad y el sello satelital y/o el contenedor han sido abiertos o vulnerados de manera forzosa durante su trayecto internacional y/o en la operación de transporte de puerto a los centros de distribución; para ser saqueado o contaminado.

### 3.2 Abreviaturas

- **DIAN:** Dirección de Impuestos y Aduanas Nacionales.
- **LA/FT:** Lavado de Activos y Financiación del Terrorismo.

	<b>POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA CADENA DE SUMINISTROS INTERNACIONAL</b>	<b>CÓDIGO: DE-PO-003</b>
		<b>VERSIÓN: 1</b>
		<b>FECHA: Jul-2022</b>
		<b>Página 5 de 16</b>

- **OFAC:** Abreviatura de “Office of Foreign Assets Control” que en español significa Oficina de Control de Activos Extranjeros, más conocida como Lista Clinton.
- **ONU:** Organización de las Naciones Unidas.
- **DTA:** Declaración de Tránsito Aduanero.

#### 4. ALCANCE Y APLICACIÓN

Esta política está basada en la siguiente normatividad:

- Decreto número 3568 de 27 de septiembre de 2011 Ministerio de Hacienda y Crédito Público, donde se determina las obligaciones derivadas de la Autorización como Operador Económico Autorizado.
- Resolución 000067 del 20 de octubre de 2016 DIAN, donde se establece el operador económico autorizado para los importadores.
- Decreto 1165 del 02 de Julio del 2019 Ministerio de Hacienda y Crédito Público, por el cual se establece la Legislación Aduanera.
- Circular Externa 0170 del 10 de octubre de 2002 DIAN, cuyo asunto es la prevención y control al lavado de activos.
- Circular Externa 100-000016 del 24 de diciembre del 2020 de Superintendencia de Sociedades, cuyo asunto es la modificación Integral al Capítulo X de la Circular Básica Jurídica de 2017.
- Circular Externa 100-000011 del 9 de agosto de 2021, la Superintendencia de Sociedades modificó integralmente la regulación sobre Programas de Transparencia y Ética Empresarial (PTEE) con el fin de ampliar su ámbito de aplicación y profundizar sobre sus requisitos mínimos para garantizar su efectividad para combatir la corrupción y soborno transnacional.

La cual define el alcance de nuestro sistema de gestión de los riesgos enfocados en la seguridad de la cadena de suministros internacional. Es aplicable a todo el equipo humano vinculado a la empresa de forma directa o indirecta como socios, junta directiva, empleados, clientes, proveedores y a todos los procesos de la cadena de suministros donde se presenten factores de riesgo relacionados con actividades ilícitas o eventos inesperados con la carga.

#### 5. OBJETIVOS DE LA POLÍTICA

En desarrollo de la política del sistema de prevención y gestión de los riesgos de la cadena de suministros internacional, la empresa declara los siguientes objetivos:

5.1 Mantener un sistema de gestión garantizando una cultura organizacional enfocada en la seguridad de la cadena de suministros previniendo y teniendo planes de contingencia ante la ocurrencia de los riesgos de contrabando técnico, contrabando abierto, contaminación por tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, lavado de activos, financiación del terrorismo, terrorismo, tráfico de armas, financiación de la proliferación de armas de destrucción masiva, corrupción, soborno, soborno trasnacional, además de todos los eventos inesperados en el transporte de la carga y situaciones como desastres naturales y riesgos asociados a la operación que impactan la continuidad del negocio; mediante entrenamiento en seguridad y la sensibilización de las políticas, controles, código, reglamento y procedimientos implementados en la empresa.

5.2 Evaluar que el sistema de gestión de riesgos de la cadena de suministros internacional implementado en la organización este alineado con la normatividad vigente.

5.3 Establecer procedimientos claros y de obligatorio cumplimiento para la selección, evaluación, conocimiento, vinculación, actualización y desvinculación de todos los asociados de negocio, con la finalidad de determinar su nivel de riesgo, criticidad y garantizar una debida diligencia en todas las etapas del proceso.

5.4 Vincular y monitorear en la organización a los asociados de negocio, personas naturales, jurídicas o cualquier otro tercero, que no se encuentren reportados en las listas restrictivas vinculantes para Colombia, donde se indique que tiene relación con actividades ilícitas de contrabando técnico, contrabando abierto, contaminación por tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, lavado de activos, financiación del terrorismo, terrorismo, tráfico de armas, proliferación de armas de destrucción masiva, corrupción, soborno, soborno trasnacional sea a nivel nacional o internacional. Si durante la relación comercial se conoce que la contraparte está relacionada con actividades ilícitas o incluidas en las listas restrictivas, se dará por terminada dicha relación comercial.

5.5 Asegurar la confiabilidad de las operaciones con los asociados de negocio críticos y de alto riesgo con los cuales se tienen tercerizadas las operaciones de la cadena de suministros internacional, mediante visitas de seguridad de vinculación y seguimiento, acuerdos de seguridad y planes de contingencia ante eventos inesperados con la carga.

5.6 Garantizar la actualización y evaluación de la información de nuestros asociados de negocio asegurando su confiabilidad y conocimiento de los cambios.

5.7 Asegurar la confiabilidad del personal vinculado, mediante procedimientos para la selección y conocimiento de los candidatos con la realización, análisis y seguimiento de estudios socioeconómicos que incluyen visitas domiciliarias al personal que ocupa cargos críticos, para detectar cambios relevantes o injustificados en el patrimonio.



5.8 Garantizar la actualización de la historia laboral del personal vinculado que incluya información personal y familiar, estudio socioeconómico con revisión de antecedentes, archivo fotográfico y registro de huella dactilar y firma.

5.9 Gestionar los riesgos de incidentes de seguridad de los contenedores en la cadena de suministros como la introducción de personal y/o materiales no autorizados y la vulneración de sellos y del contenedor mediante controles de seguridad para evitar la alteración de su integridad física.

5.10 Garantizar la realización de controles efectivos de acceso para personas y vehículos a nuestras sedes de operación, para que éstos se dirijan únicamente a las áreas autorizadas dentro de las instalaciones y para que el personal vinculado pueda identificar y afrontar a personas no autorizadas o no identificadas al interior de las instalaciones.

5.11 Garantizar una infraestructura física en todas las sedes con barreras perimetrales, señalización e iluminación adecuadas, especialmente en entradas y salidas, las áreas de manejo y almacenamiento de la carga; así como controles de vigilancia, alarmas, monitoreo de cámaras y control de estacionamiento de vehículos, que apoyen la seguridad física.

5.12 Garantizar la confidencialidad, disponibilidad e integridad de la información mediante controles de seguridad de la información, un plan de contingencia informática y políticas para el adecuado manejo de la información, para la creación, administración y asignación de roles, cuentas de acceso a los sistemas de información y correo electrónico, uso de Internet, el correcto uso de los recursos informáticos y todos los controles necesarios que permitan identificar el abuso de los sistemas de cómputo y de tecnología informática, así como el acceso inapropiado y la manipulación indebida de la información.

5.13 Realizar entrenamiento en seguridad a todo el personal mediante programas de inducción, reinducción y capacitaciones periódicas, para garantizar el conocimiento de las medidas de seguridad de la empresa sobre prevención de lavado de activos y financiación del terrorismo, sellos, envío, recibo, manejo y almacenamiento de carga, manejo del correo, consumo de alcohol y drogas, como prevenir, reconocer y actuar frente a cualquier actividad delictiva, manejo de situaciones de pánico, todas las posibles amenazas, riesgos y demás temas sensibles de cada proceso y áreas críticas.

5.14 La Organización capacitará a todos sus colaboradores para identificar y reportar oportunamente cuando se detecten irregularidades o actividades ilegales y sospechosas relacionadas con la seguridad de las operaciones de la cadena de suministros. Así como la socialización a terceros de los protocolos para reportar a las autoridades competentes.

## **6. INDICADORES, METAS Y PROGRAMAS**

Se define en esta política para cada objetivo, indicadores de gestión que permitan evaluar su cumplimiento. Todo esto se realiza con seguimiento a los programas de seguridad



**POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE  
LOS RIESGOS DE SEGURIDAD DE LA CADENA DE  
SUMINISTROS INTERNACIONAL**

**CÓDIGO: DE-PO-003**

**VERSIÓN: 1**

**FECHA: Jul-2022**

**Página 8 de 16**

establecidos y la formulación, el responsable, la fuente de los datos, la frecuencia, la definición de la meta, la medición y el análisis de cada uno de los indicadores se registra en la *DE-FO-003 Ficha Técnica de Indicadores de Gestión*.

<b>OBJETIVOS</b>	<b>INDICADORES</b>	<b>METAS</b>	<b>PROGRAMAS</b>
<b>5.1</b>	Gestión de riesgos aceptables para la organización: Apetito del Riesgo	Aumentar el nivel de riesgo aceptable (bajo) en un 5% semestral	Programa para el cumplimiento de los objetivos de seguridad
<b>5.2</b>	Cumplimiento de objetivos, políticas y controles	100% de cumplimiento de los objetivos, controles y procedimientos del proceso que se está auditando.	Programa de Auditoría
<b>5.2</b>	Revisión y actualización de la matriz de requisitos legales	1 revisión cuatrimestral	Programa para el cumplimiento de los objetivos de seguridad
<b>5.3</b>	Nivel de riesgo de Proveedores	100% de los proveedores vinculados tenga definido su nivel de riesgo en la matriz de criticidad	Programa para el cumplimiento de los objetivos de seguridad
<b>5.3</b>	Nivel de riesgo de clientes	100% de los clientes vinculados tenga definido su nivel de riesgo en la matriz de criticidad	Programa para el cumplimiento de los objetivos de seguridad
<b>5.4</b>	Clientes nuevos vinculados confiables	El 100% de los clientes nuevos vinculados, tienen un proceso de evaluación y conocimiento garantizando su confiabilidad.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.4</b>	Proveedores nuevos vinculados confiables	El 100% de los proveedores nuevos vinculados, tienen un proceso de evaluación y conocimiento garantizando su confiabilidad.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.5</b>	Cumplimiento de las visitas de vinculación, bienales, acuerdos de seguridad y planes de contingencia de los asociados de negocio críticos de la cadena de suministros internacional	El 100% de asociados de negocio, críticos verificados con el cumplimiento de requisitos mínimos de seguridad en la cadena de suministro internacional, mediante visita, acuerdo de seguridad y planes de contingencia.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.6</b>	Clientes con documentos y estudios de seguridad actualizados	Actualizar el 100% de los clientes anualmente	Programa para el cumplimiento de los objetivos de seguridad





**POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE  
LOS RIESGOS DE SEGURIDAD DE LA CADENA DE  
SUMINISTROS INTERNACIONAL**

**CÓDIGO: DE-PO-003**

**VERSIÓN: 1**

**FECHA: Jul-2022**

**Página 9 de 16**

<b>5.6</b>	Proveedores con documentos y estudios de seguridad actualizados	Actualizar el 100% de los proveedores anualmente	Programa para el cumplimiento de los objetivos de seguridad
<b>5.7</b>	Nivel de riesgo de empleados	100% de los empleados vinculados tenga definido su nivel de riesgo en la matriz de cargos críticos.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.7</b>	Empleados y/o socios nuevos vinculados confiables	El 100% de los empleados nuevos vinculados, tienen un proceso de evaluación y conocimiento garantizando su confiabilidad.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.8</b>	Empleados y socios con documentos y estudios de seguridad y socioeconómicos actualizados	Actualizar los datos, documentos y estudios del 100% de los empleados anualmente	Programa para el cumplimiento de los objetivos de seguridad
<b>5.9</b>	Eficacia de los planes de contingencias y emergencias	100% Simulacros de incidentes de seguridad con respuestas efectivas.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.9</b>	Contenedores con novedades e incidentes de seguridad.  •Faltantes, Sobrantes •Averías de la mercancía •Problemas con la documentación del despacho o documentación aduanera •Incumplimiento de especificaciones técnicas. •Requerimientos para inspección física •Materialización de riesgos en la cadena de suministros: contrabando técnico, contrabando abierto, contaminación por tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, lavado de activos, financiación del terrorismo, terrorismo, tráfico de armas, proliferación de armas de destrucción masiva; además, de los eventos inesperados con el transporte de la carga como la detención inesperada, hurto o saqueo del vehículo, desvío de la ruta, bloqueo de la vía, accidente de tránsito, falla	Menos del 5% de Contenedores con novedades e incidentes en el ingreso a los centros de distribución.	Programa para el cumplimiento de los objetivos de seguridad



**POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE  
LOS RIESGOS DE SEGURIDAD DE LA CADENA DE  
SUMINISTROS INTERNACIONAL**

**CÓDIGO: DE-PO-003**

**VERSIÓN: 1**

**FECHA: Jul-2022**

**Página 10 de 16**

	mecánica y vulneración de sellos y contenedor.		
<b>5.9</b>	Certificado de integridad del contenedor	100% de los contenedores ingresados con el certificado de integridad expedido por el proveedor en el país de origen.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.9</b>	Inspección de contenedores recibidos en los CEDIS de los Operadores Logísticos.	100% de los contenedores recibidos en el CEDIS de los Operadores Logísticos con la debida inspección	Programa para el cumplimiento de los objetivos de seguridad
<b>5.9</b>	<p>Novedades de seguridad presentadas en transporte de la mercancía:</p> <ul style="list-style-type: none"><li>•Averías de la carga.</li><li>•Incumplimiento de Acuerdos de Seguridad de proveedores de transporte.</li><li>•Problemas con la documentación del despacho.</li><li>•Eventualidades en el transporte de la carga: Hurto o saqueo del vehículo, desvío de la ruta, bloqueo de la vía, accidente de tránsito, detención inesperada, contaminación, contrabando, alteración de la información (Trazabilidad de la Carga), tráfico de ilícitos (Dinero, armas, estupefacientes, sustancias para el procesamiento de narcóticos).</li></ul>	Menos del 10% de novedades e incidentes de seguridad en la distribución	Programa para el cumplimiento de los objetivos de seguridad
<b>5.9</b>	Inspección de contenedores recibidos en CEDI BOGOTA	100% de los contenedores recibidos en los CEDI BOGOTA con la debida inspección	Programa para el cumplimiento de los objetivos de seguridad
<b>5.9</b>	Inspección de contenedores recibidos en CEDI TABLAZA	100% de los contenedores recibidos en los CEDI TABLAZA con la debida inspección	Programa para el cumplimiento de los objetivos de seguridad
<b>5.10</b>	Cobertura y monitoreo de CCTV frente a áreas críticas en cada sede	100% de todas las áreas críticas cubiertas y monitoreadas por CCTV	Programa para el cumplimiento de los objetivos de seguridad



**POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE  
LOS RIESGOS DE SEGURIDAD DE LA CADENA DE  
SUMINISTROS INTERNACIONAL**


**CÓDIGO: DE-PO-003**

**VERSIÓN: 1**

**FECHA: Jul-2022**

**Página 11 de 16**

<b>5.11</b>	Cobertura de Controles de Acceso y Seguridad Física definidos frente a áreas críticas de cada sede	El 100% de las áreas críticas por cada sede cubiertas por los controles de acceso y seguridad física: carnet, biométricos, llaves, alarmas, botones de pánico, revisiones e inspecciones, vigilancia, barreras perimetrales	Programa para el cumplimiento de los objetivos de seguridad
<b>5.12</b>	Cierre efectivo de los incidentes de tecnología  Nota. Se clasifican en Seguridad, Software, Hardware, Móvil, Telefonía, Ofimática.	El 90% del total de incidentes reportados mensualmente que se encuentren efectivamente cerrados	Programa para el cumplimiento de los objetivos de seguridad
<b>5.12</b>	Cobertura de Back up de información de servidores	90% Cobertura de los Back up de la información de servidores	Programa para el cumplimiento de los objetivos de seguridad
<b>5.12</b>	Efectividad de los Back up realizados	100% Efectividad de los Back up realizados sobre los programados.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.12</b>	Controles de Seguridad Informática en la Creación/ Inactivación de Usuarios de Tecnología	El 100% Controles de Seguridad Informática implementados en la creación y/o inactivación de usuarios de tecnología	Programa para el cumplimiento de los objetivos de seguridad
<b>5.12</b>	Controles de Seguridad Informática en la Asignación de Equipos de Tecnología	El 100% Controles de Seguridad Informática implementados en la Asignación de Equipos de Tecnología	Programa para el cumplimiento de los objetivos de seguridad
<b>5.13</b>	Personas entrenadas, capacitadas, con inducción y reinducción.	100% de cobertura anual en entrenamiento, capacitación y divulgación en riesgos asociados a la prevención, políticas, controles y procedimientos de seguridad de la cadena de suministros.	Programa de Capacitaciones del Sistema Integrado de Gestión
<b>5.13</b>	Eficacia del entrenamiento en seguridad	1 capacitación en seguridad OEA mensual en el programa de capacitaciones	Programa de Capacitaciones del Sistema Integrado de Gestión

	<b>POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA CADENA DE SUMINISTROS INTERNACIONAL</b>	<b>CÓDIGO: DE-PO-003</b>
		<b>VERSIÓN: 1</b>
		<b>FECHA: Jul-2022</b>
		<b>Página 12 de 16</b>

<b>5.14</b>	Nivel de Transparencia Efectividad de las alertas	100 % de las operaciones sospechosas e ilegales detectadas en la cadena de suministros, analizadas y reportadas efectivamente a las autoridades competentes.	Programa para el cumplimiento de los objetivos de seguridad
<b>5.14</b>	Análisis de vulnerabilidad	Monitoreo 100 % de Vulnerabilidades en la seguridad de la cadena de suministros.	Programa para el cumplimiento de los objetivos de seguridad

## 6.1 Programa para el cumplimiento de los objetivos de seguridad

### Objetivos y Actividades:

- a. Simulacros de los planes de emergencia y de contingencia.
- b. Monitoreo de las operaciones de los asociados de negocio de alto riesgo o criticidad.
- c. Auditorías a los procedimientos de vinculación y actualización de asociados de negocios: clientes, proveedores.
- d. Visitas de seguridad y acuerdos de seguridad con los asociados de negocios críticos: clientes, proveedores.
- e. Auditorías a los procedimientos de vinculación, actualización y retiro de los empleados.
- f. Visitas de seguridad y domiciliarias a los empleados.
- g. Monitoreo a la matriz legal: revisión y actualización.
- h. Evaluación al sistema de prevención y administración de riesgos enfocados en la cadena de suministros.
- i. Validación de copias de seguridad de la información efectivamente realizadas.
- j. Realización de controles de seguridad informática.
- k. Reporte de creación/activación de usuarios, e-mail, líneas telefónicas.
- l. Auditoría a los controles de acceso implementados: Uso del carnet, biométrico, registro de planillas, llaves, cámaras, alarmas, botones de pánico, vigilancia.
- m. Capacitación y divulgación en temas de seguridad de la cadena de suministros y de la Información, prevención de riesgos, controles y procedimientos de seguridad.
- n. Programa de Auditoría Interna.
- o. Revisión de los riesgos en la matriz de la cadena de suministros.
- p. Análisis y reporte a las autoridades de las alertas, novedades, operaciones sospechosas e ilegales detectadas en la cadena de suministros y en los estudios de seguridad.
- q. Revisión de las matrices de criticidad de clientes y proveedores y matriz de cargos críticos.
- r. Auditoría a las matrices de documentación de clientes y proveedores.
- s. Revisión para su actualización de la política de prevención y gestión de los riesgos de seguridad de la cadena de suministros internacional.
- t. Registro de la Inspección de contenedores en los diferentes Cedi (Tablaza, Bogotá, Cali).
- u. Registro ajustes de inventario para el análisis de novedades.
- v. Revisión de certificados de integridad del contenedor.
- w. Monitoreo al transporte de la carga.

## **6.2 Programa de Auditorías**

Objetivos y Actividades: Realizar auditorías por procesos, para validar y garantizar el cumplimiento de los requisitos mínimos de seguridad de cada uno de los capítulos OEA, además de las políticas, controles y procedimientos definidos por la organización.

- a. Procedimientos gestión de la cadena de suministros: ingreso y recepción de los contenedores, asignación de transporte, trazabilidad de los contenedores, procedimiento de recepción de la mercancía y almacenamiento y procedimiento de despachos.
- b. Control documental: registros a los documentos de control de la mercancía a los cedis Bogotá. Tablaza y Cali: inspección física de contenedores, remisiones manuales, soportes de entrega de mercancía, soportes de ingreso de mercancía, planillas de despacho a urbanos.
- c. Inventarios: toma física inventario, cruce virtual de inventarios ERP-DMS y Montana, revisión de diferencias: sobrantes y faltantes, garantías y disposición final en los Cedi Tablaza, Bogotá, Cali.
- d. Manejo de efectivo: caja menor, arqueo caja menor.
- e. Procedimientos gestión comercial: listas de precios, descuentos otorgados, condiciones de pago, plan de visita a clientes, estado de los pedidos, bodegas de consignación de clientes revisión de stock, stock vs facturas en cartera.
- f. Procedimientos de asociados de negocio: clientes y proveedores vinculados a la organización con una debida diligencia, actualización de clientes y proveedores, matriz de documentos, matriz de criticidad.
- g. Procedimientos de Compras: conciliación bancaria, cuentas por pagar proveedores por edades, circularización cxp, notas débito y notas crédito a proveedores, pagos a terceros, egresos, manejo de chequeras, nómina, préstamos a empleados.
- h. Procedimientos de Crédito y Cobranza: Cartera, circularización de cuentas por cobrar, cupos de crédito, total cartera, notas débito y notas crédito, saldos vencidos en estado de cuenta de clientes.
- i. Procedimientos de Gestión Humana: empleados-socios vinculados a la organización con una debida diligencia, actualización de empleados, matriz de cargos críticos, matriz de criticidad.
- j. Políticas de seguridad.
- k. Trazabilidad, investigación y seguimiento a incidentes de seguridad reportados en la organización.

## **6.3 Programa de Capacitaciones del Sistema Integrado de Gestión**

Objetivos y Actividades: Realizar inducciones, reinducciones, entrenamiento y capacitaciones en los requisitos mínimos de seguridad de los capítulos de OEA:

- I. Análisis y Administración del riesgo: Reinducción de la política, procedimientos y controles del sistema de gestión de riesgos de la cadena de suministros, alertas, operaciones Inusuales, sospechosas y actividades ilegales en la cadena de suministros; sensibilización presentación OEA y plan de trabajo, gestión de riesgos en el proceso de vinculación de clientes y proveedores.



II Asociados de Negocio: Capacitación modulo virtual solicitud de vinculación de clientes - plataforma virtual, socialización procedimiento conocimiento y vinculación de proveedores, socialización procedimiento conocimiento y vinculación de clientes, matriz de criticidad de clientes, matriz de criticidad de clientes, seguridad en asociados de negocio OEA.

III Seguridad de contenedor y unidades de carga: Seguridad del contenedor y unidades de carga, Inspección de contenedores y sellos de seguridad, reinducción y socialización nueva regulación aduanera, Decreto 1165 de 2019.

IV Controles de acceso físico: Socialización planos áreas críticas, simulacro de detección de paquetes extraños, controles de acceso a cada sede, inspección de personas, paquetes, correspondencia y seguridad física

V. Seguridad del personal: Socialización y entrega código de ética y buen gobierno, socialización organigrama y de las políticas de seguridad del personal, proceso de vinculación, actualización y retiro.

VI. Seguridad de los procesos: Listado maestro de documentos e indicadores de gestión, socialización cadena de suministros, proveedores y planes de contingencia importaciones.

VII. Seguridad física: Inducción para activar e inactivar la alarma Oficina Poblado, Seguridad del sistema de Alarma CEDI Bogotá, Inducción para activar e inactivar la alarma CEDI Tablaza, levantamiento de puesto de trabajo.

VIII. Seguridad en T.I: Sensibilización en seguridad de la información, políticas de seguridad de la información.

Todos los colaboradores, de todos los niveles y cargos, se encuentran en la obligación de velar por el interés general de la Organización y acatar la presente Política para evitar que se materialicen los riesgos que afecten la seguridad de la cadena de suministros y que impactan la continuidad del negocio. Cualquier infracción a la misma, será considerada como una falta grave, de acuerdo con lo establecido en el Reglamento Interno de Trabajo.

Esta política aprobada se firma a los 14 días del mes de julio de 2022.

**EDUARDO ENRIQUE ROJO SALAZAR**  
**Representante Legal**



<b>RESUMEN DE ACTUALIZACIONES</b>		
<b>VERSION MODIFICADA</b>	<b>DESCRIPCION DEL CAMBIO</b>	<b>OBSERVACIONES</b>
0	<p>Se actualiza la Política Integral para darle alcance a la nueva normatividad del SAGRILAFT e incluir dentro del Sistema de Gestión Integral de Redllantas el Programa de Transparencia y Ética Corporativa – PTEE, de acuerdo con: Circular Externa 100-000016 del 24 de diciembre del 2020 de Superintendencia de Sociedades, cuyo asunto es la modificación Integral al Capítulo X de la Circular Básica Jurídica de 2017. Y la Circular Externa 100-000011 del 9 de agosto de 2021, la Superintendencia de Sociedades modificó integralmente la regulación sobre Programas de Transparencia y Ética Empresarial.</p> <p>Además, se actualiza la Política dada la identificación de nuevos riesgos en la Matriz de la Cadena de suministros:</p> <p>_R016: Errores en Finalizaciones de Importación (DTA) _R030: Errores en Finalizaciones de Importación (DTA) _R040: Errores en transporte de Contenedores en (DTA)</p>	



**POLÍTICA PARA LA PREVENCIÓN Y GESTIÓN DE  
LOS RIESGOS DE SEGURIDAD DE LA CADENA DE  
SUMINISTROS INTERNACIONAL**

**CÓDIGO: DE-PO-003**

**VERSIÓN: 1**

**FECHA: Jul-2022**

**Página 16 de 16**

	<p>_R046: Incumplimiento con el manejo de los inventarios FIFO (Mercancía Nacionalizada o DTA) _R071: Pandemia _R072: "Bloqueo de la vía (Paros armados y problemas de orden público)"</p>	

<b>REVISION Y APROBACIÓN</b>		
<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>APROBADO POR</b>
Jefe de Mejoramiento Continuo - Líder OEA Gerente Administrativo	Jefe de Mejoramiento Continuo	Gerente General
<b>FECHA:</b> Julio de 2022	<b>FECHA:</b> Julio de 2022	<b>FECHA:</b> Julio de 2022

<b>REVISIONES DEL DOCUMENTO</b>		
<b>FECHA</b>	<b>REVISADO POR</b>	<b>OBSERVACIONES</b>
10 de julio del 2021	Jefe de Mejoramiento Continuo	No se presentan cambios para una nueva versión
14 de julio del 2022	Jefe de Mejoramiento Continuo	Se ajusta la política generando cambio de versión V1.